Amtsblatt der Europäischen Union

L 135

Ausgabe in deutscher Sprache

Rechtsvorschriften

62. Jahrgang

22. Mai 2019

Inhalt

DE

Bei Rechtsakten, deren Titel in magerer Schrift gedruckt sind, handelt es sich um Rechtsakte der laufenden Verwaltung im Bereich der Agrarpolitik, die normalerweise nur eine begrenzte Geltungsdauer haben.

Rechtsakte, deren Titel in fetter Schrift gedruckt sind und denen ein Sternchen vorangestellt ist, sind sonstige Rechtsakte.

I

(Gesetzgebungsakte)

VERORDNUNGEN

VERORDNUNG (EU) 2019/816 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 17. April 2019

zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 82 Absatz 1 Unterabsatz 2 Buchstabe d,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

gemäß dem ordentlichen Gesetzgebungsverfahren ([1]),

in Erwägung nachstehender Gründe:

(1) Die Union verfolgt das Ziel, ihren Bürgerinnen und Bürgern einen Raum der Freiheit, der Sicherheit und des Rechts ohne Binnengrenzen zu bieten, in dem der freie Personenverkehr gewährleistet ist. Dieses Ziel sollte unter anderem mittels geeigneter Maßnahmen zur Verhütung und Bekämpfung von Kriminalität, einschließlich organisierter Kriminalität und Terrorismus, erreicht werden.

(2) Hierzu ist es nötig, dass Informationen zu Verurteilungen, die in den Mitgliedstaaten erfolgt sind, auch außerhalb des Urteilsmitgliedstaats herangezogen werden können, und zwar zur Berücksichtigung in neuen Strafverfahren, wie das im Rahmenbeschluss 2008/675/JI des Rates ([2]) vorgesehen ist, sowie zur Verhütung neuer Straftaten.

(3) Damit dieses Ziel erreicht werden kann, müssen Informationen aus den Strafregistern zwischen den zuständigen Behörden der Mitgliedstaaten ausgetauscht werden. Ein entsprechender Informationsaustausch wird gemäß den Bestimmungen des Rahmenbeschlusses 2009/315/JI des Rates ([3]) und über das Europäische Strafregisterinformationssystem (European Criminal Records Information System — ECRIS), das durch den Beschluss 2009/316/JI des Rates ([4]) eingerichtet wurde, durchgeführt und erleichtert.

(4) Der geltende Rechtsrahmen für das ECRIS trägt jedoch den Besonderheiten von Anfragen zu Drittstaatsangehörigen nicht in ausreichendem Maße Rechnung. Zwar ist ein Austausch von Informationen zu Drittstaatsangehörigen über ECRIS bereits möglich, jedoch gibt es kein einheitliches Unionsverfahren, um diesen Austausch effizient, schnell und präzise abzuwickeln.

(5) Innerhalb der Union werden Informationen zu Drittstaatsangehörigen nicht wie bei Staatsangehörigen der Mitgliedstaaten im jeweiligen Herkunftsmitgliedstaat erhoben, sondern nur in den Mitgliedstaaten gespeichert, in denen die Verurteilungen erfolgt sind. Ein vollständiger Überblick über die Vorstrafen eines Drittstaatsangehörigen lässt sich daher nur gewinnen, wenn aus allen Mitgliedstaaten entsprechende Informationen angefordert werden.

([1]) Stellungnahme des Europäischen Parlaments vom 12. März 2019 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 9. April 2019.

([2]) Rahmenbeschluss 2008/675/JI des Rates vom 24. Juli 2008 zur Berücksichtigung der in anderen Mitgliedstaaten der Europäischen Union ergangenen Verurteilungen in einem neuen Strafverfahren (ABl. L 220 vom 15.8.2008, S. 32).

([3]) Rahmenbeschluss 2009/315/JI des Rates vom 26. Februar 2009 über die Durchführung und den Inhalt des Austauschs von Informationen aus dem Strafregister zwischen den Mitgliedstaaten (ABl. L 93 vom 7.4.2009, S. 23).

([4]) Beschluss 2009/316/JI des Rates vom 6. April 2009 zur Einrichtung des Europäischen Strafregisterinformationssystems (ECRIS) gemäß Artikel 11 des Rahmenbeschlusses 2009/315/JI (ABl. L 93 vom 7.4.2009, S. 33).

(6) Derartige generelle Auskunftsersuchen stellen einen unverhältnismäßig hohen Verwaltungsaufwand für alle Mitgliedstaaten dar, auch für diejenigen, die über keine Informationen zu dem betreffenden Drittstaatsangehörigen verfügen. In der Praxis hält dieser Aufwand die Mitgliedstaaten von Auskunftsersuchen zu Drittstaatsangehörigen bei anderen Mitgliedstaaten ab, wodurch der Informationsaustausch zwischen ihnen stark beeinträchtigt wird und ihr Zugang zu Strafregisterinformationen auf die im jeweiligen nationalen Strafregister gespeicherten Daten beschränkt bleibt. In der Folge erhöht sich die Gefahr eines ineffizienten und unvollständigen Austauschs von Informationen zwischen den Mitgliedstaaten, was sich wiederum auf die Sicherheit der Unionsbürger und der in der Union wohnhaften Personen auswirkt.

(7) Zur Abhilfe sollte ein System eingerichtet werden, mit dem die Zentralbehörde eines Mitgliedstaats umgehend und effizient feststellen kann, welche anderen Mitgliedstaaten über Strafregisterinformationen zu einem Drittstaatsangehörigen (TCN — third country national) verfügen (, im Folgenden „ECRIS-TCN“). Anschließend könnte auf den bestehenden ECRIS-Rahmen zurückgegriffen werden, um die betreffenden Mitgliedstaaten gemäß dem Rahmenbeschluss 2009/315/JI um die Strafregisterinformationen zu ersuchen.

(8) Diese Verordnung sollte daher Vorschriften über die Einrichtung eines zentralisierten Systems vorsehen, in dem auf Unionsebene personenbezogene Daten erfasst werden, und Vorschriften über die Aufteilung der Zuständigkeiten zwischen den Mitgliedstaaten sowie zur Bestimmung, welche Organisation für die Entwicklung und Wartung des zentralisierten Systems zuständig ist, sowie zusätzlich zu den bestehenden datenschutzrechtlichen Regelungen spezifische datenschutzrechtliche Bestimmungen, um einen insgesamt angemessenen Datenschutz, eine angemessene Datensicherheit und den Schutz der Grundrechte der betroffenen Personen zu gewährleisten.

(9) Um den Bürgerinnen und Bürgern der Union ein Raum der Freiheit, der Sicherheit und des Rechts ohne Binnengrenzen zu bieten, in dem der freie Personenverkehr gewährleistet ist, müssen auch die Informationen über Verurteilungen von Unionsbürgern, die zusätzlich die Staatsangehörigkeit eines Drittstaats besitzen, vollständig sein. Da diese Personen mit einer oder mehreren Staatsangehörigkeiten auftreten können und in den Urteilsmitgliedstaaten, oder in dem Herkunftsmitgliedstaat verschiedene Verurteilungen gespeichert sein können, müssen Unionsbürger, die auch die Staatsangehörigkeit eines Drittstaats besitzen, in den Anwendungsbereich dieser Verordnung aufgenommen werden. Diese Personen auszuschließen würde dazu führen, dass die im ECRIS-TCN gespeicherte Information unvollständig wäre. Das würde die Zuverlässigkeit des Systems aufs Spiel setzen. Da jedoch diese Personen die Unionsbürgerschaft besitzen, sollten für die Einstellung ihrer Fingerabdruckdaten in das ECRIS-TCN vergleichbare Bedingungen wie für den Austausch von Fingerabdruckdaten von Unionsbürgern im Rahmen des durch den Rahmenbeschluss 2009/315/JI und den Beschluss 2009/316/JI geschaffenen ECRIS- zwischen den Mitgliedstaaten gelten. Somit sollten die Fingerabdruckdaten von Unionsbürgern, die auch die Staatsangehörigkeit eines Drittstaats besitzen, nur dann in das ECRIS-TCN eingestellt werden, wenn sie gemäß dem nationalen Recht während eines Strafverfahrens erhoben wurden, wobei die Mitgliedstaaten für diese Eingabe Fingerabdruckdaten nutzen dürfen, die zu anderen Zwecken als Strafverfahren abgenommen wurden, wenn diese Nutzung nach nationalem Recht zulässig ist.

(10) Mit dem ECRIS-TCN sollte die Verarbeitung von Fingerabdruckdaten ermöglicht werden, um festzustellen, in welchen Mitgliedstaaten Informationen über Strafregistereinträge eines Drittstaatsangehörigen vorliegen. Außerdem sollte es die Verarbeitung von Gesichtsbildern ermöglichen, um die Identität des Drittstaatsangehörigen zu bestätigen. Es ist wesentlich, dass die Eingabe und Verwendung von Fingerabdruckdaten und Gesichtsbildern nicht über das zur Erreichung des Ziels unbedingt erforderliche Maß hinausgehen, die Grundrechte und das Kindeswohl wahren und mit den anwendbaren Datenschutzvorschriften der Union vereinbar sind.

(11) Die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), die durch die Verordnung (EU) Nr. 2018/1726 des Europäischen Parlaments und des Rates ([5]) errichtet wurde, sollte aufgrund ihrer Erfahrung mit anderen Großsystemen im Bereich Justiz und Inneres mit der Entwicklung und dem Betrieb des ECRIS-TCN betraut werden. Diese neuen Aufgaben sollten auch in ihr Mandat aufgenommen werden.

(12) eu-LISA sollte mit geeigneten Finanzressourcen und Personal ausgestattet werden, damit sie die Aufgaben gemäß dieser Verordnung erfüllen kann.

(13) Da das gegenwärtige ECRIS-TCN und ECRIS technisch eng miteinander verknüpft werden müssen, sollte eu-LISA auch die Aufgabe übertragen werden, die ECRIS-Referenzimplementierung weiterzuentwickeln und zu warten, und das Mandat der Agentur sollte entsprechend angepasst werden.

(14) Vier Mitgliedstaaten haben eine eigene nationale ECRIS-Implementierungssoftware gemäß dem Beschluss 2009/316/JI des Rates entwickelt und verwenden diese anstelle der ECRIS-Referenzimplementierung für den Austausch von Strafregisterinformationen. Angesichts der spezifischen Merkmale, die diese Mitgliedstaaten für nationale Anwendungszwecke in ihre Systeme aufgenommen haben, sowie der von ihnen getätigten Investitionen sollten sie ihre nationale ECRIS-Implementierungssoftware für die Zwecke des ECRIS-TCN ebenfalls verwenden dürfen, sofern die in dieser Verordnung genannten Bedingungen erfüllt sind.

([5]) Verordnung (EU) 2018/1726 des Europäischen Parlaments und des Rates vom 14. November 2018 über die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Beschlusses 2007/533/JI des Rates sowie zur Aufhebung der Verordnung (EU) Nr. 10772011 (ABl. L 295 vom 21.11.2018, S. 99).

(15) Das ECRIS-TCN sollte nur Angaben zur Identität von Drittstaatsangehörigen enthalten, die von einem Strafgericht in der Union verurteilt wurden. Diese Identitätsangaben sollten alphanumerische Daten und Fingerabdruckdaten umfassen. Es sollte auch möglich sein, Gesichtsbilder aufzunehmen, sofern das Recht des Urteilsmitgliedstaats die Erhebung und Speicherung von Gesichtsbildern einer verurteilten Person zulässt.

(16) Die alphanumerischen Daten, die von den Mitgliedstaaten in das Zentralsystem einzugeben sind, sollten den Nachnamen (Familiennamen) und den bzw. die Vornamen der verurteilten Person sowie — sofern die Zentralbehörde über solche Informationen verfügt — alle etwaigen Pseudonyme oder Aliasdaten dieser Person enthalten. Wenn dem betreffenden Mitgliedstaat andere abweichende personenbezogene Daten, wie z. B. die unterschiedliche Schreibweise eines Namens in einem anderen Alphabet, bekannt sind, so sollte es möglich sein, diese Daten als zusätzliche Informationen in das Zentralsystem einzugeben.

(17) Die alphanumerischen Daten sollten ferner als zusätzliche Information die Identitätsnummer oder die Art und Nummer der Identitätsdokumente der Person sowie die Bezeichnung der Ausstellungsbehörde enthalten, sofern die Zentralbehörde über diese Informationen verfügt. Der Mitgliedstaat sollte versuchen, die Echtheit der Identitätsdokumente zu überprüfen, bevor die entsprechenden Daten in das Zentralsystem eingegeben werden. Da diese Informationen unzuverlässig sein könnten, sollten sie in jedem Fall mit Vorsicht verwendet werden.

(18) Die Zentralbehörden sollten das ECRIS-TCN nutzen, um festzustellen, in welchen Mitgliedstaaten Strafregisterinformationen zu einem Drittstaatsangehörigen vorliegen, wenn in dem betreffenden Mitgliedstaat entsprechende Strafregisterinformationen zu dieser Person für die Zwecke eines gegen sie gerichteten Strafverfahrens oder für die in dieser Verordnung genannten Zwecke benötigt werden. Zwar sollte das ECRIS-TCN in derartigen Fällen grundsätzlich immer genutzt werden, doch sollte die für die Durchführung des Strafverfahrens zuständige Behörde entscheiden können, dass das System nicht verwendet werden sollte, wenn das im konkreten Fall nicht angezeigt wäre, zum Beispiel bei bestimmten Arten von Eilverfahren, bei Transitreisenden, wenn bereits kurz zuvor Strafregisterinformationen über das ECRIS abgerufen wurden oder bei geringfügigen Zuwiderhandlungen, insbesondere geringfügigen Verkehrsübertretungen, geringfügigen Zuwiderhandlungen gegen allgemeine Gemeindeverordnungen und geringfügigen Zuwiderhandlungen gegen die öffentliche Ordnung.

(19) Die Mitgliedstaaten sollten ferner das ECRIS-TCN für andere als die in dieser Verordnung genannten Zwecke nutzen können, sofern das nach und gemäß dem nationalen Recht vorgesehen ist. Um die Nutzung des ECRIS-TCN transparenter zu gestalten, sollten die Mitgliedstaaten jedoch diese anderen Zwecke der Kommission mitteilen, die dafür sorgen sollte, dass alle diese Mitteilungen im *Amtsblatt der Europäischen Union* veröffentlicht werden.

(20) Es sollte auch für andere Behörden, die Strafregisterinformationen anfordern, möglich sein zu entscheiden, dass das ECRIS-TCN nicht genutzt werden sollte, wenn das im konkreten Fall nicht angezeigt wäre, zum Beispiel wenn bestimmte administrative Standardabfragen im Zusammenhang mit den beruflichen Qualifikationen einer Person durchgeführt werden müssen, vor allem wenn bekannt ist, dass unabhängig vom Ergebnis der Suche im ECRIS-TCN keine Strafregisterinformationen aus anderen Mitgliedstaaten angefordert werden. Das ECRIS-TCN sollte allerdings stets genutzt werden, wenn die Abfrage der Strafregisterinformationen von einer Person initiiert wurde, die einen Antrag auf Informationen über die sie betreffenden Strafregistereintragungen gemäß dem Rahmenbeschluss 2009/315/JI stellt, oder wenn der Antrag gestellt wird, um Strafregisterinformationen gemäß Richtlinie 2011/93/EU des Europäischen Parlaments und des Rates ([6]) zu erhalten.

(21) Drittstaatsangehörige sollten das Recht haben, schriftliche Auskunft über die eigenen Strafregisterinformationen gemäß dem Recht des Mitgliedstaats, in dem sie die Bereitstellung solcher Informationen beantragen, und gemäß dem Rahmenbeschluss 2009/315/JI zu erhalten. Bevor der betreffende Mitgliedstaat diese Auskunft einem Drittstaatsangehörigen erteilt, sollte er das ECRIS-TCN abfragen.

(22) Unionsbürger, die auch die Staatsangehörigkeit eines Drittstaats besitzen, werden nur dann in das ECRIS-TCN aufgenommen, wenn den zuständigen Behörden bekannt ist, dass die betreffenden Personen die Staatsangehörigkeit eines Drittstaats besitzen. Ist den zuständigen Behörden nicht bekannt, dass Unionsbürger auch die Staatsangehörigkeit eines Drittstaats besitzen, so kann es dennoch vorkommen, dass diese Personen früher bereits als Staatsangehörige eines Drittstaats verurteilt worden sind. Damit sichergestellt ist, dass die zuständigen Behörden einen vollständigen Überblick über Vorstrafen erhalten, sollte es möglich sein, Abfragen im ECRIS-TCN durchzuführen, um zu überprüfen, ob zu einem Unionsbürger in einem Mitgliedstaat Strafregisterinformationen zu dieser Person als Drittstaatsangehörigem vorliegen.

(23) Wenn es zwischen den von einem Mitgliedstaat verwendeten Suchanfragedaten und den im Zentralsystem gespeicherten Daten eine Übereinstimmung gibt (im Folgenden „Treffer“), sollten die Identitätsangaben, auf die sich der Treffer bezieht, zusammen mit dem Treffer angezeigt werden. Das Suchergebnis sollte von den Zentralbehörden nur zum Zweck eines Auskunftsersuchens über ECRIS, oder von der Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust), errichtet durch die Verordnung (EU) 2018/1727

([6]) Richtlinie 2011/92/EU des Europäischen Parlaments und des Rates vom 13. Dezember 2011 zur Bekämpfung des sexuellen Missbrauchs und der sexuellen Ausbeutung von Kindern sowie der Kinderpornografie sowie zur Ersetzung des Rahmenbeschlusses 2004/68/JI des Rates (ABl. L 335 vom 17.12.2011, S. 1).

des Europäischen Parlamentes und des Rates ([7]), von der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol), errichtet durch die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates ([8]) und von der Europäischen Staatsanwaltschaft (EPPO), errichtet durch die Verordnung (EU) 2017/1939 des Rates ([9]), nur zum Zweck eines Auskunftsersuchens zu Verurteilungen gemäß der vorliegenden Verordnung genutzt werden.

(24) Vorerst sollten im ECRIS-TCN enthaltene Gesichtsbilder ausschließlich für die Bestätigung der Identität eines Drittstaatsangehörigen verwendet werden, um die Mitgliedstaaten zu ermitteln, in denen Informationen über frühere Verurteilungen dieses Drittstaatsangehörigen vorliegen. In Zukunft sollte es möglich sein, Gesichtsbilder für den automatisierten Abgleich biometrischer Daten zu verwenden, sofern die technischen und politischen Voraussetzungen dafür erfüllt sind. Die Kommission sollte unter Berücksichtigung der Notwendigkeit und Verhältnismäßigkeit sowie der technischen Entwicklungen auf dem Gebiet der Gesichtserkennungssoftware die Verfügbarkeit und Einsatzfähigkeit der benötigten Technologie bewerten, bevor sie einen delegierten Rechtsaktüber die Verwendung von Gesichtsbildern zur Identifizierung von Drittstaatsangehörigen erlässt, um festzustellen, in welchen Mitgliedstaaten Informationen über frühere Verurteilungen der betreffenden Personen vorliegen.

(25) Biometrische Daten werden benötigt, weil sie die zuverlässigste Grundlage für die Identifizierung von Drittstaatsangehörigen im Hoheitsgebiet der Mitgliedstaaten bieten, die oftmals weder Ausweispapiere noch sonstige Identitätsdokumente mit sich führen, und zudem einen zuverlässigeren Abgleich der Angaben zu Drittstaatsangehörigen ermöglichen.

(26) Die Mitgliedstaaten sollten in das Zentralsystem Fingerabdruckdaten eingeben, die verurteilten Drittstaatsangehörigen nach Maßgabe des nationalen Rechts im Rahmen eines Strafverfahrens abgenommen wurden. Damit das Zentralsystem möglichst vollständige Identitätsangaben enthält, sollten die Mitgliedstaaten in dieses System auch Fingerabdruckdaten eingeben können, die für andere Zwecke als die eines Strafverfahrens abgenommen wurden, sofern diese Fingerabdruckdaten gemäß nationalem Recht in Strafverfahren genutzt werden können.

(27) In dieser Verordnung sollten Mindestkriterien für Fingerabdruckdaten festgelegt werden, die die Mitgliedstaaten in das Zentralsystem einstellen sollten. Die Mitgliedstaaten sollten wählen können, ob sie entweder die Fingerabdruckdaten von Drittstaatsangehörigen eingeben, die zu einer Freiheitsstrafe von mindestens sechs Monaten verurteilt wurden, oder ob sie die Fingerabdruckdaten von Drittstaatsangehörigen eingeben, die wegen einer Tat verurteilt wurden, die nach dem Recht des jeweiligen Mitgliedstaats mit einer Freiheitsstrafe im Höchstmaß von mindestens zwölf Monaten bedroht ist.

(28) Die Mitgliedstaaten sollten im ECRIS-TCN Datensätze über verurteilte Drittstaatsangehörige anlegen. Das sollte, soweit möglich, automatisch und unverzüglich nach Erfassung der Verurteilung im nationalen Strafregister erfolgen. Die Mitgliedstaaten sollten gemäß dieser Verordnung alphanumerische Daten und Fingerabdruckdaten im Zusammenhang mit Verurteilungen in das Zentralsystem eingeben, die nach dem Tag des Beginns der Dateneingabe in das ECRIS-TCN erfolgt sind. Ab demselben oder einem späteren Zeitpunkt sollten die Mitgliedstaaten Gesichtsbilder in das Zentralsystem eingeben können.

(29) Die Mitgliedstaaten sollten gemäß dieser Verordnung auch im ECRIS-TCN Datensätze für Verurteilungen von Drittstaatsangehörigen anlegen, die vor dem Zeitpunkt des Beginns der Dateneingabe ergangen sind, um eine größtmögliche Wirksamkeit des Systems zu gewährleisten. In diesem Zusammenhang sollten die Mitgliedstaaten jedoch nicht verpflichtet sein, Informationen zu erheben, die vor dem Beginn der Dateneingabe noch nicht in ihrem Strafregister erfasst waren. Die Fingerabdruckdaten von Drittstaatsangehörigen, die im Zusammenhang mit solchen früheren Verurteilungen abgenommen werden, sollten nur dann gespeichert werden, wenn sie im Rahmen von Strafverfahren abgenommen wurden und der betreffende Mitgliedstaat der Auffassung ist, dass sie anderen Identitätsangaben in Strafregistern eindeutig zugeordnet werden können.

(30) Ein besserer Austausch von Informationen zu Verurteilungen sollte den Mitgliedstaaten die Umsetzung des Rahmenbeschlusses 2008/675/JI erleichtern, dem zufolge die Mitgliedstaaten verpflichtet sind, frühere Verurteilungen in anderen Mitgliedstaaten im Rahmen neuer Strafverfahren in dem Maße zu berücksichtigen, wie Vorstrafen nach innerstaatlichem Recht berücksichtigt werden.

([7]) Verordnung (EU) 2018/1727 des Europäischen Parlaments und des Rates vom 14. November 2018 betreffend die Agentur der Europäischen Union für justizielle Zusammenarbeit in Strafsachen (Eurojust) und zur Ersetzung und Aufhebung des Beschlusses 2002/187/JI des Rates (ABl. L 295 vom 21.11.2018, S. 138).

([8]) Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).

([9]) Verordnung (EU) 2017/1939 des Rates vom 12. Oktober 2017 zur Durchführung einer Verstärkten Zusammenarbeit zur Errichtung der Europäischen Staatsanwaltschaft (EUStA) (ABl. L 283 vom 31.10.2017, S. 1).

(31) Wenn eine Abfrage im ECRIS-TCN einen Treffer ergibt, sollte das nicht automatisch so verstanden werden, dass der betreffende Drittstaatsangehörige in dem bzw. den angegebenen Mitgliedstaaten verurteilt worden ist. Das Vorliegen von Vorstrafen sollte ausschließlich anhand der Angaben aus dem Strafregister der betreffenden Mitgliedstaaten nachgewiesen werden.

(32) Ungeachtet der Möglichkeit, die Finanzprogramme der Union nach Maßgabe der geltenden Vorschriften in Anspruch zu nehmen, sollten die Mitgliedstaaten ihre eigenen Kosten tragen, die aus der Umsetzung, Verwaltung, Verwendung und Wartung ihrer Strafregisterdatenbanken und ihrer nationalen Fingerabdruckdatenbanken sowie aus der Umsetzung, Verwaltung, Verwendung und Wartung der für die Nutzung des ECRIS-TCN benötigten technischen Änderungen, einschließlich der Anbindung der Datenbanken an die zentrale nationale Zugangsstelle, entstehen.

(33) Eurojust, Europol und die EUStA sollten Zugang zum ECRIS-TCN haben, damit sie ermitteln können, in welchen Mitgliedstaaten Strafregisterinformationen zu einem Drittstaatsangehörigen vorliegen, und somit ihre gesetzlichen Aufgaben effizienter erfüllen können. Unbeschadet der Anwendung der Grundsätze der justiziellen Zusammenarbeit in Strafsachen einschließlich der Vorschriften über die Rechtshilfe sollte Eurojust ebenfalls direkten Zugang zum ECRIS-TCN haben, um so die gemäß dieser Verordnung zugewiesene Aufgabe wahrnehmen zu können, als Ansprechpartner für Drittländer und internationale Organisationen zu dienen. Zwar sollte der Standpunkt der nicht an der Verstärkten Zusammenarbeit zur Errichtung der EUStA beteiligten Mitgliedstaaten berücksichtigt werden, doch sollte der EUStA der Zugang zu Informationen zu Verurteilungen nicht allein aufgrund der Tatsache verweigert werden, dass sich der betreffende Mitgliedstaat nicht an dieser Verstärkten Zusammenarbeit beteiligt.

(34) Diese Verordnung sieht strenge Vorschriften für den Zugang zum ECRIS-TCN und die notwendigen Garantien vor, einschließlich der Verantwortung der Mitgliedstaaten für die Erhebung und Verwendung der Daten. Außerdem ist festgelegt, wie Einzelpersonen ihr Recht auf Schadenersatz, Auskunft, Berichtigung, Löschung und Regress ausüben können, insbesondere das Recht, einen wirksamen Rechtsbehelf einzulegen, und dass die Datenverarbeitung von unabhängigen Behörden überwacht wird. Somit steht diese Verordnung im Einklang mit den Grundrechten und -freiheiten und den Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden, darunter das Recht auf den Schutz personenbezogener Daten, der Grundsatz der Gleichheit vor dem Gesetz und das allgemeine Diskriminierungsverbot. In dieser Hinsicht trägt sie auch der Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten, dem Internationalen Pakt über bürgerliche und politische Rechte und anderen völkerrechtlichen Menschenrechtsverpflichtungen Rechnung.

(35) Die Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates ([10]) sollte für die Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor Gefahren für die öffentliche Sicherheit und deren Abwehr gelten. Sofern die Verarbeitung personenbezogener Daten durch nationale Behörden nicht in den Anwendungsbereich der Richtlinie (EU) 2016/680 fällt, sollte für diese Verarbeitung die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([11]) gelten. Gemäß der Verordnung (EU) 2018/1725 ([12]), die auch für die Verarbeitung personenbezogener Daten durch eu-LISA gelten sollte, sollte eine koordinierte Aufsicht sichergestellt werden.

(36) Die Zentralbehörden sollten die alphanumerischen Daten zu früheren Verurteilungen bis zum Ablauf der Frist für die Eingabe von Daten gemäß dieser Verordnung und die Fingerabdruckdaten innerhalb von zwei Jahren nach dem Tag der Inbetriebnahme des ECRIS-TCN- eingeben. Die Mitgliedstaaten sollten befugt sein, auch alle Daten zum gleichen Zeitpunkt einzugeben, sofern diese Fristen eingehalten werden.

(37) Ferner sollten Vorschriften erlassen werden über die Haftung der Mitgliedstaaten, von Eurojust, von Europol, der EUStA und von eu-LISAfür Schäden aufgrund eines Verstoßes gegen diese Verordnung.

(38) Damit besser ermittelt werden kann, in welchen Mitgliedstaaten Informationen über frühere Verurteilungen von Drittstaatsangehörigen vorliegen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte zur Ergänzung dieser Verordnung durch Bestimmungen über die Verwendung von Gesichtsbildern zur Identifizierung von Drittstaatsangehörigen zu erlassen, um festzustellen, in welchen Mitgliedstaaten Informationen über frühere Verurteilungen vorliegen. Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der

([10]) Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

([11]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

([12]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([13]) niedergelegt wurden. Um insbesondere für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(39) Um einheitliche Bedingungen für die Einrichtung und das Betriebsmanagement des ECRIS-TCN zu gewährleisten, sollten der Kommission Durchführungsbefugnisse übertragen werden. Diese Befugnisse sollten gemäß der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ausgeübt werden ([14]).

(40) Die Mitgliedstaaten sollten die erforderlichen Maßnahmen treffen, um dieser Verordnung so bald wie möglich nachzukommen, damit das ordnungsgemäße Funktionieren des ECRIS-TCN gewährleistet ist, und dabei der Zeit Rechnung tragen, die eu-LISA für die Entwicklung und Umsetzung des ECRIS-TCN benötigt. Die Mitgliedstaaten sollten jedoch nach Inkrafttreten dieser Verordnung mindestens 36 Monate Zeit haben, um Maßnahmen zur Einhaltung dieser Verordnung zu treffen.

(41) Da das Ziel dieser Verordnung, nämlich die Ermöglichung eines raschen und effizienten Austauschs von richtigen Strafregisterinformationen zu Drittstaatsangehörigen, auf Ebene der Mitgliedstaaten nicht ausreichend verwirklicht werden kann sondern vielmehr durch die Einführung gemeinsamer Vorschriften auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das zur Verwirklichung dieses Ziels erforderliche Maß hinaus.

(42) Nach den Artikeln 1 und 2 des dem EUV und dem AEUV beigefügten Protokolls Nr. 22 über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Verordnung und ist weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet.

(43) Nach den Artikeln 1 und 2 sowie Artikel 4a Absatz 1 des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts und unbeschadet des Artikels 4 dieses Protokolls beteiligt sich Irland nicht an der Annahme dieser Verordnung und ist weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet.

(44) Nach Artikel 3 und Artikel 4a Absatz 1 des Protokolls Nr. 21 hat das Vereinigte Königreich mitgeteilt, dass es sich an der Annahme und Anwendung dieser Verordnung beteiligen möchte.

(45) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates ([15]) gehört und hat am 12. Dezember 2017 ([16]) eine Stellungnahme abgegeben —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand

Mit dieser Verordnung

a) wird ein System zur Ermittlung der Mitgliedstaaten eingerichtet, in denen Informationen zu früheren Verurteilungen von Drittstaatsangehörigen vorliegen („ECRIS-TCN“);

b) wird festgelegt, unter welchen Bedingungen die Zentralbehörden das ECRIS-TCN zu verwenden haben, um Informationen zu solchen früheren Verurteilungen über das mit dem Beschluss 2009/316/JI eingerichtete Europäische Strafregisterinformationssystem (ECRIS) zu erhalten, und unter welchen Bedingungen Eurojust, Europol und die EUStA das ECRIS-TCN zu verwenden haben.

([13]) ABl. L 123 vom 12.5.2016, S. 1.
([14]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).
([15]) Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).
([16]) ABl. C 55 vom 14.2.2018, S. 4.

Artikel 2

Anwendungsbereich

Diese Verordnung gilt für die Verarbeitung von Informationen zu der Person eines in Mitgliedstaaten verurteilten Drittstaatsangehörigen zum Zweck der Feststellung, in welchen Mitgliedstaaten solche Verurteilungen erfolgt sind. Mit Ausnahme von Artikel 5 Absatz 1 Buchstabe b Ziffer ii finden die für Drittstaatsangehörige geltenden Bestimmungen dieser Verordnung auch auf Unionsbürger Anwendung, die auch die Staatsangehörigkeit eines Drittstaats haben und in den Mitgliedstaaten verurteilt worden sind.

Artikel 3

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Verurteilung“ jede rechtskräftige Entscheidung eines Strafgerichts gegen eine natürliche Person im Zusammenhang mit einer Straftat, sofern diese Entscheidung in das Strafregister des Urteilsmitgliedstaats eingetragen wird;

2. „Strafverfahren“ die Phase vor dem Strafverfahren, das Strafverfahren und die Strafvollstreckung;

3. „Strafregister“ das nationale oder die nationalen Register, in das bzw. die Verurteilungen nach Maßgabe des nationalen Rechts eingetragen werden;

4. „Urteilsmitgliedstaat“ den Mitgliedstaat, in dem ein Verurteilung erfolgt ist;

5. „Zentralbehörde“ eine gemäß Artikel 3 Absatz 1 des Rahmenbeschlusses 2009/315/JI des Rates benannte Behörde;

6. „zuständige Behörden“ die Zentralbehörden und Eurojust, Europol und die EUStA, die gemäß der vorliegenden Verordnung Zugang zum ECRIS-TCN haben und dieses System abfragen dürfen;

7. „Drittstaatsangehöriger“ eine Person, die kein Bürger der Union im Sinne des Artikels 20 Absatz 1 AEUV ist, oder eine staatenlose Person oder eine Person, deren Staatsangehörigkeit nicht bekannt ist;

8. „Zentralsystem“ die von eu-LISA entwickelte(n) und gewartete(n) Datenbank(en), in der/denen Identitätsangaben zu den in den Mitgliedstaaten verurteilten Drittstaatsangehörigen gespeichert werden;

9. „Schnittstellensoftware“ die Software der zuständigen Behörden, mittels deren sie über die Kommunikationsinfrastruktur nach Artikel 4 Absatz 1 Buchstabe d Zugang zum Zentralsystem erhalten;

10. „Identitätsangaben“ alphanumerische Daten, Fingerabdruckdaten und Gesichtsbilder, die verwendet werden, um eine Verbindung zwischen diesen Daten und einer natürlichen Person herzustellen;

11. „alphanumerische Daten“ Daten in Form von Buchstaben, Ziffern, Sonderzeichen, Leerzeichen und Satzzeichen;

12. „Fingerabdruckdaten“ die Daten zu den flachen und abgerollten Abdrücken aller Finger einer Person;

13. „Gesichtsbild“ ein digitales Bild des Gesichts einer Person;

14. „Treffer“ eine oder mehrere festgestellte Übereinstimmungen zwischen den im Zentralsystem gespeicherten Identitätsangaben und den für eine Suche verwendeten Identitätsangaben;

15. „zentrale nationale Zugangsstelle“ den nationalen Zugangspunkt zur Kommunikationsinfrastruktur nach Artikel 4 Absatz 1 Buchstabe d;

16. „ECRIS-Referenzimplementierung“ die Software, die die Kommission entwickelt und den Mitgliedstaaten für den Austausch von Strafregisterinformationen über das ECRIS zur Verfügung stellt.

17. „nationale Aufsichtsbehörde“ eine von einem Mitgliedstaat gemäß den dafür geltenden Datenschutzbestimmungen der Union eingerichtete unabhängige staatliche Stelle;

18. „Aufsichtsbehörden“ der Europäische Datenschutzbeauftragte und die nationalen Aufsichtsbehörden.

Artikel 4

Technische Architektur des ECRIS-TCN

(1) ECRIS-TCN setzt sich zusammen aus:

a) einem Zentralsystem, in dem Identitätsangaben zu verurteilten Drittstaatsangehörigen gespeichert sind;

b) einer nationalen zentralen Zugangsstelle in jedem Mitgliedstaat;

c) einer Schnittstellensoftware, mittels deren die zuständigen Behörden über die zentrale nationale Zugangsstelle und die in Buchstabe d genannte Kommunikationsinfrastruktur Zugang zum Zentralsystem erhalten;

d) einer Kommunikationsinfrastruktur zwischen dem Zentralsystem und den zentralen nationalen Zugangsstellen.

(2) Das Zentralsystem ist an den technischen Betriebsstätten von eu-LISA angesiedelt.

(3) Die Schnittstellensoftware wird in die ECRIS-Referenzimplementierung integriert. Die Mitgliedstaaten verwenden die ECRIS-Referenzimplementierung oder — in den Fällen und unter den Voraussetzungen der Absätze 4 bis 8 — die nationale ECRIS-Implementierungssoftware für Abfragen im ECRIS-TCN sowie für die Übermittlung darauffolgender Ersuchen um Strafregisterinformationen.

(4) Die Mitgliedstaaten, die ihre nationale ECRIS-Implementierungssoftware verwenden, sind dafür verantwortlich, ihre nationale ECRIS-Implementierungssoftware so zu gestalten, dass die nationalen Strafregisterbehörden das ECRIS-TCN, mit Ausnahme der Schnittstellensoftware, nach Maßgabe dieser Verordnung nutzen können. Zu diesem Zweck gewährleisten sie vor dem Zeitpunkt der Aufnahme des Betriebs des ECRIS-TCN gemäß Artikel 35 Absatz 4, dass ihre nationale ECRIS-Implementierungssoftware gemäß den Protokollen und technischen Spezifikationen funktioniert, die mit den in Artikel 10 genannten Durchführungsrechtsakten festgelegt werden, sowie gemäß allen weiteren auf diesen Durchführungsrechtsakten beruhenden technischen Vorschriften, die von eu-LISA gemäß dieser Verordnung festgelegt werden.

(5) Solange die Mitgliedstaaten, die ihre nationale ECRIS-Implementierungssoftware verwenden, die ECRIS-Referenzimplementierung nicht verwenden, stellen sie zudem sicher, dass alle späteren technischen Anpassungen ihrer nationalen ECRIS-Implementierungssoftware, die infolge etwaiger Änderungen der technischen Anforderungen erforderlich sind, die mit den in Artikel 10 genannten Durchführungsrechtsakten festgelegt werden, oder die infolge von Änderungen aller weiteren, auf diesen Rechtsakten beruhenden technischen Anforderungen von eu-LISA gemäß dieser Verordnung beschlossen werden, unverzüglich implementiert werden.

(6) Die Mitgliedstaaten, die ihre nationale ECRIS-Implementierungssoftware verwenden, tragen alle Kosten im Zusammenhang mit der Implementierung, Wartung und Weiterentwicklung ihrer nationalen ECRIS-Implementierungssoftware und deren Verbindung zum ECRIS-TCN, mit Ausnahme der Schnittstellensoftware.

(7) Ist ein Mitgliedstaat, der seine nationale ECRIS-Implementierungssoftware verwendet, nicht in der Lage, seine Verpflichtungen nach diesem Artikel zu erfüllen, so ist er verpflichtet, zur Nutzung des ECRIS-TCN die ECRIS-Referenzimplementierung einschließlich der integrierten Schnittstellensoftware zu verwenden.

(8) Für die Zwecke der von der Kommission nach Artikel 36 Absatz 10 Buchstabe b durchzuführenden Bewertung stellen die betreffenden Mitgliedstaaten der Kommission alle erforderlichen Informationen bereit.

KAPITEL II

Eingabe und Verwendung von Daten durch Zentralbehörden

Artikel 5

Eingabe von Daten in das ECRIS-TCN

(1) Für jeden verurteilten Drittstaatsangehörigen legt die Zentralbehörde des Urteilsmitgliedstaats einen Datensatz im Zentralsystem an. Der Datensatz enthält folgende Angaben:

a) alphanumerische Daten:

i) einzufügende Informationen, es sei denn, diese Informationen sind der Zentralbehörde im Einzelfall nicht bekannt (obligatorische Informationen):

— Nachname (Familienname);

— Vorname(n);

— Geburtsdatum;

— Geburtsort (Gemeinde und Staat);

— Staatsangehörigkeit(en);

— Geschlecht;

— gegebenenfalls frühere Namen;

— nationale Referenznummer des Urteilsmitgliedstaats;

ii) Informationen, die aufzunehmen sind, wenn sie in das Strafregister eingetragen sind (fakultative Informationen):

— Namen der Eltern;

iii) Informationen, die aufzunehmen sind, wenn sie der Zentralbehörde vorliegen (zusätzliche Informationen):

— Identitätsnummer der Person oder Art und Nummer der Identitätsdokumente der Person sowie Name der ausstellenden Behörde;

— Pseudonyme oder Aliasnamen;

b) Fingerabdruckdaten:

i) Fingerabdrückedruckdaten, die gemäß dem nationalen Recht im Rahmen eines Strafverfahrens abgenommen wurden;

ii) mindestens Fingerabdruckdaten, die nach einem der folgenden Kriterien abgenommen wurden:

— wenn der Drittstaatsangehörige zu einer Freiheitsstrafe von mindestens sechs Monaten verurteilt wurde;

— wenn der Drittstaatsangehörige für eine Straftat verurteilt wurde, die nach dem Recht des Mitgliedstaats mit einer Freiheitsstrafe im Höchstmaß von mindestens zwölf Monaten bedroht ist.

(2) Die Fingerabdruckdaten nach Absatz 1 Buchstabe b dieses Artikels müssen den technischen Spezifikationen an Qualität, Auflösung und Verarbeitung von Fingerabdruckdaten gemäß dem in Artikel 10 Absatz 1 Buchstabe b genannten Durchführungsakt entsprechen. Die Referenznummer der Fingerabdruckdaten der verurteilten Person muss die nationale Referenznummer des Urteilsmitgliedstaats enthalten.

(3) Der Datensatz kann auch Gesichtsbilder des verurteilten Drittstaatsangehörigen enthalten, sofern gemäß dem nationalen Recht des Urteilsmitgliedstaats die Aufnahme und Speicherung von Gesichtsbildern verurteilter Personen zulässig sind.

(4) Nach Erfassung der Verurteilung im Strafregister legt der Urteilsmitgliedstaat den Datensatz soweit möglich automatisch und unverzüglich an.

(5) Die Urteilsmitgliedstaaten legen auch Datensätze zu Verurteilungen an, die vor dem Tag des Beginns der Dateneingabe nach Artikel 35 Absatz 1 erfolgt sind, soweit Daten zu verurteilten Personen in ihren nationalen Datenbanken erfasst werden. In diesen Fällen werden Fingerabdruckdaten nur aufgenommen, wenn sie im Rahmen von Strafverfahren gemäß dem nationalen Recht abgenommen wurden und wenn sie mit anderen Identitätsangaben in Strafregistern eindeutig übereinstimmen.

(6) Um den Anforderungen des Absatzes 1 Buchstabe b Ziffern i und ii und des Absatzes 5 nachzukommen, können die Mitgliedstaaten Fingerabdruckdaten verwenden, die für andere Zwecke als Strafverfahren abgenommen wurden, sofern eine solche Verwendung nach nationalem Recht zulässig ist.

Artikel 6

Gesichtsbilder

(1) Bis zum Inkrafttreten des in Absatz 2 vorgesehenen delegierten Rechtsakts dürfen Gesichtsbilder nur verwendet werden, um die Identität eines Drittstaatsangehörigen, der infolge eines Abgleichs von alphanumerischen Daten oder Fingerabdruckdaten identifiziert wurde, nachzuweisen.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 37 zur Ergänzung dieser Verordnung delegierte Rechtsakte über die Verwendung von Gesichtsbildern zur Identifizierung von Drittstaatsangehörigen zu erlassen, um — sobald das technisch möglich ist — auf der Grundlage dieses biometrischen Identifikators festzustellen, in welchen Mitgliedstaaten Informationen über frühere Verurteilungen dieser Personen vorliegen. Bevor die Kommission diese Befugnis ausübt, bewertet sie unter Berücksichtigung der Notwendigkeit und Verhältnismäßigkeit sowie der technischen Entwicklungen im Bereich der Gesichtserkennungssoftware die Verfügbarkeit und Einsatzfähigkeit der erforderlichen Technik.

Artikel 7

Nutzung des ECRIS-TCN für die Ermittlung der Mitgliedstaaten, in denen Strafregisterinformationen vorliegen

(1) Die Zentralbehörden nutzen das ECRIS-TCN zur Ermittlung der Mitgliedstaaten, in denen Strafregisterinformationen zu einem Drittstaatsangehörigen vorliegen, um über das ECRIS Informationen zu früheren Verurteilungen erhalten zu können, wenn in dem betreffenden Mitgliedstaat entsprechende Informationen zu dieser Person für die Zwecke eines gegen sie gerichteten Strafverfahrens oder für einen der folgenden, nach Maßgabe des nationalen Rechts vorgesehenen und zulässigen Zwecke benötigt werden:

— Überprüfung der eigenen Strafregistereintragungen einer Person auf deren Antrag hin;

— Sicherheitsüberprüfungen;

— Einholung einer Genehmigung oder Lizenz;

— Überprüfung bei Personaleinstellung;

— Überprüfung auf ehrenamtliche Tätigkeiten, bei denen es zu direkten und regelmäßigen Kontakten mit Kindern oder schutzbedürftigen Personen kommt;

— Visa-, Einbürgerungs- und Migrationsverfahren, einschließlich Asylverfahren, und

— Überprüfungen im Zusammenhang mit öffentlichen Aufträgen und öffentlichen Auswahlverfahren.

In besonderen Fällen — außer in den Fällen, in denen ein Drittstaatsangehöriger bei der Zentralbehörde einen Antrag auf Informationen über die ihn betreffenden Strafregistereintragungen stellt, oder wenn der Antrag gestellt wird, um Strafregisterinformationen gemäß Artikel 10 Absatz 2 der Richtlinie 2011/93/EU zu erhalten — kann die Behörde, die Auskunft aus dem Strafregisterbeantragt, jedoch entscheiden, dass eine solche Nutzung des ECRIS-TCN nicht angezeigt ist.

(2) Jeder Mitgliedstaat, der — sofern gemäß und entsprechend dem nationalen Recht vorgesehen — beschließt, das ECRIS-TCN für andere als die in Absatz 1 aufgeführten Zwecke zu nutzen, um über das ECRIS Informationen zu früheren Verurteilungen zu erhalten, teilt der Kommission bis zum Zeitpunkt der Aufnahme des Betriebs gemäß Artikel 35 Absatz 4 oder zu einem späteren Zeitpunkt diese anderen Zwecke sowie jede Änderung dieser Zwecke mit. Die Kommission veröffentlicht solche Mitteilungen im *Amtsblatt der Europäischen Union* innerhalb von 30 Tagen nach dem Eingang der Mitteilungen.

(3) Eurojust, Europol und die EUStA sind berechtigt, gemäß den Artikeln 14 bis 18 das ECRIS-TCN abzufragen, um festzustellen, in welchen Mitgliedstaaten Strafregisterinformationen zu einem Drittstaatsangehörigen vorliegen. Diese Unionseinrichtungen und -agenturen sind allerdings nicht berechtigt, Daten in das ECRIS-TCN einzugeben oder darin enthaltene Daten zu berichtigen oder zu löschen.

(4) Zu den Zwecken der Absätze 1, 2 und 3 können die zuständigen Behörden Abfragen im ECRIS-TCN auch durchführen, um zu überprüfen, ob zu einer Person, die die Unionsbürgerschaft besitzt, in einem Mitgliedstaat Strafregisterinformationen zu dieser Person als Drittstaatsangehörigem vorliegen.

(5) Die zuständigen Behörden dürfen bei der Abfrage des ECRIS-TCN alle oder lediglich einige der in Artikel 5 Absatz 1 genannten Daten verwenden. Der zur Abfrage des Systems erforderliche Mindestdatensatz wird in einem Durchführungsrechtsakt festgelegt, der nach Artikel 10 Absatz 1 Buchstabe g erlassen wird.

(6) Die zuständigen Behörden können Abfragen im ECRIS-TCN auch anhand von Gesichtsbildern durchführen, sofern diese Funktion gemäß Artikel 6 Absatz 2 in das System integriert ist.

(7) Bei einem Treffer stellt das Zentralsystem der zuständigen Behörde automatisch Informationen darüber bereit, in welchen Mitgliedstaaten Strafregisterinformationen zu den betreffenden Drittstaatsangehörigen vorliegen, einschließlich der damit verbundenen nationalen Referenznummern und sämtlicher dazugehörigen Identitätsangaben. Diese Identitätsangaben dürfen nur verwendet werden, um die Identität des betreffenden Drittstaatsangehörigen nachzuweisen. Das Ergebnis einer Abfrage im Zentralsystem darf lediglich für die Zwecke eines Ersuchens nach Artikel 6 des Rahmenbeschlusses 2009/315/JI oder eines Ersuchens nach Artikel 17 Absatz 3 dieser Verordnung genutzt werden.

(8) Wenn es keinen Treffer gibt, wird die zuständige Behörde automatisch vom Zentralsystem informiert.

KAPITEL III

Speicherung und Änderung der Daten

Artikel 8

Speicherfrist

(1) Jeder Datensatz wird so lange im Zentralsystem gespeichert, wie die Daten zu der/den Verurteilung(en) der betreffenden Person in den Strafregistern gespeichert sind.

(2) Nach Ablauf der in Absatz 1 genannten Speicherfrist löscht die Zentralbehörde des Urteilsmitgliedstaats den Datensatz einschließlich aller Fingerabdruckdaten oder Gesichtsbilder aus dem Zentralsystem. Die Löschung erfolgt nach Möglichkeit automatisch und in jedem Fall spätestens einen Monat nach Ablauf der Speicherfrist.

Artikel 9

Änderung und Löschung von Daten

(1) Die Mitgliedstaaten dürfen die Daten, die sie in das ECRIS-TCN eingespeist haben, ändern oder löschen.

(2) Wenn Informationen in den Strafregistern, auf deren Grundlage ein Datensatz nach Artikel 5 angelegt wurde, geändert werden, so führt der Urteilsmitgliedstaat unverzüglich dieselbe Änderung des im Zentralsystem gespeicherten Datensatzes durch.

(3) Hat ein Urteilsmitgliedstaat Grund zu der Annahme, dass die von ihm im Zentralsystem gespeicherten Daten unrichtig sind oder dass bei der Verarbeitung der Daten im Zentralsystem gegen Bestimmungen dieser Verordnung verstoßen wurde, so wird er wie folgt tätig:

a) Er leitet umgehend ein Verfahren zur Überprüfung der Richtigkeit der betreffenden Daten oder gegebenenfalls der Rechtmäßigkeit ihrer Verarbeitung ein;

b) erforderlichenfalls berichtigt er die Daten unverzüglich oder löscht sie unverzüglich aus dem Zentralsystem.

(4) Hat ein anderer Mitgliedstaat als der Urteilsmitgliedstaat, der die Daten eingespeist hat, Grund zu der Annahme, dass die im Zentralsystem gespeicherten Daten unrichtig sind oder dass bei der Verarbeitung der Daten im Zentralsystem gegen Bestimmungen dieser Verordnung verstoßen wurde, so benachrichtigt er unverzüglich die Zentralbehörde des Urteilsmitgliedstaats.

Der Urteilsmitgliedstaat wird wie folgt tätig:

a) Er leitet umgehend ein Verfahren zur Überprüfung der Richtigkeit der betreffenden Daten oder gegebenenfalls der Rechtmäßigkeit ihrer Verarbeitung ein;

b) erforderlichenfalls berichtigt er die Daten unverzüglich oder löscht sie unverzüglich aus dem Zentralsystem;

c) er unterrichtet den anderen Mitgliedstaat unverzüglich über die Berichtigung oder Löschung der Daten oder über die Gründe, weshalb von einer Berichtigung oder Löschung abgesehen wurde.

KAPITEL IV

Entwicklung, Betrieb und Zuständigkeiten

Artikel 10

Erlass von Durchführungsrechtsakten durch die Kommission

(1) Die Kommission erlässt so bald wie möglich die für die technische Entwicklung und Implementierung des ECRIS-TCN erforderlichen Durchführungsrechtsakte, insbesondere Bestimmungen über:

a) die technischen Spezifikationen für die Verarbeitung von alphanumerischen Daten;

b) die technischen Spezifikationen für die Qualität, Auflösung und Verarbeitung von Fingerabdruckdaten;

c) die technischen Spezifikationen für die Schnittstellensoftware;

d) die technischen Spezifikationen für die Qualität, Auflösung und Verarbeitung von Gesichtsbildern für die Zwecke und nach Maßgabe des Artikels 6;

e) die Qualität der Daten, einschließlich eines Mechanismus und Verfahren zur Durchführung von Kontrollen zur Datenqualität;

f) die Dateneingabe gemäß Artikel 5;

g) den Zugang zum ECRIS-TCN und dessen Abfrage gemäß Artikel 7;

h) die Änderung und Löschung von Daten gemäß den Artikeln 8 und 9;

i) das Führen von Protokollen und den Zugang zu diesen gemäß Artikel 31;

j) den Betrieb des Zentralregisters und die für das Zentralregister geltenden Datenschutz- und Sicherheitsvorschriften gemäß Artikel 32;

k) die Erstellung von Statistiken gemäß Artikel 32;

l) die Leistungs- und Verfügbarkeitskriterien des ECRIS-TCN, einschließlich Mindestspezifikationen und -anforderungen an die Verarbeitung und Speicherung biometrischer Daten des ECRIS-TCN insbesondere zu den maximal zulässigen Quoten der falsch positiven Identifizierungen und der falsch negativen Identifizierungen.

(2) Die in Absatz 1 genannten Durchführungsrechtsakte werden nach dem in Artikel 38 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 11

Entwicklung und Betriebsmanagement des ECRIS-TCN

(1) Für die Entwicklung des ECRIS-TCN nach dem Grundsatz des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen ist eu-LISA verantwortlich. Außerdem ist eu-LISA für das Betriebsmanagement des ECRIS-TCN verantwortlich. Die Entwicklung umfasst die Ausarbeitung und Anwendung der technischen Spezifikationen, die Erprobung und die Projektgesamtkoordination.

(2) eu-LISA ist auch für die Weiterentwicklung und Wartung der ECRIS-Referenzimplementierung verantwortlich.

(3) eu-LISA legt das Konzept für die physische Architektur des ECRIS-TCN einschließlich der technischen Spezifikationen und der Weiterentwicklung des Zentralsystems, der zentralen nationalen Zugangsstelle und der Schnittstellensoftware fest. Dieses Konzept wird, vorbehaltlich einer befürwortenden Stellungnahme der Kommission, vom Verwaltungsrat von eu-LISA verabschiedet.

(4) eu-LISA sorgt dafür, dass das ECRIS-TCN so bald wie möglich nach Inkrafttreten dieser Verordnung und nach Erlass der in Artikel 10 genannten Durchführungsrechtsakte durch die Kommission entwickelt und implementiert wird.

(5) Vor der Konzeptions- und Entwicklungsphase des ECRIS-TCN richtet der Verwaltungsrat von eu-LISA einen Programmverwaltungsrat ein, der aus zehn Mitgliedern besteht.

Dem Programmverwaltungsrat gehören acht vom Verwaltungsrat ernannte Mitglieder, der Vorsitzende der Beratergruppe nach Artikel 39 sowie ein von der Kommission ernanntes Mitglied an. Die vom Verwaltungsrat ernannten Mitglieder werden nur aus dem Kreis derjenigen Mitgliedstaaten gewählt, die nach dem Unionsrecht in vollem Umfang durch die für das ECRIS geltenden Rechtsinstrumente gebunden sind und die sich am ECRIS-TCN beteiligen werden. Der Verwaltungsrat sorgt dafür, dass die von ihm ernannten Mitglieder im Programmverwaltungsrat über die notwendige Erfahrung und Fachkompetenz in der Entwicklung und Verwaltung von IT-Systemen zur Unterstützung der Justiz- und Strafregisterbehörden verfügen.

eu-LISA beteiligt sich an den Arbeiten des Programmverwaltungsrats. Zu diesem Zweck nehmen Vertreter von eu-LISA an den Sitzungen des Programmverwaltungsrats teil, um über die Arbeiten an der Konzeption und Entwicklung des ECRIS-TCN und über weitere damit zusammenhängende Arbeiten und Tätigkeiten zu berichten.

Der Programmverwaltungsrat tritt mindestens alle drei Monate zusammen, nötigenfalls auch häufiger. Er gewährleistet die angemessene Verwaltung der Konzeptions- und Entwicklungsphase des ECRIS-TCN sowie die Kohärenz zwischen zentralen und nationalen ECRIS-TCN-Projekten und der nationalen Implementierungssoftware. Der Programmverwaltungsrat erstattet dem Verwaltungsrat von eu-LISA regelmäßig — nach Möglichkeit monatlich — schriftlich Bericht über die Fortschritte des Projekts. Der Programmverwaltungsrat hat keine Entscheidungsbefugnis und kein Mandat zur Vertretung der Mitglieder des Verwaltungsrats.

(6) Der Programmverwaltungsrat legt seine Geschäftsordnung fest, in der insbesondere Folgendes geregelt ist:

a) Vorsitz,

b) Sitzungsorte,

c) Vorbereitung von Sitzungen,

d) Zulassung von Sachverständigen zu den Sitzungen,

e) Kommunikationspläne, durch die gewährleistet ist, dass die nichtteilnehmenden Mitglieder des Verwaltungsrats lückenlos unterrichtet werden.

(7) Den Vorsitz des Programmverwaltungsrats übernimmt ein Mitgliedstaat, der nach dem Unionsrecht in vollem Umfang durch die Rechtsinstrumente gebunden ist, die für das ECRIS und für die Entwicklung, die Errichtung, den Betrieb und die Nutzung aller von eu-LISA verwalteten IT-Großsysteme gelten.

(8) eu-LISA trägt sämtliche Kosten für Reise und Aufenthalt, die den Mitgliedern des Programmverwaltungsrates entstehen. Artikel 10 der Geschäftsordnung von eu-LISA gilt entsprechend. Das Sekretariat des Programmverwaltungsrats wird von eu-LISA gestellt.

(9) Während der Konzeptions- und Entwicklungsphase gehören der Beratergruppe nach Artikel 39 die nationalen ECRIS-TCN- -Projektmanager an, wobei eu-LISA den Vorsitz innehat. Während der Konzeptions- und Entwicklungsphase bis zur Aufnahme des Betriebs des ECRIS-TCN tritt die Gruppe regelmäßig, nach Möglichkeit mindestens einmal im Monat zusammen. Nach jeder Sitzung erstattet sie dem Programmverwaltungsrat Bericht. Sie stellt den technischen Sachverstand zur Unterstützung des Programmverwaltungsrats bei seinen Aufgaben bereit und überwacht den Stand der Vorbereitung in den Mitgliedstaaten.

(10) Um die Vertraulichkeit und Integrität der im ECRIS-TCN gespeicherten Daten jederzeit zu gewährleisten, sorgt eu-LISA in Zusammenarbeit mit den Mitgliedstaaten für geeignete technische und organisatorische Maßnahmen, wobei der Stand der Technik, die Durchführungskosten und die durch die Verarbeitung entstehenden Risiken zu berücksichtigen sind.

(11) eu-LISA ist für folgende Aufgaben im Zusammenhang mit der Kommunikationsinfrastruktur nach Artikel 4 Absatz 1 Buchstabe d zuständig:

a) Überwachung,

b) Sicherheit,

c) Koordinierung der Beziehungen zwischen den Mitgliedstaaten und dem Betreiber der Kommunikationsinfrastruktur.

(12) Für alle sonstigen Aufgaben im Zusammenhang mit der Kommunikationsinfrastruktur gemäß Artikel 4 Absatz 1 Buchstabe d ist die Kommission zuständig, insbesondere für:

a) Aufgaben im Zusammenhang mit dem Haushaltsvollzug,

b) Anschaffung und Erneuerung,

c) vertragliche Fragen.

(13) eu-LISA entwickelt und unterhält einen Mechanismus und Verfahren für die Durchführung von Kontrollen zur Qualität der im ECRIS-TCN gespeicherten Daten und erstattet den Mitgliedstaaten regelmäßig darüber Bericht. eu-LISA erstattet der Kommission regelmäßig Bericht über die aufgetretenen Probleme und die betroffenen Mitgliedstaaten.

(14) Das Betriebsmanagement des ECRIS-TCN umfasst alle Aufgaben, die erforderlich sind, um das ECRIS-TCN nach Maßgabe dieser Verordnung betriebsbereit zu halten; dazu gehören insbesondere die Wartungsarbeiten und technischen Entwicklungen, die erforderlich sind, um sicherzustellen, dass das ECRIS-TCN in Übereinstimmung mit den technischen Spezifikationen mit zufriedenstellender Betriebsqualität funktioniert.

(15) eu-LISA führt Aufgaben im Zusammenhang mit Schulungen zur technischen Nutzung des ECRIS-TCN und der ECRIS-Referenzimplementierung durch.

(16) Unbeschadet des Artikels 17 des Statuts der Beamten der Europäischen Union gemäß der Verordnung (EWG, Euratom, EGKS) Nr. 259/68 [17] wendet eu-LISA angemessene Regeln zur Gewährleistung der beruflichen Schweigepflicht oder einer anderen vergleichbaren Geheimhaltungspflicht auf alle Bediensteten an, die mit im Zentralsystem gespeicherten Daten arbeiten. Diese Pflicht besteht auch nach dem Ausscheiden dieser Bediensteten aus dem Amt oder der Beendigung ihres Dienstverhältnisses oder ihrer Tätigkeit weiter.

Artikel 12

Zuständigkeiten der Mitgliedstaaten

(1) Jeder Mitgliedstaat ist zuständig für:

a) die Gewährleistung einer sicheren Verbindung zwischen seinen nationalen Strafregister- und Fingerabdruckdatenbanken und der zentralen nationalen Zugangsstelle;

b) die Entwicklung, den Betrieb und die Wartung der Verbindung gemäß Buchstabe a;

c) die Gewährleistung einer Verbindung zwischen seinen nationalen Systemen und der ECRIS-Referenzimplementierung;

[17] ABl. L 56 vom 4.3.1968, S. 1.

d) die Verwaltung und die Regelung des Zugangs von dazu ermächtigten Bediensteten der Zentralbehörden zum ECRIS-TCN gemäß dieser Verordnung, sowie die Erstellung und regelmäßige Aktualisierung eines Verzeichnisses der betreffenden Bediensteten und ihres jeweiligen, in Artikel 19 Absatz 3 Buchstabe g genannten Profils.

(2) Jeder Mitgliedstaat stellt den Bediensteten seiner Zentralbehörden, die auf das ECRIS-TCN zugreifen dürfen, angemessene Schulungen insbesondere über die Vorschriften zu Datensicherheit und Datenschutz sowie über die anwendbaren Grundrechte bereit, bevor sie ermächtigt werden, im Zentralsystem gespeicherte Daten zu verarbeiten.

Artikel 13

Verantwortung für die Verwendung von Daten

(1) Gemäß den anwendbaren Datenschutzvorschriften der Union stellt jeder Mitgliedstaat sicher, dass die im ECRIS-TCN erfassten Daten rechtmäßig verarbeitet werden und insbesondere, dass

a) nur dazu ordnungsgemäß ermächtigte Bedienstete zum Zweck der Wahrnehmung ihrer Aufgaben Zugang zu den Daten haben;

b) die Daten rechtmäßig und unter uneingeschränkter Achtung der Menschenwürde und der Grundrechte des Drittstaatsangehörigen erhoben werden;

c) die Daten rechtmäßig in das ECRIS-TCN eingespeist werden;

d) die Daten richtig und aktuell sind, wenn sie in das ECRIS-TCN eingespeist werden.

(2) eu-LISA stellt sicher, dass das ECRIS-TCN gemäß dieser Verordnung, den delegierten Rechtsakten nach Artikel 6 Absatz 2 und den Durchführungsrechtsakten nach Artikel 10 sowie gemäß der Verordnung (EU) 2018/1725 betrieben wird. Insbesondere ergreift eu-LISA unbeschadet der Zuständigkeiten der einzelnen Mitgliedstaaten die nötigen Maßnahmen, um die Sicherheit des Zentralsystems und der Kommunikationsinfrastruktur gemäß Artikel 4 Absatz 1 Buchstabe d zu gewährleisten.

(3) eu-LISA unterrichtet das Europäische Parlament, den Rat und die Kommission sowie den Europäischen Datenschutzbeauftragten so bald wie möglich über die Maßnahmen, die eu-LISA gemäß Absatz 2 für die Aufnahme des Betriebs des ECRIS-TCN ergreift.

(4) Die Kommission stellt den Mitgliedstaaten und der Öffentlichkeit die in Absatz 3 genannten Informationen über eine regelmäßig aktualisierte öffentliche Website zur Verfügung.

Artikel 14

Zugang von Eurojust, Europol und der EUStA

(1) Eurojust hat für die Durchführung des Artikels 17 und für die Erfüllung ihrer in Artikel 2 derVerordnung (EU) 2018/1727 genannten Aufgaben direkten Zugang zum ECRIS-TCN, um ermitteln zu können, in welchen Mitgliedstaaten Informationen zu vorherigen Verurteilungen von Drittstaatsangehörigen vorliegen.

(2) Europol hat für die Erfüllung ihrer in Artikel 4 Absatz 1 Buchstaben a bis e und h der Verordnung (EU) 2016/794 genannten Aufgaben direkten Zugang zum ECRIS-TCN, um ermitteln zu können, in welchen Mitgliedstaaten Informationen zu vorherigen Verurteilungen von Drittstaatsangehörigen vorliegen.

(3) Die EUStA hat für die Erfüllung ihrer in Artikel 4 der Verordnung (EU) 2017/1939 genannten Aufgaben direkten Zugang zum ECRIS-TCN, um ermitteln zu können, in welchen Mitgliedstaaten Informationen zu vorherigen Verurteilungen von Drittstaatsangehörigen vorliegen.

(4) Wenn aus einem Treffer hervorgeht, in welchen Mitgliedstaaten Strafregisterinformationen zu einem Drittstaatsangehörigen vorliegen, können Eurojust, Europol und die EUStA die nationalen Behörden der betreffenden Mitgliedstaaten kontaktieren, um diese um Übermittlung der Strafregisterinformationen gemäß deren jeweiligen Gründungsrechtsakten zu ersuchen.

Artikel 15

Zugang der ermächtigten Bediensteten von Eurojust, Europol und der EUStA

Eurojust, Europol und die EUStA sind zuständig für die Verwaltung und die Regelung des Zugangs von dazu ordnungsgemäß ermächtigten Bediensteten zum ECRIS-TCN gemäß dieser Verordnung und für die Erstellung und regelmäßige Aktualisierung eines Verzeichnisses dieser Bediensteten und ihres jeweiligen Profils.

Artikel 16

Zuständigkeiten von Eurojust, Europol und der EUStA

Eurojust, Europol und die EUStA

a) treffen die technischen Vorkehrungen für eine Verbindung zum ECRIS-TCN und sind für die Aufrechterhaltung dieser Verbindung zuständig;

b) lassen ihren Bediensteten, die auf das ECRIS-TCN zugreifen dürfen, angemessene Schulungen, insbesondere über die Vorschriften über Datensicherheit und Datenschutz sowie die einschlägigen Grundrechte zukommen, bevor diese ermächtigt werden, im Zentralsystem gespeicherte Daten zu verarbeiten;

c) sorgen dafür, dass die von ihnen im Rahmen dieser Verordnung verarbeiteten personenbezogenen Daten gemäß den geltenden Datenschutzbestimmungen geschützt sind.

Artikel 17

Kontaktstelle für Drittstaaten und internationale Organisationen

(1) Drittstaaten und internationale Organisationen können für die Zwecke eines Strafverfahrens Ersuchen um Auskunft darüber, welche Mitgliedstaaten eventuell Strafregisterinformationen über Drittstaatsangehörige haben, an Eurojust richten. Dazu ist das Formblatt im Anhang dieser Verordnung zu verwenden.

(2) Erhält Eurojust ein Ersuchen nach Absatz 1, so ermittelt es mit Hilfe des ECRIS-TCN die Mitgliedstaaten, in denen eventuell Strafregisterinformationen zu dem betreffenden Drittstaatsangehörigen vorliegen.

(3) Gibt es einen Treffer, so fragt Eurojust bei dem Mitgliedstaat, in dem Strafregisterinformationen zu dem betreffenden Drittstaatsangehörigen vorliegen, an, ob dieser zustimmt, dass Eurojust dem Drittstaat oder der internationalen Organisation den Namen des betreffenden Mitgliedstaats mitteilt. Gibt der Mitgliedstaat seine Zustimmung, so teilt Eurojust dem Drittstaat oder der internationalen Organisation den Namen des betreffenden Mitgliedstaats mit und informiert den Drittstaat oder die internationale Organisation darüber, wie ein Ersuchen um Auszüge aus dem Strafregister bei diesem Mitgliedstaat nach Maßgabe der anwendbaren Verfahren eingereicht werden kann.

(4) Gibt es keinen Treffer oder kann Eurojust ein nach diesem Artikel eingereichtes Ersuchen nicht gemäß Absatz 3 beantworten, so teilt Eurojust dem betreffenden Drittstaat oder der betreffenden internationalen Organisation mit, dass es das Verfahren abgeschlossen hat, ohne in irgendeiner Form anzugeben, ob in einem Mitgliedstaat Strafregisterinformationen zu der betreffenden Person vorliegen.

Artikel 18

Übermittlung von Informationen an einen Drittstaat, eine internationale Organisation oder eine private Stelle

Weder Eurojust, noch Europol, noch die EUStA noch eine Zentralbehörde darf Informationen aus dem ECRIS-TCN über einen Drittstaatsangehörigen an einen Drittstaat, eine internationale Organisation oder eine private Stelle weitergeben oder diesen zur Verfügung stellen. Dieser Artikel gilt unbeschadet des Artikels 17 Absatz 3.

Artikel 19

Datensicherheit

(1) Unbeschadet der Zuständigkeiten der einzelnen Mitgliedstaaten ergreift eu-LISA die erforderlichen Maßnahmen, um unter Berücksichtigung der in Absatz 3 genannten Sicherheitsmaßnahmen die Sicherheit des ECRIS-TCN zu gewährleisten.

(2) Für den Betrieb des ECRIS-TCN ergreift eu-LISA die erforderlichen Maßnahmen, um die in Absatz 3 genannten Ziele zu erreichen, einschließlich der Verabschiedung eines Sicherheitsplans sowie eines Notfallplans zur Aufrechterhaltung und eines Notfallplans zur Wiederherstellung des Betriebs, und um zu gewährleisten, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können.

(3) Die Mitgliedstaaten gewährleisten die Datensicherheit vor und während der Übermittlung von Daten an die und während des Empfangs von Daten von der zentralen nationalen Zugangsstelle. Jeder Mitgliedstaat

a) sorgt für den physischen Schutz der Daten, unter anderem durch Aufstellung von Notfallplänen für den Schutz der Infrastruktur;

b) verwehrt Unbefugten den Zugang zu nationalen Einrichtungen, in denen der Mitgliedstaat Tätigkeiten im Zusammenhang mit dem ECRIS-TCN durchführt;

c) verhindert, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden können;

d) verhindert die unbefugte Dateneingabe sowie die unbefugte Kenntnisnahme, Änderung oder Löschung gespeicherter personenbezogener Daten;

e) verhindert die unbefugte Verarbeitung von Daten im ECRIS-TCN und die unbefugte Änderung oder Löschung von Daten, die im ECRIS-TCN verarbeitet werden;

f) stellt sicher, dass die zum Zugang zum ECRIS-TCN berechtigten Personen nur mittels einer persönlichen Benutzerkennung und vertraulicher Zugriffsverfahren und ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können;

g) stellt sicher, dass alle zum Zugang zum ECRIS-TCN berechtigten Behörden Profile mit einer Beschreibung der Aufgaben und Befugnisse der Personen erstellen, die berechtigt sind, die Daten einzugeben, zu berichtigen, zu löschen, abzufragen und zu durchsuchen, und stellt diese Profile den nationalen Aufsichtsbehörden auf deren Anfrage unverzüglich zur Verfügung;

h) stellt sicher, dass überprüft und festgestellt werden kann, welchen Einrichtungen, Stellen und Agenturen der Union personenbezogene Daten unter Verwendung von Einrichtungen zur Datenübertragung übermittelt werden dürfen;

i) stellt sicher, dass überprüft und festgestellt werden kann, welche Daten wann, von wem und zu welchem Zweck im ECRIS-TCN verarbeitet wurden;

j) verhindert das unbefugte Lesen, Kopieren, Ändern oder Löschen von personenbezogenen Daten während der Übermittlung personenbezogener Daten an das oder aus dem ECRIS-TCN oder während des Transports von Datenträgern, insbesondere durch geeignete Verschlüsselungstechniken;

k) überwacht die Wirksamkeit der in diesem Absatz genannten Sicherheitsmaßnahmen und trifft die erforderlichen organisatorischen Maßnahmen zur Eigenkontrolle und zur Kontrolle, um die Einhaltung dieser Verordnung sicherzustellen.

(4) eu-LISA und die Mitgliedstaaten arbeiten zusammen, um für ein kohärentes Vorgehen im Bereich der Datensicherheit zu sorgen, das auf einem das ganze ECRIS-TCN umfassenden Verfahren zum Management von Sicherheitsrisiken beruht.

Artikel 20

Haftung

(1) Jede Person und jeder Mitgliedstaat, der bzw. dem durch eine rechtswidrige Verarbeitung oder durch andere gegen diese Verordnung verstoßende Handlungen ein materieller oder immaterieller Schaden entsteht, hat das Recht, Schadenersatz zu verlangen von

a) dem für den Schaden verantwortlichen Mitgliedstaat oder

b) eu-LISA, wenn eu-Lisa ihren Verpflichtungen gemäß dieser Verordnung oder der Verordnung (EU) 2018/1725 nicht nachgekommen ist.

Der Mitgliedstaat, der für den entstandenen Schaden verantwortlich ist bzw. eu-LISA werden teilweise oder vollständig von ihrer Haftung befreit, wenn sie nachweisen, dass sie für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich sind.

(2) Für Schäden am ECRIS-TCN, die darauf zurückzuführen sind, dass ein Mitgliedstaat, Eurojust, Europol oder die EUStA seinen bzw. ihren Verpflichtungen aus dieser Verordnung nicht nachgekommen ist, haftet der betreffende Mitgliedstaat, Eurojust, Europol bzw. die EUSt, es sei denn und soweit eu-LISA oder ein anderer am ECRIS-TCN beteiligter Mitgliedstaat keine angemessenen Maßnahmen ergriffen hat, um den Schaden abzuwenden oder zu mindern.

(3) Die Geltendmachung von Schadenersatzansprüchen nach den Absätzen 1 und 2 gegen einen Mitgliedstaat unterliegt dem Recht des beklagten Mitgliedstaats. Die Geltendmachung von Schadenersatzansprüchen nach den Absätzen 1 und 2 gegen eu-LISA, Eurojust, Europol oder die EUStA richtet sich nach deren jeweiligen Gründungsrechtsakten.

Artikel 21

Eigenkontrolle

Die Mitgliedstaaten stellen sicher, dass jede Zentralbehörde die erforderlichen Maßnahmen zur Einhaltung der Bestimmungen dieser Verordnung trifft und erforderlichenfalls mit den Aufsichtsbehörden zusammenarbeitet.

Artikel 22

Sanktionen

Jeder Missbrauch der in das ECRIS-TCN eingegebenen Daten wird gemäß einzelstaatlichem Recht oder Unionsrecht mit Sanktionen oder Disziplinarmaßnahmen geahndet, die wirksam, verhältnismäßig und abschreckend sind.

KAPITEL V

Datenschutzrechte und Datenschutzaufsicht

Artikel 23

Datenverantwortlicher und Datenverarbeiter

(1) Jede Zentralbehörde gilt für die Verarbeitung personenbezogener Daten durch den Mitgliedstaat dieser Zentralbehörde im Rahmen dieser Verordnung als Datenverantwortlicher im Sinne der anwendbaren Datenschutzvorschriften der Union.

(2) eu-LISA gilt für die von den Mitgliedstaaten in das Zentralsystem eingegebenen personenbezogenen Daten gemäß der Verordnung (EU) 2018/1725 als Datenverarbeiter.

Artikel 24

Zweck der Verarbeitung personenbezogener Daten

(1) Die in das Zentralsystem eingegebenen Daten dürfen nur verarbeitet werden, um festzustellen, in welchen Mitgliedstaaten Strafregisterinformationen zu Drittstaatsangehörigen vorliegen.

(2) Mit Ausnahme der dazu ordnungsgemäß ermächtigten Bediensteten von Eurojust, Europol und der EUStA, die Zugang zum ECRIS-TCN für die Zwecke dieser Verordnung haben, ist der Zugang zum ECRIS-TCN allein den dazu ordnungsgemäß ermächtigten Bediensteten der Zentralbehörden vorbehalten. Der Zugang ist gemäß dem in Absatz 1 genannten Zweck auf das für die Wahrnehmung der Aufgaben erforderliche Maß beschränkt und geht nicht über das hinaus, was für die verfolgten Ziele erforderlich und verhältnismäßig ist.

Artikel 25

Recht auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung

(1) Anträge von Drittstaatsangehörigen im Rahmen des in den geltenden Datenschutzbestimmungen der Union niedergelegten Rechts, Auskunft über personenbezogene Daten, die Berichtigung und Löschung sowie die Einschränkung der Verarbeitung personenbezogener Daten zu verlangen, können an die Zentralbehörde eines beliebigen Mitgliedstaats gerichtet werden.

(2) Wird ein Antrag bei einem anderen als dem Urteilsmitgliedstaat gestellt, so leitet der Mitgliedstaat, bei dem der Antrag gestellt wurde, diesen unverzüglich, jedoch spätestens innerhalb von 10 Arbeitstagen nach Eingang des Antrags an den Urteilsmitgliedstaat weiter. Nach Eingang des Antrags geht der Urteilsmitgliedstaat wie folgt vor:

a) Er leitet umgehend ein Verfahren zur Überprüfung der Richtigkeit der betreffenden Daten und der Rechtmäßigkeit ihrer Verarbeitung im ECRIS-TCN ein und

b) er antwortet unverzüglich dem Mitgliedstaat, der den Antrag weitergeleitet hat.

(3) Wenn im ECRIS-TCN erfasste Daten unrichtig sind oder unrechtmäßig verarbeitet wurden, so berichtigt oder löscht der Urteilsmitgliedstaat die Daten gemäß Artikel 9. Der Urteilsmitgliedstaat oder gegebenenfalls der Mitgliedstaat, an den der Antrag gerichtet wurde, bestätigt der betroffenen Person unverzüglich schriftlich, dass Maßnahmen zur Berichtigung bzw. Löschung der sie betreffenden Daten ergriffen wurden. Ferner unterrichtet der Urteilsmitgliedstaat unverzüglich alle anderen Mitgliedstaaten, die infolge einer Abfrage im ECRIS-TCN Informationen zu Verurteilungen erhalten haben, über die ergriffenen Maßnahmen.

(4) Ist der Urteilsmitgliedstaat nicht der Ansicht, dass die im ECRIS-TCN gespeicherten Daten unrichtig sind oder unrechtmäßig verarbeitet wurden, so erlässt er eine Verwaltungsentscheidung oder eine gerichtliche Entscheidung, in der er der betroffenen Person schriftlich erläutert, warum er nicht zu einer Berichtigung oder Löschung der sie betreffenden Daten bereit ist. Solche Fälle können erforderlichenfalls der nationalen Aufsichtsbehörden gemeldet werden.

(5) Der Mitgliedstaat, der eine Entscheidung gemäß Absatz 4 erlassen hat, teilt der betroffenen Person ferner mit, welche Schritte sie ergreifen kann, wenn sie mit der Erläuterung gemäß Absatz 4 nicht einverstanden ist. Hierzu gehören Angaben darüber, auf welche Weise bei den zuständigen Behörden oder Gerichten dieses Mitgliedstaats Klage erhoben bzw. ein Rechtsbehelf eingelegt werden kann, und darüber, ob gemäß dem Recht dieses Mitgliedstaats eine Unterstützung, unter anderem durch die nationalen Aufsichtsbehörden, vorgesehen ist.

(6) Jeder Antrag nach Absatz 1 muss die zur Identifizierung der betroffenen Person notwendigen Informationen enthalten. Diese Daten werden ausschließlich verwendet, um dem Antragsteller die Wahrnehmung der in Absatz 1 genannten Rechte zu ermöglichen, und anschließend unverzüglich gelöscht.

(7) Findet Absatz 2 Anwendung, so hält die Zentralbehörde, an die der Antrag gerichtet wurde, schriftlich fest, dass ein solcher Antrag gestellt wurde, die Art und Weise seiner Bearbeitung sowie, an welche Behörde der Antrag weitergeleitet wurde. Auf Antrag der nationalen Aufsichtsbehörden stellt die Zentralbehörde diese Aufzeichnung unverzüglich dieser Aufsichtsbehörde zur Verfügung. Die Zentralbehörde und die nationale Aufsichtsbehörde löschen die Aufzeichnung drei Jahre nach ihrer Anfertigung.

Artikel 26

Zusammenarbeit zur Gewährleistung der Datenschutzrechte

(1) Die Zentralbehörden arbeiten zusammen, um die Gewährleistung der in Artikel 25 genannten Rechte sicherzustellen.

(2) Die nationale Aufsichtsbehörde jedes Mitgliedstaats informiert auf Antrag jede betroffene Person darüber, wie sie ihr Recht auf Berichtigung oder Löschung der sie betreffenden Daten gemäß den geltenden Datenschutzvorschriften der Union ausüben kann.

(3) Für die Zwecke dieses Artikels arbeitet die nationale Aufsichtsbehörde des Mitgliedstaats, der die Daten übermittelt hat, sowie die nationale Aufsichtsbehörde des Mitgliedstaats, bei der der Antrag gestellt wurde, zusammen.

Artikel 27

Rechtsbehelfe

Jede Person hat gemäß dem nationalen Recht oder dem Unionsrecht das Recht, eine Beschwerde oder einen Rechtsbehelf im Urteilsmitgliedstaat einzulegen, wenn dieser das in Artikel 25 vorgesehene Recht auf Auskunft über die diese Person betreffenden Daten oder das Recht auf Berichtigung oder Löschung dieser Daten verweigert hat.

Artikel 28

Kontrolle durch die nationalen Aufsichtsbehörden

(1) Jeder Mitgliedstaat stellt sicher, dass die nach den anwendbaren Datenschutzvorschriften der Union benannten nationalen Aufsichtsbehörden die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gemäß Artikel 5 und 6 durch den betreffenden Mitgliedstaat, einschließlich der Übermittlung an das und aus dem ECRIS-TCN, kontrollieren.

(2) Die nationale Aufsichtsbehörde gewährleistet, dass die Datenverarbeitungsvorgänge in den nationalen Strafregister- und Fingerabdruckdatenbanken, die mit dem Datenaustausch zwischen diesen Systemen und dem ECRIS-TCN zusammenhängen, ab dem Tag der Aufnahme des Betriebs des ECRIS-TCN mindestens alle drei Jahre gemäß einschlägigen internationalen Prüfungsnormen überprüft werden.

(3) Die Mitgliedstaaten stellen sicher, dass ihre nationalen Aufsichtsbehörden über ausreichende Ressourcen zur Wahrnehmung der Aufgaben verfügt, die ihnen mit dieser Verordnung übertragen werden.

(4) Jeder Mitgliedstaat erteilt alle von seinen nationalen Aufsichtsbehörden erbetenen Auskünfte, insbesondere zu den Tätigkeiten, die gemäß den Artikeln 12, 13 und 19 durchgeführt wurden. Jeder Mitgliedstaat gewährt seinen nationalen Aufsichtsbehörden Zugang zu seinen Aufzeichnungen nach Artikel 25 Absatz 7 und zu seinen Protokollen gemäß Artikel 31 Absatz 6 und ermöglicht ihnen jederzeit Zutritt zu allen seinen, mit dem ECRIS-TCN in Verbindung stehenden, Räumlichkeiten.

Artikel 29

Kontrolle durch den Europäischen Datenschutzbeauftragten

(1) Der Europäische Datenschutzbeauftragte überwacht, dass die das ECRIS-TCN betreffende Verarbeitung personenbezogener Daten durch eu-LISA nach Maßgabe dieser Verordnung erfolgt.

(2) Der Europäische Datenschutzbeauftragte trägt dafür Sorge, dass die Verarbeitung personenbezogener Daten durch eu-LISA mindestens alle drei Jahre gemäß einschlägigen internationalen Prüfungsnormen überprüft wird. Der Prüfbericht wird dem Europäischen Parlament, dem Rat, der Kommission, eu-LISA, den Aufsichtsbehörden übermittelt. eu-LISA erhält Gelegenheit, vor der Annahme des Berichts eine Stellungnahme abzugeben.

(3) eu-LISA erteilt die vom Europäischen Datenschutzbeauftragten erbetenen Auskünfte, gewährt ihm Zugang zu allen Dokumenten und zu ihren Protokollen nach Artikel 31 und ermöglicht ihm jederzeit Zutritt zu allen ihren Gebäuden.

Artikel 30

Zusammenarbeit zwischen den nationalen Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten

Eine koordinierte Aufsicht des ECRIS-TCN gemäß Artikel 62 der Verordnung (EU) 2018/1725 wird sichergestellt.

Artikel 31

Führen von Protokollen

(1) eu-LISA und die zuständigen Behörden stellen gemäß ihren jeweiligen Zuständigkeiten sicher, dass alle Datenverarbeitungsvorgänge im ECRIS-TCN gemäß Absatz 2 zur Prüfung der Zulässigkeit von Anträgen, zur Überwachung der Datenintegrität und -sicherheit und der Rechtmäßigkeit der Datenverarbeitung sowie zur Eigenkontrolle aufgezeichnet werden.

(2) Das Protokoll enthält folgende Angaben:

a) den Zweck des Antrags auf Zugang zu ECRIS-TCN- Daten;

b) die gemäß Artikel 5 übermittelten Daten;

c) die nationale Referenznummer;

d) das Datum und den genauen Zeitpunkt des Vorgangs;

e) die für die Abfrage verwendeten Daten;

f) die Kennung des Bediensteten, der die Abfrage vorgenommen hat.

(3) Das Protokoll der Abfragen und Offenlegungen muss es ermöglichen, die Rechtmäßigkeit der Vorgänge nachzuvollziehen.

(4) Die Protokolle dürfen nur zur Überwachung der Rechtmäßigkeit der Datenverarbeitung sowie zur Gewährleistung der Datenintegrität und -sicherheit verwendet werden. Für Kontrolle und Bewertung gemäß Artikel 36 dürfen nur Protokollen verwendet werden, die keine personenbezogenen Daten enthalten. Die Protokolle werden durch geeignete Maßnahmen vor unbefugtem Zugriff geschützt und nach drei Jahren gelöscht, sofern sie nicht für bereits eingeleitete Kontrollverfahren benötigt werden.

(5) Auf Antrag stellt eu-LISA die Aufzeichnungen über ihre Datenverarbeitungsvorgänge den Zentralbehörden unverzüglich zur Verfügung.

(6) Die für die Prüfung der Zulässigkeit des Antrags, die Überwachung der Rechtmäßigkeit der Datenverarbeitung und der Datenintegrität und -sicherheit zuständigen nationalen Aufsichtsbehörden haben auf Antrag zur Erfüllung ihrer Aufgaben Zugang zu diesen Protokollen. Auf Antrag stellen die Zentralbehörden die Protokolle über ihre Datenverarbeitungsvorgänge den zuständigen nationalen Aufsichtsbehörden unverzüglich zur Verfügung.

KAPITEL VI

Schlussbestimmungen

Artikel 32

Datenverwendung zur Erstellung von Berichten und Statistiken

(1) Die dazu ordnungsgemäß ermächtigten Bediensteten von eu-LISA, der zuständigen Behörden und der Kommission dürfen auf die im ECRIS-TCN verarbeiteten Daten ausschließlich zur Erstellung von Berichten und Statistiken zugreifen, ohne dass die Identifizierung einzelner Personen möglich ist.

(2) Für die Zwecke des Absatzes 1 sorgt eu-LISA an ihren technischen Standorten für die Einrichtung, die Bereitstellung und Betriebsführung eines Zentralregisters, das die Daten nach Absatz 1 enthält; dieses Register ermöglicht die Erstellung anpassbarer Berichte und Statistiken, ohne dass die Identifizierung einzelner Personen möglich ist. Der Zugang zum Zentralregister erfolgt durch einen gesicherten Zugang mit Zugangskontrollen und spezifischen Nutzerprofilen, die ausschließlich Berichterstattungs- und Statistikzwecken dienen.

(3) Die von eu-LISA zur Überwachung der Funktionsweise des ECRIS-TCN eingeführten Verfahren gemäß Artikel 36 und die ECRIS-Referenzimplementierung schließen die Möglichkeit ein, regelmäßige Statistiken zu Überwachungszwecken zu erstellen.

eu-LISA übermittelt der Kommission jeden Monat Statistiken, die die Erfassung, die Speicherung und den über das ECRIS-TCN und die ECRIS-Referenzimplementierung erfolgten Austausch von Strafregisterinformationen betreffen. eu-LISA gewährleistet, dass eine Identifizierung einzelner Personen auf der Grundlage dieser Statistiken nicht möglich ist. eu-LISA stellt der Kommission auf deren Ersuchen Statistiken zu spezifischen Aspekten der Umsetzung dieser Verordnung zur Verfügung.

(4) Die Mitgliedstaaten stellen eu-LISA die Statistiken zur Verfügung, die diese benötigt, um ihren in diesem Artikel genannten Pflichten nachzukommen. Sie stellen der Kommission Statistiken über die Zahl der verurteilten Drittstaatsangehörigen und über die Zahl der in ihrem Hoheitsgebiet erfolgten Verurteilungen von Drittstaatsangehörigen zur Verfügung.

Artikel 33

Kosten

(1) Die Kosten im Zusammenhang mit der Einrichtung und dem Betrieb des Zentralsystems, der Kommunikationsinfrastruktur gemäß Artikel 4 Absatz 1 Buchstabe d, der Schnittstellensoftware und der ECRIS-Referenzimplementierung werden vom Gesamthaushaltsplans der Union getragen.

(2) Die jeweiligen Kosten der Anbindung von Eurojust, Europol und der EUStA an das ECRIS-TCN gehen zulasten ihrer jeweiligen Haushalte.

(3) Sonstige Kosten, insbesondere die Kosten der Anbindung der bestehenden nationalen Strafregister, der Fingerabdruckdatenbanken und der Zentralbehörden an das ECRIS-TCN sowie die Kosten der Betriebsführung der ECRIS-Referenzimplementierung gehen zulasten der Mitgliedstaaten.

Artikel 34

Mitteilungen

(1) Jeder Mitgliedstaat teilt eu-LISA seine Zentralbehörde oder -behörden mit, die berechtigt ist bzw. sind, Daten einzugeben, zu berichtigen, zu löschen, abzufragen oder zu durchsuchen; zudem teilt er ihr gegebenenfalls Änderungen daran mit.

(2) eu-LISA sorgt dafür, dass sowohl im *Amtsblatt der Europäischen Union* als auch auf ihrer Webseite eine Liste der von den Mitgliedstaaten gemeldeten Zentralbehörden veröffentlicht wird. eu-LISA aktualisiert die Liste unverzüglich, sobald ihr ein Mitgliedstaat eine Veränderung bei seiner Zentralbehörde meldet.

Artikel 35

Eingabe von Daten und Aufnahme des Betriebs

(1) Sobald sich die Kommission vergewissert hat, dass die folgenden Voraussetzungen erfüllt sind, bestimmt sie den Tag, ab dem die Mitgliedstaaten mit der Eingabe der Daten nach Artikel 5 in das ECRIS-TCN beginnen:

a) Die einschlägigen Durchführungsakte nach Artikel 10 sind angenommen worden;

b) die Mitgliedstaaten haben die technischen und rechtlichen Vorkehrungen zur Erhebung der Daten nach Artikel 5 und zu ihrer Übermittlung an das ECRIS-TCN bestätigt und der Kommission mitgeteilt;

c) eu-Lisa hat in Zusammenarbeit mit den Mitgliedstaaten einen umfassenden Test des ECRIS-TCN unter Verwendung anonymer Testdaten durchgeführt.

(2) Nachdem die Kommission den Tag für den Beginn der Dateneingabe nach Absatz 1 bestimmt hat, teilt sie dieses Datum den Mitgliedstaaten mit. Binnen zweier Monate ab diesem Tag geben die Mitgliedstaaten unter Berücksichtigung von Artikel 41 Absatz 2 die Daten nach Artikel 5 in das ECRIS-TCN ein.

(3) Nach Ablauf der in Absatz 2 genannten Frist führt eu-LISA in Zusammenarbeit mit den Mitgliedstaaten einen abschließenden Test des ECRIS-TCN durch.

(4) Sobald der in Absatz 3 genannte Test erfolgreich abgeschlossen wurde und eu-LISA der Ansicht ist, dass das ECRIS-TCN betriebsbereit ist, teilt sie das der Kommission mit. Die Kommission unterrichtet das Europäische Parlament und den Rat über die Ergebnisse des Tests und legt den Termin für die Inbetriebnahme des ECRIS-TCN fest.

(5) Der Beschluss der Kommission über den Tag der Inbetriebnahme des ECRIS-TCN gemäß Absatz 4 wird im *Amtsblatt der Europäischen Union* veröffentlicht.

(6) Die Mitgliedstaaten beginnen mit der Nutzung des ECRIS-TCN ab dem von der Kommission gemäß Absatz 4 bestimmten Tag.

(7) Bei Fassung der Beschlüsse nach diesem Artikel kann die Kommission unterschiedliche Termine für die Eingabe von alphanumerischen Daten und Fingerabdruckdaten gemäß Artikel 5 in das ECRIS-TCN sowie für die Inbetriebnahme für diese unterschiedlichen Datenkategorien angeben.

Artikel 36

Kontrolle und Bewertung

(1) eu-LISA trägt dafür Sorge, dass Verfahren vorhanden sind, mit denen die Entwicklung des ECRIS-TCN anhand von Zielen für Planung und Kosten, sowie die Funktionsweise des ECRIS-TCN und der ECRIS-Referenzimplementierung anhand von Zielen für die technische Leistung, die Kostenwirksamkeit, die Sicherheit und die Dienstleistungsqualität überwacht werden kann.

(2) Zur Überwachung der Funktionsweise des ECRIS-TCN und seiner technischen Wartung hat eu-LISA Zugang zu den erforderlichen Informationen über die Datenverarbeitungsvorgänge im ECRIS-TCN und in der ECRIS-Referenzimplementierung.

(3) Bis zum 12. Dezember 2019 und danach alle sechs Monate während der Gestaltungs- und Entwicklungsphase übermittelt eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über den Stand der Entwicklung des ECRIS-TCN und der ECRIS-Referenzimplementierung.

(4) Der in Absatz 3 genannte Bericht umfasst einen Überblick über die aktuellen Kosten und den Projektfortschritt, eine Bewertung der finanziellen Auswirkungen sowie Informationen über alle technischen Probleme und Risiken, die sich auf die gemäß Artikel 33 vom Gesamthaushaltsplan der Union zu tragenden Gesamtkosten des ECRIS-TCN auswirken können.

(5) Im Falle wesentlicher Verzögerungen des Entwicklungsprozesses informiert eu-LISA das Europäische Parlament und den Rat so bald wie möglich über die Gründe für diese Verzögerungen sowie über die zeitlichen und finanziellen Auswirkungen.

(6) Sobald die Entwicklung des ECRIS-TCN und der ECRIS-Referenzimplementierung abgeschlossen ist, übermittelt eu-LISA dem Europäischen Parlament und dem Rat einen Bericht, in dem dargelegt wird, wie die Ziele, insbesondere bei Planung und Kosten, erreicht wurden, und in dem etwaige Abweichungen begründet werden.

(7) Im Falle einer technischen Aufrüstung des ECRIS-TCN- s, die mit erheblichen Kosten verbunden sein könnte, unterrichtet eu-LISA das Europäische Parlament und den Rat entsprechend.

(8) Zwei Jahre nach der Inbetriebnahme des ECRIS-TCN und danach jedes Jahr übermittelt eu-LISA der Kommission einen Bericht über die technische Funktionsweise des ECRIS-TCN und der ECRIS-Referenzimplementierung einschließlich ihrer Sicherheit, der insbesondere auf den Statistiken über die Funktionsweise und die Nutzung des ECRIS-TCN für den Austausch von Strafregisterinformationen über die ECRIS-Referenzimplementierung beruht.

(9) Vier Jahre nach der Inbetriebnahme des ECRIS-TCN und danach alle vier Jahre nimmt die Kommission eine Gesamtbewertung des ECRIS-TCN und der ECRIS-Referenzimplementierung vor. In dem auf dieser Grundlage erstellten Gesamtbewertungsbericht wird die Anwendung dieser Verordnung bewertet und werden die erzielten Ergebnisse an den gesetzten Zielen gemessen und die Auswirkungen auf die Grundrechte untersucht. Im Bericht wird auch bewertet, ob die grundlegenden Prinzipien des Betriebs des ECRIS-TCN weiterhin Gültigkeit haben und ob die Verwendung biometrischer Daten für die Zwecke des ECRIS-TCN angemessen ist; ferner werden die Sicherheit des ECRIS-TCN und etwaige sicherheitsrelevante Auswirkungen auf den künftigen Betrieb bewertet. Die Bewertung umfasst erforderlichenfalls Empfehlungen. Die Kommission übermittelt den Bericht dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten und der Agentur der Europäischen Union für Grundrechte.

(10) Bei der ersten Gesamtbewertung nach Absatz 5 wird außerdem auch

a) bewertet, inwieweit laut den einschlägigen statistischen Angaben und weiteren Informationen der Mitgliedstaaten die Aufnahme von Identitätsangaben von Unionsbürgern, die auch die Staatsangehörigkeit eines Drittstaats besitzen, in das ECRIS-TCN zur Verwirklichung der Ziele dieser Verordnung beigetragen hat;

b) überprüft, ob es für einige Mitgliedstaaten möglich ist, weiterhin die nationale ECRIS-Implementierungssoftware nach Artikel 4 zu verwenden;

c) die Aufnahme von Fingerabdruckdaten in das ECRIS-TCN, insbesondere die Anwendung der Mindestkriterien gemäß Artikel 5 Absatz 1 Buchstabe b Ziffer ii bewertet;

d) die Auswirkung des ECRIS und des ECRIS-TCN auf den Schutz personenbezogener Daten bewertet.

Der Bewertung können erforderlichenfalls Gesetzgebungsvorschläge beigefügt werden. Bei anschließenden Gesamtbewertungen können einer oder alle Aspekte bewertet werden.

(11) Die Mitgliedstaaten, Eurojust, Europol und die EUStA stellen eu-LISA und der Kommission die Informationen zur Verfügung, die für die Ausarbeitung der in den Absätzen 3, 8 und 9 genannten Berichte entsprechend den von der Kommission und/oder eu-LISA zuvor festgelegten quantitativen Indikatoren erforderlich sind. Diese Informationen dürfen nicht zu einer Störung der Arbeitsverfahren führen oder Angaben enthalten, die Rückschlüsse auf Quellen, Bedienstete oder Ermittlungen gestatten.

(12) Gegebenenfalls stellen die Aufsichtsbehörden eu-LISA und der Kommission die Informationen zur Verfügung, die für die Ausarbeitung der in Absatz 9 genannten Berichte entsprechend den von der Kommission und/oder eu-LISA zuvor festgelegten quantitativen Indikatoren erforderlich sind. Diese Informationen dürfen nicht zu einer Störung der Arbeitsverfahren führen oder Angaben enthalten, die Rückschlüsse auf Quellen, Bedienstete oder Ermittlungen gestatten.

(13) eu-LISA stellt der Kommission die Informationen zur Verfügung, die zur Durchführung der in Absatz 9 genannten Gesamtbewertung erforderlich sind.

Artikel 37

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 6 Absatz 2 wird der Kommission auf unbestimmte Zeit ab dem 11. Juni 2019 übertragen.

(3) Die Befugnisübertragung gemäß Artikel 6 Absatz 2 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnis. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen im Einklang mit den in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung enthaltenen Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 6 Absatz 2 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist sowohl das Europäische Parlament als auch der Rat der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 38

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

Gibt der Ausschuss keine Stellungnahme ab, so erlässt die Kommission den Durchführungsrechtsakt nicht, und Artikel 5 Absatz 4 Unterabsatz 3 der Verordnung (EU) Nr. 182/2011 findet Anwendung.

Artikel 39

Beratergruppe

eu-LISA setzt eine Beratergruppe ein, um Fachkenntnisse über das ECRIS-TCN und die ECRIS-Referenzimplementierung insbesondere bei der Vorbereitung ihres Jahresarbeitsprogramms und ihres Jahrestätigkeitsberichts einzuholen. Während der Gestaltungs- und Entwicklungsphase findet Artikel 11 Absatz 9 Anwendung.

Artikel 40

Änderung der Verordnung (EU) 2018/1726

Die Verordnung (EU) 2018/1726 wird wie folgt geändert:

1. Artikel 1 Absatz 4 erhält folgende Fassung:

„(4) Die Agentur ist für die Konzeption, die Entwicklung und das Betriebsmanagement des Einreise-/Ausreisesystems (EES), von DubliNet, des Europäischen Reiseinformations- und -genehmigungssystems (ETIAS), des ECRIS-TCN und der ECRIS-Referenzimplementierung verantwortlich."

2. Folgender Artikel wird eingefügt:

„*Artikel 8a*

Aufgaben im Zusammenhang mit dem ECRIS-TCN und der ECRIS-Referenzimplementierung

Im Zusammenhang mit dem ECRIS-TCN und der ECRIS-Referenzimplementierung nimmt die Agentur die folgenden Aufgaben wahr:

a) die ihr mit der Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates übertragenen Aufgaben (*);

b) Aufgaben im Zusammenhang mit Schulungen zur technischen Nutzung des ECRIS-TCN und der ECRIS-Referenzimplementierung.

(*) Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen vorliegen, sowie zur Ergänzung des Europäischen Strafregisterinformationssystems (ECRIS-TCN) und zur Änderung der Verordnung (EU) 2018/1726 (ABl. L 135 vom 22.5.2019, S. 1)."

3. Artikel 14 Absatz 1 erhält folgende Fassung:

„(1) Die Agentur verfolgt die Entwicklungen in der Forschung, die für das Betriebsmanagement des SIS II, des VIS, des Eurodac, des EES, des ETIAS, des DubliNet, des ECRIS-TCN und anderer IT-Großsysteme im Sinne des Artikels 1 Absatz 5 von Belang sind."

4. Artikel 19 Absatz 1 wird wie folgt geändert:

a) Buchstabe ee erhält folgende Fassung:

„ee) die Berichte über den Stand der Entwicklung des EES nach Artikel 72 Absatz 2 der Verordnung (EU) 2017/2226, über den Stand der Entwicklung des ETIAS nach Artikel 92 Absatz 2 der Verordnung (EU) 2018/1240 und über den Stand der Entwicklung des ECRIS-TCN und der ECRIS-Referenzimplementierung nach Artikel 36 Absatz 3 der Verordnung (EU) 2019/816 anzunehmen;"

b) Buchstabe ff. erhält folgende Fassung:

„ff) die Berichte über die technische Funktionsweise des SIS II nach Artikel 50 Absatz 4 der Verordnung (EG) Nr. 1987/2006 und Artikel 66 Absatz 4 des Beschlusses 2007/533/JI, des VIS nach Artikel 50 Absatz 3 der Verordnung (EG) Nr. 767/2008 und Artikel 17 Absatz 3 des Beschlusses 2008/633/JI, des EES nach Artikel 72 Absatz 4 der Verordnung (EU) 2017/2226 und des ETIAS nach Artikel 92 Absatz 4 der Verordnung (EU) 2018/1240 sowie des ECRIS-TCN und der ECRIS-Referenzimplementierung nach Artikel 36 Absatz 8 der Verordnung (EU) 2019/816 anzunehmen;"

c) Buchstabe hh erhält folgende Fassung:

„hh) zu den Berichten des Europäischen Datenschutzbeauftragten über die Überprüfungen gemäß nach Artikel 45 Absatz 2 der Verordnung (EG) Nr. 1987/2006, Artikel 42 Absatz 2 der Verordnung (EG) Nr. 767/2008, Artikel 31 Absatz 2 der Verordnung (EU) Nr. 603/2013, Artikel 56 Absatz 2 der Verordnung (EU) 2017/2226, Artikel 67 der Verordnung (EU) 2018/1240 und Artikel 29 Absatz 2 der Verordnung (EU) 2019/816 förmliche Stellungnahmen anzunehmen und für geeignete Folgemaßnahmen zu diesen Überprüfungen zu sorgen;“

d) Folgender Buchstabe wird eingefügt:

„lla) der Kommission Statistiken zum ECRIS-TCN und zur ECRIS-Referenzimplementierung gemäß Artikel 32 Absatz 4 Unterabsatz 2 der Verordnung (EU) 2019/816 vorzulegen;“

e) Buchstabe mm erhält folgende Fassung:

„mm) die jährliche Veröffentlichung folgender Auflistungen sicherzustellen: der Liste der zuständigen Behörden, die nach Artikel 31 Absatz 8 der Verordnung (EG) Nr. 1987/2006 und Artikel 46 Absatz 8 des Beschlusses 2007/533/JI berechtigt sind, die im SIS II gespeicherten Daten unmittelbar abzufragen, zusammen mit einer Liste der Stellen der nationalen Systeme des SIS II (N.SIS-II-Stellen) und der SIRENE-Büros nach Artikel 7 Absatz 3 der Verordnung (EG) Nr. 1987/2006 und Artikel 7 Absatz 3 des Beschlusses 2007/533/JI und der Liste der zuständigen Behörden nach Artikel 65 Absatz 2 der Verordnung (EU) 2017/2226, der Liste der zuständigen Behörden nach Artikel 87 Absatz 2 der Verordnung (EU) 2018/1240 und der Liste der Zentralbehörden nach Artikel 34 Absatz 2 der Verordnung (EU) 2019/816;“

5. In Artikel 22 Absatz 4 wird nach dem dritten Unterabsatz folgender Unterabsatz eingefügt:

„Eurojust, Europol und die EUStA können auch an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine Angelegenheit des ECRIS-TCN s, die die Anwendung der Verordnung (EU) 2019/816 betrifft, auf der Tagesordnung steht.“

6. Artikel 24 Absatz 3 Buchstabe p erhält folgende Fassung:

„p) unbeschadet des Artikels 17 des Statuts der Beamten Geheimhaltungsvorschriften festzulegen, um Artikel 17 der Verordnung (EG) Nr. 1987/2006, Artikel 17 des Beschlusses 2007/533/JI, Artikel 26 Absatz 9 der Verordnung (EG) Nr. 767/2008, Artikel 4 Absatz 4 der Verordnung (EU) Nr. 603/2013, Artikel 37 Absatz 4 der Verordnung (EU) 2017/2226, Artikel 74 Absatz 2 der Verordnung (EU) 2018/2140 und Artikel 11 Absatz 16 der Verordnung (EU) 2019/816 nachzukommen;“

7. In Artikel 27 Absatz 1 wird folgender Buchstabe eingefügt:

„(da) die ECRIS-TCN Beratergruppe;“.

Artikel 41

Umsetzung und Übergangsbestimmungen

(1) Die Mitgliedstaaten treffen die erforderlichen Maßnahmen, um dieser Verordnung so bald wie möglich nachzukommen, um das ordnungsgemäße Funktionieren des ECRIS-TCN zu gewährleisten.

(2) Die Zentralbehörden legen für Urteile, die vor dem Tag des Beginns der Dateneingabe gemäß Artikel 35 Absatz 1 ergangen sind, wie folgt individuelle Datensätze im Zentralsystem an:

a) alphanumerische Daten werden bis zum Ablauf der in Artikel 35 Absatz 2 genannten Frist in das Zentralsystem eingegeben;

b) Fingerabdruckdaten werden innerhalb von zwei Jahren nach der Inbetriebnahme gemäß Artikel 35 Absatz 5 in das Zentralsystem eingegeben.

Artikel 42

Inkrafttreten

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß den Verträgen unmittelbar in den Mitgliedstaaten.

Geschehen zu Straßburg am 17. April 2019.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
A. TAJANI	G. CIAMBA

ANHANG

STANDARDFORMBLATT FÜR AUSKUNFTSERSUCHEN GEMÄSS ARTIKEL 17 ABSATZ 1 DER VERORDNUNG (EU) 2019/816 ZUR EINHOLUNG VON INFORMATIONEN DARÜBER, IN WELCHEM MITGLIEDSTAAT EVENTUELL STRAFREGISTERINFORMATIONEN ÜBER EINEN DRITTSTAATSANGEHÖRIGEN VORLIEGEN

Dieses Formblatt ist in allen 24 Amtssprachen der Organe der Union auf der Webseite www.eurojust.europa.eu abrufbar und ist in einer dieser Sprachen an ECRIS-TCN@eurojust.europa.eu zu übersenden.über einen Drittstaatsangehörigen vorliegen

Ersuchender Staat bzw. ersuchende internationale Organisation:

Name des Staates bzw. der internationalen Organisation:
Ersuchende Behörde:
Vertreten durch (*Name der Person*):
Titel:
Anschrift:
Telefonnummer:
E-Mail-Adresse:

Strafverfahren, in dessen Zusammenhang Informationen eingeholt werden:

Nationale Referenznummer:
Zuständige Behörde:
Art der Straftaten, die Gegenstand der Ermittlungen sind (bitte geben Sie den/die maßgeblichen Artikel des Strafgesetzbuchs an):
Sonstige relevante Angaben (z. B. Dringlichkeit des Ersuchens):

Angaben zur Identität der Person, die die Staatsangehörigkeit eines Drittstaats besitzt, zu der Informationen über den Urteilsmitgliedstaat eingeholt werden:

NB: Geben Sie bitte so viele verfügbare Informationen wie möglich an.

Nachname (*Familienname*):
Vorname(n):
Geburtsdatum:
Geburtsort (*Gemeinde und Staat*):
Staatsangehörigkeit(en):
Geschlecht:
(gegebenenfalls) frühere/r Name/n:
Namen der Eltern:
Identitätsnummer:
Art und Nummer des/der Identitätsdokuments/e der Person:
Behörde, die das/die Dokument(e) ausgestellt hat:
Pseudonyme oder Aliasnamen:

Handelt es sich um mehrere Personen, so führen Sie sie bitte einzeln auf.

Mithilfe eines Drop-Down-Menüs können weitere Personen aufgenommen werden.

Ort	
Datum	

(Elektronische) Unterschrift und Stempel:

VERORDNUNG (EU) 2019/817 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 20. Mai 2019

zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION –

gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16 Absatz 2, Artikel 74 und Artikel 77 Absatz 2 Buchstaben a, b, d und e,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

(1) Die Kommission hat in ihrer Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“ vom 6. April 2016 darauf hingewiesen, dass die Datenverwaltungsarchitektur der Union im Bereich der Grenzkontrolle und der Sicherheit verbessert werden muss. Durch die Mitteilung wurde ein Prozess eingeleitet, durch den die Interoperabilität zwischen den EU-Informationssystemen für die Bereiche Sicherheit, Grenzmanagement und Migrationssteuerung hergestellt werden soll, um die strukturellen, die Arbeit der nationalen Behörden behindernden Mängel dieser Systeme zu beheben und sicherzustellen, dass Grenzschutzbeamten, Zollbehörden, Polizeibediensteten und Justizbehörden die erforderlichen Informationen zur Verfügung stehen.

(2) Der Rat hat in seinem Fahrplan zur Verbesserung des Informationsaustauschs und des Informationsmanagements einschließlich von Interoperabilitätslösungen im Bereich Justiz und Inneres vom 6. Juni 2016 verschiedene rechtliche, technische und praktische Probleme auf dem Weg zur Interoperabilität der EU-Informationssysteme aufgezeigt und Lösungen dafür gefordert.

(3) Das Europäische Parlament hat in seiner Entschließung vom 6. Juli 2016 zu den strategischen Prioritäten für das Arbeitsprogramm der Kommission für 2017 ([3]) dazu aufgefordert, Vorschläge für die Verbesserung und Weiterentwicklung von bestehenden EU-Informationssystemen, die Schließung von Informationslücken und Wege hin zur Interoperabilität sowie Vorschläge für einen zwingend vorgeschriebenen Informationsaustausch auf EU-Ebene mit den erforderlichen Datenschutzvorkehrungen vorzulegen.

(4) In seinen Schlussfolgerungen vom 15. Dezember 2016 forderte der Europäische Rat, dass die Arbeiten zur Gewährleistung der Interoperabilität von EU-Informationssystemen und -Datenbanken fortgesetzt werden.

(5) Die hochrangige Expertengruppe für Informationssysteme und Interoperabilität kam in ihrem Abschlussbericht vom 11. Mai 2017 zu dem Schluss, dass es notwendig und technisch möglich ist, auf Lösungen für die Interoperabilität hinzuarbeiten, und dass diese Interoperabilität grundsätzlich sowohl operative Verbesserungen bewirken als auch gemäß den Datenschutzvorschriften umgesetzt werden könnte.

([1]) ABl. C 283 vom 10.8.2018, S. 48.
([2]) Standpunkt des Europäischen Parlaments vom 16. April 2019 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 14. Mai 2019.
([3]) ABl. C 101 vom 16.3.2018, S. 116.

(6) Gemäß ihrer Mitteilung vom 6. April 2016 und mit den Erkenntnissen und Empfehlungen der Expertengruppe für Informationssysteme und Interoperabilität hat die Kommission in ihrer Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion — Siebter Fortschrittsbericht“ vom 16. Mai 2017 ein neues Konzept für die Verwaltung grenz-, sicherheits- und migrationsrelevanter Daten vorgestellt, durch das unter uneingeschränkter Achtung der Grundrechte die Interoperabilität aller EU-Informationssysteme für die Bereiche Sicherheit, Grenzmanagement und Migrationssteuerung gewährleistet wäre.

(7) Der Rat hat die Kommission in seinen Schlussfolgerungen vom 9. Juni 2017 zum weiteren Vorgehen zur Verbesserung des Informationsaustauschs und zur Sicherstellung der Interoperabilität der EU-Informationssysteme aufgefordert, die von der hochrangigen Expertengruppe vorgeschlagenen Lösungen zur Verbesserung der Interoperabilität umzusetzen.

(8) In seinen Schlussfolgerungen vom 23. Juni 2017 hat der Europäische Rat die Notwendigkeit einer besseren Interoperabilität zwischen den Datenbanken betont und die Kommission aufgefordert, so rasch wie möglich Gesetzgebungsvorschläge auf der Grundlage der Vorschläge der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität vorzubereiten.

(9) Um die Effektivität und Effizienz von Kontrollen an den Außengrenzen zu verbessern und um zur Verhinderung und Bekämpfung illegaler Einwanderung und zur Gewährleistung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Union einschließlich der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der inneren Sicherheit im Hoheitsgebiet der Mitgliedstaaten beizutragen, um die Umsetzung der gemeinsamen Visumpolitik zu verbessern, um die Prüfung von Anträgen auf internationalen Schutz zu unterstützen, um zur Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten beizutragen, um die Identifizierung von unbekannten Personen, die sich nicht ausweisen können, oder von nicht identifizierten sterblichen Überresten bei Naturkatastrophen, Unfällen oder terroristischen Anschlägen zu erleichtern, und damit das Vertrauen der Öffentlichkeit in das Migrations- und Asylsystem der Union, die Sicherheitsmaßnahmen der Union und die Fähigkeit der Union zum Schutz der Außengrenzen erhalten bleibt, sollte Interoperabilität zwischen den Informationssystemen der EU — d.h. zwischen dem Einreise-/Ausreisesystem (im Folgenden „EES“), dem Visa-Informationssystem (im Folgenden „VIS“), dem Europäischen Reiseinformations- und -genehmigungssystem (im Folgenden „ETIAS“), Eurodac, dem Schengener Informationssystem (im Folgenden „SIS“) und dem Europäischen Strafregisterinformationssystem für Drittstaatsangehörige (im Folgenden „ECRIS-TCN“) — hergestellt werden, damit diese Informationssysteme der EU und ihre Daten einander ergänzen können, wobei die Grundrechte des Einzelnen, insbesondere das Recht auf Schutz personenbezogener Daten, zu achten sind. Als Interoperabilitätskomponenten sollten zu diesem Zweck ein Europäisches Suchportal (European search portal - ESP), ein gemeinsamer Dienst für den Abgleich biometrischer Daten (biometric matching service — im Folgenden „BMS“), ein gemeinsamer Speicher für Identitätsdaten (common identity repository — im Folgenden „CIR“) und ein Detektor für Mehrfachidentitäten (multiple-identity detector — im Folgenden „MID“) geschaffen werden.

(10) Die EU-Informationssysteme sollten so miteinander verbunden werden, dass sie einander ergänzen, damit die korrekte Identifizierung von Personen, einschließlich unbekannter Personen, die sich nicht ausweisen können, oder nicht identifizierter sterblicher Überreste, vereinfacht und ein Beitrag zur Bekämpfung von Identitätsbetrug geleistet wird, damit die Datenqualitätsanforderungen der verschiedenen EU-Informationssysteme verbessert und harmonisiert werden, damit den Mitgliedstaaten die technische und die operative Umsetzung der EU-Informationssysteme erleichtert wird, damit die für die einzelnen EU-Informationssysteme geltenden Sicherheitsvorkehrungen für die Sicherheit und den Schutz der Daten verschärft werden und damit der Zugang zum EES, zum VIS, zum ETIAS und zu Eurodac zum Zwecke der Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten einheitlich geregelt wird und die Zwecke des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN gefördert werden.

(11) Die Interoperabilitätskomponenten sollten sich auf das EES, das VIS, das ETIAS, Eurodac, das SIS und das ECRIS-TCN erstrecken. Zudem sollten sie sich auf Europol-Daten erstrecken, jedoch nur, soweit es erforderlich ist, um Europol- Daten gleichzeitig zu diesen EU-Informationssystemen abfragen zu können.

(12) Die Interoperabilitätskomponenten sollten die personenbezogenen Daten von Personen verarbeiten, deren personenbezogene Daten in den zugrundeliegenden EU-Informationssystemen und von Europol verarbeitet werden.

(13) Das ESP sollte mit dem Ziel geschaffen werden, den mitgliedstaatlichen Behörden und den Stellen der Union mit technischen Mitteln einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu den EU-Informationssystemen, den Europol-Daten und den Datenbanken der Internationalen kriminalpolizeilichen Organisation (Interpol) nach Maßgabe ihrer Zugangsrechte zu erleichtern, soweit das notwendig ist, um

ihren Aufgaben nachzukommen. Das ESP sollte auch geschaffen werden, um die Ziele des EES, des VIS, des ETIAS, von Eurodac, des SIS, des ECRIS-TCN und der Europol-Daten zu unterstützen. Das ESP sollte die gleichzeitige, parallel erfolgende Abfrage aller einschlägigen EU-Informationssysteme sowie der Europol-Daten und der Interpol-Datenbanken ermöglichen und auf diese Weise als einzige Schnittstelle (im Folgenden „Fenster“) für eine nahtlose, unter vollständiger Wahrung der Zugangskontroll- und Datenschutzanforderungen der zugrundeliegenden Systeme erfolgende Abfrage der erforderlichen Informationen in den verschiedenen Zentralsystemen dienen.

(14) Das ESP sollte so konzipiert werden, dass bei der Abfrage der Interpol-Datenbanken sichergestellt ist, dass die von einem Nutzer des ESP für eine Abfrage eingegebenen Daten nicht mit den Eigentümern der Interpol-Daten geteilt werden. Durch die Konzipierung des ESP sollte auch sichergestellt werden, dass die Interpol-Datenbanken nur gemäß dem anwendbaren Unionsrecht und nationalen Recht abgefragt werden.

(15) Anhand der Interpol-Datenbank für gestohlene und verlorene Reisedokumente (Stolen and Lost Travel Documents, SLTD-Datenbank) können zugangsberechtigte Stellen der Mitgliedstaaten, die für die Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten zuständig sind, einschließlich der Einwanderungs- und Grenzschutzbehörden, die Gültigkeit eines Reisedokuments überprüfen. Das ETIAS fragt die SLTD-Datenbank und die Interpol-Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (TDAWN-Datenbank) im Zusammenhang mit der Prüfung, ob beispielsweise ein Antragsteller auf eine Reisegenehmigung irregulär einzureisen beabsichtigt oder möglicherweise eine Gefahr für die Sicherheit darstellt. Das ESP sollte die Abfrage der Datenbanken SLTD und TDAWN anhand von Identitätsdaten oder Daten Ausreisedokumenten ermöglichen. Die über das ESP erfolgende Übermittlung personenbezogener Daten von der Union an Interpol sollte den Bestimmungen über grenzüberschreitende Datenübermittlungen gemäß Kapitel V der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([4]) oder den nationalen Bestimmungen zur Umsetzung von Kapitel V der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates ([5]) unterliegen. Die spezifischen Vorschriften im Gemeinsamen Standpunkt 2005/69/JI des Rates ([6]) und im Beschluss 2007/533/JI des Rates ([7]) sollten davon unberührt bleiben.

(16) Das ESP sollte so konzipiert und konfiguriert werden, dass nur solche Datenabfragen zugelassen werden, die Daten verwenden, die sich auf Personen oder Reisedokumente beziehen, die in einem EU-Informationssystem, in den Europol-Daten oder in den Interpol-Datenbanken vorhanden sind.

(17) Um den systematischen Rückgriff auf die einschlägigen EU-Informationssysteme zu ermöglichen, sollte das ESP für die Abfrage des CIR, des EES, des VIS, des ETIAS, von Eurodac und des ECRIS-TCN verwendet werden. Gleichwohl sollte eine nationale Verbindung zu den verschiedenen EU-Informationssystemen aufrechterhalten werden, um eine technische Ausweichmöglichkeit zu haben. Das ESP sollte zudem von den Stellen der Union dazu genutzt werden, das zentrale SIS in Übereinstimmung mit ihren jeweiligen Zugangsrechten abzufragen und ihren Aufgaben nachzukommen. Das ESP sollte als zusätzliches, die bestehenden spezifischen Schnittstellen ergänzendes Werkzeug für die Abfrage des zentralen SIS, von Europol-Daten und der Interpol-Datenbanken dienen.

(18) Biometrische Daten wie Fingerabdrücke und Gesichtsbilder sind einmalig und daher für die Personenidentifizierung weit zuverlässiger als alphanumerische Daten. Der gemeinsame BMS sollte als technisches Hilfsmittel für die Verstärkung und Vereinfachung der Funktion der einschlägigen EU-Informationssysteme und der anderen Interoperabilitätskomponenten dienen. Der Hauptzweck des gemeinsamen BMS sollte darin bestehen, die Identifizierung einer in mehreren Datenbanken erfassten Person unter Rückgriff auf eine einzige technologische Komponente (anstatt auf mehrere Komponenten) anhand eines systemübergreifenden Abgleichs ihrer biometrischen Daten zu ermöglichen. Der gemeinsame BMS sollte zur Sicherheit beitragen und finanzielle, wartungstechnische und operative Vorteile bieten. Alle automatischen Systeme zur Identifizierung von Fingerabdrücken einschließlich der derzeit für Eurodac, das VIS und das SIS eingesetzten Systeme arbeiten mit biometrischen Merkmalsdaten (im Folgenden „Templates“), die aus einem Merkmalsauszug konkreter biometrischer Proben generiert werden. Sämtliche biometrischen Templates dieser Art sollten im gemeinsamen BMS an einem einzigen Ort logisch voneinander getrennt nach den Informationssystemen, aus denen sie stammen, zusammengefasst und gespeichert werden, um dadurch den systemübergreifenden Vergleich anhand biometrischer Templates zu vereinfachen und Größenvorteile bei der Entwicklung und Wartung der EU-Zentralsysteme zu ermöglichen.

([4]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

([5]) Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

([6]) Gemeinsamer Standpunkt 2005/69/JI des Rates vom 24. Januar 2005 zum Austausch bestimmter Daten mit Interpol (ABl. L 27 vom 29.1.2005, S. 61).

([7]) Beschluss 2007/533/JI des Rates vom 12. Juni 2007 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems der zweiten Generation (SIS II) (ABl. L 205 vom 7.8.2007, S. 63).

(19) Die im gemeinsamen BMS gespeicherten biometrischen Templates, sollten aus Daten bestehen, die aus einem Merkmalsauszug konkreter biometrischer Proben stammen und die in einer Weise generiert werden, dass eine Umkehr des Auszugsprozesses nicht möglich ist. Biometrische Templates sollten zwar aus biometrischen Daten generiert werden, aber es sollte nicht möglich sein, dieselben biometrischen Daten aus biometrischen Templates zu erhalten. Da Daten in Form von Handballenabdrücken und DNA-Profile nur im SIS gespeichert werden und gemäß den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit nicht zum Abgleich mit Daten in anderen Informationssystemen genutzt werden können, sollten im gemeinsamen BMS keine DNA-Profile oder biometrische Templates gespeichert werden, die aus Daten in Form von Handballenabdrücken generiert wurden.

(20) Bei biometrischen Daten handelt es sich um sensible personenbezogene Daten. Mit dieser Verordnung sollten die Grundlagen und die Garantien für die Verarbeitung derartiger Daten für die Zwecke einer eindeutigen Identifizierung betroffener Personen festgelegt werden.

(21) Das EES, das VIS, das ETIAS, Eurodac und das ECRIS-TCN erfordern eine genaue Identifizierung der Personen, deren personenbezogene Daten in diesen Systemen erfasst werden. Der CIR sollte daher die korrekte Identifizierung der in diesen Systemen erfassten Personen erleichtern.

(22) Die in diesen EU-Informationssystemen gespeicherten personenbezogenen Daten können sich auf unterschiedliche oder unvollständige Identitäten ein und derselben Person beziehen. Die Mitgliedstaaten verfügen über effiziente Möglichkeiten zur Identifizierung ihrer Staatsangehörigen oder von als dauerhaft in ihrem Hoheitsgebiet wohnhaft gemeldeten Personen. Die Interoperabilität zwischen den EU-Informationssystemen sollte zur korrekten Identifizierung der in diesen Systemen erfassten Personen beitragen. Im CIR sollten jene personenbezogenen Daten von in den Systemen erfassten Personen gespeichert werden, die für eine genauere Identifizierung der Personen erforderlich sind, einschließlich deren Identitäts-, Reisedokumenten- und biometrische Daten — und das unabhängig davon, in welchem System die betreffenden Daten ursprünglich erfasst wurden. Im CIR sollten ausschließlich solche personenbezogenen Daten gespeichert werden, die für eine genaue Identitätsprüfung unbedingt erforderlich sind. Die im CIR erfassten personenbezogenen Daten sollten nicht länger als für die Zwecke der zugrunde liegenden Systeme unbedingt erforderlich gespeichert und entsprechend den Bestimmungen über die logische Trennung dieser Daten automatisch gelöscht werden, wenn die betreffenden Daten in den zugrunde liegenden Systemen gelöscht werden.

(23) Ein neuer Datenverarbeitungsvorgang, der darin besteht, dass derartige Daten anstatt in den einzelnen separaten Systemen im CIR gespeichert werden, ist erforderlich, um eine genauere Identifizierung durch den automatischen Ver- und Abgleich solcher Daten zu ermöglichen. Die Tatsache, dass die Identitäts-, die Reisedokumenten- und die biometrischen Daten im CIR gespeichert werden, sollte die Datenverarbeitung für die Zwecke des EES, des VIS, des ETIAS, von Eurodac oder des ECRIS-TCN in keiner Weise behindern, da der CIR eine neue gemeinsame Komponente dieser zugrunde liegenden Systeme darstellen sollte.

(24) Daher ist es notwendig, im CIR für jede im EES, im VIS, im ETIAS, in Eurodac oder im ECRIS-TCN erfasste Person eine individuelle Datei anzulegen, um die bezweckte korrekte Personenidentifizierung im Schengen-Raum zu ermöglichen und den MID zu unterstützen, durch den zugleich die Identitätsprüfung von Bona-fide-Reisenden vereinfacht und Identitätsbetrug bekämpft werden soll. In der individuellen Datei sollten alle mit einer Person verknüpften Identitätsangaben an einem Ort gespeichert und den ordnungsgemäß ermächtigten Endnutzern zugänglich gemacht werden.

(25) Der CIR sollte auf diese Weise den Zugang von Behörden, die für die Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten zuständig sind, zu jenen EU-Informationssystemen, die nicht ausschließlich für die Zwecke der Verhinderung, Aufdeckung oder Untersuchung schwerer Straftaten errichtet wurden, erleichtern und vereinheitlichen.

(26) Der CIR sollte eine gemeinsame Speichereinheit für Identitäts-, Reisedokumenten- und biometrische Daten von im EES, im VIS, im ETIAS, in Eurodac und im ECRIS-TCN erfassten Personen einschließen. Sie sollte Teil der technischen Architektur dieser Systeme sein und als gemeinsame Komponente von ihnen für die Speicherung und Abfrage der von ihnen verarbeiteten Identitäts-, Reisedokumenten- und biometrischen Daten dienen.

(27) Sämtliche Datensätze im CIR sollten logisch voneinander getrennt werden, indem jeder Datensatz durch eine entsprechende Kennzeichnung automatisch mit dem Namen des zugrunde liegenden Systems, zu dem er gehört, verknüpft wird. Die Zugangskontrollen des CIR sollten nach Maßgabe dieser Kennzeichnungen darüber entscheiden, ob Zugang zu den betreffenden Datensätzen gewährt wird.

(28) Wenn die Polizeibehörde eines Mitgliedstaats eine Person wegen des Fehlens eines Reisedokuments oder eines anderen glaubwürdigen Dokuments zum Nachweis der Identität dieser Person nicht identifizieren kann oder wenn Zweifel an den von dieser Person vorgelegten Identitätsdaten, der Echtheit des Reisedokuments oder der

Identität des Inhabers bestehen oder wenn die Person zu einer Zusammenarbeit nicht in der Lage ist oder sie verweigert, sollte diese Polizeibehörde eine Abfrage im CIR vornehmen können, um die Person zu identifizieren. Für diese Zwecke sollten die Polizeibehörden Fingerabdrücke unter Einsatz von Livescanner-Techniken für Fingerabdrücke abnehmen, vorausgesetzt, dass das Verfahren im Beisein dieser Person eingeleitet wurde. Solche Abfragen im CIR sollten nicht für die Zwecke der Identifizierung Minderjähriger unter zwölf Jahren zulässig sein, es sei denn, das erfolgt zum Wohl des Kindes.

(29) Falls die biometrischen Daten einer Person nicht verwendet werden können oder eine Abfrage anhand dieser Daten nicht erfolgreich ist, sollte die Abfrage mittels Identitätsdaten der Person in Verbindung mit Reisedokumentendaten vorgenommen werden. Falls die Abfrage ergibt, dass im CIR Daten über diese Person gespeichert sind, sollten die mitgliedstaatlichen Behörden Zugriff auf den CIR erhalten, um in die Identitäts- und Reisedokumentendaten dieser Person Einsicht nehmen zu können, ohne dass das CIR in irgendeiner Form anzeigt, aus welchem EU-Informationssystem die Daten stammen.

(30) Die Mitgliedstaaten sollten nationale gesetzgeberische Maßnahmen zur Benennung der zu Identitätsprüfungen unter Rückgriff auf den CIR befugten Behörden und zur Festlegung der Verfahren, Bedingungen und Kriterien für derartige Prüfungen erlassen, die in Übereinstimmung mit dem Grundsatz der Verhältnismäßigkeit erfolgen sollten. Insbesondere sollte durch nationales Recht die Befugnis eingeführt werden, biometrische Daten einer Person in Gegenwart eines Bediensteten dieser Behörden während einer Identitätsprüfung zu erheben.

(31) Durch diese Verordnung sollte zudem eine neue Möglichkeit zur Vereinheitlichung des Zugangs der von den Mitgliedstaaten benannten Behörden, die für die Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten zuständig sind, und von Europol zu im EES, im VIS, im ETIAS oder in Eurodac gespeicherten Daten, die über Identitäts- - oder Reisedokumentendaten hinausgehen, eingeführt werden. Derartige Daten können nämlich im Einzelfall für die Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten benötigt werden, wenn vernünftige Gründe für die Annahme vorliegen, dass deren Abfrage zur Verhinderung, Aufdeckung oder Untersuchung der terroristischen Straftaten oder sonstigen schweren Straftaten beitragen würde, insbesondere, wenn ein Verdacht besteht, dass der Verdächtige, der Täter oder das Opfer einer terroristischen Straftat oder einer sonstigen schweren Straftat eine Person ist, deren Daten im EES, im VIS, im ETIAS und in Eurodac gespeichert sind.

(32) Die Frage eines vollständigen Zugangs zu im EES, im VIS, im ETIAS oder in Eurodac gespeicherten Daten, welche für die Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erforderlich sind und über die im CIR gespeicherten Identitätsdaten und Reisedokumentendaten hinausgehen, sollte weiterhin durch die einschlägigen Rechtsinstrumente geregelt werden. Die benannten Behörden, die für die Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten zuständig sind, und Europol wissen nicht im Voraus, in welchen EU-Informationssystemen Daten zu den Personen, die Gegenstand ihrer Ermittlungen sind, gespeichert sind. Das führt zu Verzögerungen und Ineffizienz. Den von der benannten Behörde ermächtigten Endnutzern sollte daher angezeigt werden, in welchem dieser EU-Informationssysteme die dem Ergebnis einer Abfrage entsprechenden Daten gespeichert sind. Zu diesem Zweck sollte im Anschluss an die automatische Prüfung auf Vorliegen einer Übereinstimmung das betreffende Informationssystem automatisch gekennzeichnet werden (im Folgenden „Übereinstimmungskennzeichnungsfunktion“).

(33) In diesem Zusammenhang sollte ein Treffer im CIR nicht als Grund oder Anlass interpretiert oder verwendet werden, Schlussfolgerungen über eine Person zu ziehen oder Maßnahmen gegen diese zu ergreifen, sondern sollte nur zum Zwecke einer Beantragung des Zugangs zu den zugrunde liegenden EU-Informationssystemen genutzt werden, vorbehaltlich der Bedingungen und Verfahren, die in den entsprechenden Rechtsinstrumenten zur Regelung dieses Zugangs festgelegt wurden. Jeder derartige Zugangsantrag sollte Kapitel VII dieser Verordnung und gegebenenfalls der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 oder der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([8]) unterliegen.

(34) Als allgemeine Regel sollten die benannten Behörden oder Europol in dem Fall, dass eine Übereinstimmungskennzeichnung anzeigt, dass Daten im EES, im VIS, im ETIAS oder in Eurodac gespeichert sind, uneingeschränkten Zugang zu mindestens einem der betreffenden EU-Informationssysteme beantragen. Wenn ein solcher uneingeschränkter Zugang ausnahmsweise nicht beantragt wird, beispielsweise weil die benannten Behörden oder Europol die Daten bereits über andere Mittel erhalten haben oder der Erhalt der Daten nach nationalem Recht nicht mehr zulässig ist, sollte die Begründung dafür, dass kein Zugang beantragt wird, aufgezeichnet werden.

([8]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

(35) In den Protokollen der Datenabfragen im CIR sollte der Zweck der jeweiligen Abfragen aufgeführt werden. Bei Datenabfragen, die nach dem zweistufigen Datenabfrageverfahren erfolgen, sollte in den Protokollen das Aktenzeichen des betreffenden nationalen Untersuchungsdossiers bzw. Falls angegeben werden, um dadurch anzuzeigen, dass die Abfrage zu den Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erfolgte.

(36) Von den benannten Behörden und von Europol vorgenommene Datenabfragen im CIR, die zu dem Zweck erfolgen, eine Antwort in Form einer Übereinstimmungskennzeichnung zu erhalten, in der angezeigt wird, dass die betreffenden Daten im EES, im VIS, im ETIAS oder in Eurodac gespeichert sind, erfordern eine automatische Verarbeitung personenbezogener Daten. Bei einer Übereinstimmungskennzeichnung sollten außer dem Hinweis, dass Daten der betroffenen Person in einem der EU-Informationssysteme gespeichert sind, keine personenbezogenen Daten der betroffenen Person angezeigt werden. Ermächtigte Endnutzer sollten keine die betroffene Person beschwerenden Entscheidungen treffen, die sich allein auf das Vorliegen einer Übereinstimmungskennzeichnung gründen. Der Zugriff des Endnutzers auf eine Übereinstimmungskennzeichnung würde somit einen nur sehr begrenzten Eingriff in das Recht der betroffenen Person auf Schutz ihrer personenbezogenen Daten bedeuten; gleichzeitig würde es den benannten Behörden und Europol aber erlauben, effizientere Anträge auf Zugang zu personenbezogenen Daten zu stellen.

(37) Der MID sollte mit dem Ziel geschaffen werden, das Funktionieren des CIR und die Ziele des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN zu unterstützen. Damit die jeweiligen Ziele dieser EU-Informationssysteme wirksam umgesetzt werden können, ist es erforderlich, dass die Personen, deren personenbezogene Daten in diesen Systemen gespeichert werden, genau identifiziert werden.

(38) Um die Ziele von EU-Informationssystemen besser zu erreichen, sollte es den auf diese Systeme zurückgreifenden Behörden möglich sein, die Identität von Personen, deren Daten in den einzelnen Systemen gespeichert sind, mit hinreichender Zuverlässigkeit zu verifizieren. Bei den in einem gegebenen System gespeicherten Identitätsdaten oder Reisedokumentendaten kann es sich um unbewusst gemachte Falschangaben, unvollständige Angaben oder bewusst gemachte Falschangaben handeln, und mit den bisher bestehenden Möglichkeiten können unbewusst falsche, unvollständige oder bewusst falsche Identitätsdaten und Reisedokumentendaten nicht mittels Vergleich mit in anderen Systemen gespeicherten Daten als solche erkannt werden. Um hier Abhilfe zu schaffen, ist es erforderlich, auf Unionsebene ein technisches Instrument einzuführen, das die genaue Identifizierung von Personen zu diesen Zwecken ermöglicht.

(39) Der MID sollte Verknüpfungen zwischen den in den einzelnen EU-Informationssystemen erfassten Daten herstellen und speichern, damit Mehrfachidentitäten aufgedeckt werden können, um zugleich die Identitätsprüfung von Bona-fide-Reisenden zu vereinfachen und Identitätsbetrug zu bekämpfen. Der MID sollte ausschließlich Verknüpfungen zwischen Daten über Personen enthalten, die in mehr als einem EU-Informationssystem erfasst sind. Die verknüpften Daten sollten strikt auf die Daten begrenzt werden, welche erforderlich sind, um zu verifizieren, ob eine Person in gerechtfertigter oder in ungerechtfertigter Weise mit mehreren Identitäten in unterschiedlichen Systemen erfasst ist, oder um zu überprüfen, ob es sich bei zwei Personen mit ähnlichen Identitätsdaten um ein und dieselbe Person handelt. Die durch das ESP und den gemeinsamen BMS erfolgende Datenverarbeitung zum Zwecke der systemübergreifenden Verknüpfung von individuellen Dateien sollte ein absolutes Mindestmaß nicht überschreiten und zu diesem Zweck auf eine Prüfung auf Mehrfachidentitäten begrenzt werden, welche dann erfolgen sollte, wenn neue Daten in eines der Systeme, die Daten im CIR hinterlegt haben, oder in das SIS aufgenommen werden. Der MID sollte Absicherungen gegen eine mögliche Diskriminierung von Personen mit legalen Mehrfachidentitäten und gegen derartige Personen beschwerende Entscheidungen einschließen.

(40) Diese Verordnung sieht die Einführung neuer Datenverarbeitungsverfahren vor, die die korrekte Identifizierung der betroffenen Personen ermöglichen sollen. Diese Verfahren bedeuten einen Eingriff in die nach den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union geschützten Grundrechte dieser Personen. Da die EU-Informationssysteme nur im Falle einer korrekten Identifizierung der betroffenen Personen wirksam genutzt werden können, ist ein solcher Eingriff aufgrund der Ziele, zu deren Erreichung die einzelnen EU-Informationssysteme errichtet wurden (wirksames Management der Unionsgrenzen, Wahrung der inneren Sicherheit der Union und wirksame Umsetzung der Asyl- und der Visapolitik der Union), gerechtfertigt.

(41) Das ESP und der gemeinsame BMS sollten immer dann, wenn von einer nationalen Behörde oder von einer Stelle der Union neue Datensätze angelegt oder hochgeladen werden, einen Datenabgleich über die im CIR und im SIS erfassten Personen vornehmen. Der Datenabgleich sollte automatisch erfolgen. Um etwaige Verknüpfungen anhand biometrischer Daten aufzudecken, sollten der CIR und das SIS auf den gemeinsamen BMS zurückgreifen. Um etwaige Verknüpfungen anhand alphanumerischer Daten aufzudecken, sollten der CIR und das SIS auf das ESP zurückgreifen. Der CIR und das SIS sollten dazu geeignet sein, die gleichen oder ähnlichen Daten über eine in verschiedenen Systemen erfasste Person zu ermitteln. Werden solche Daten ermittelt, sollte eine Verknüpfung angelegt werden, die anzeigt, dass es sich jeweils um ein und dieselbe Person handelt. Der CIR und das SIS sollten so konfiguriert werden, dass etwaige kleinere Transliterations- oder Buchstabierfehler in einer Weise erkannt werden, dass sie keine nicht gerechtfertigten beschwerenden Maßnahmen für die betreffende Person zur Folge haben.

(42) Die nationale Behörde oder die Stelle der Union, die die Daten in das betreffende EU-Informationssystem eingegeben hat, sollte diese Verknüpfungen bestätigen bzw. entsprechend ändern. Diese nationale Behörde oder Stelle der Union sollte auf die im CIR oder im SIS und im MID gespeicherten Daten für die Zwecke einer manuellen Verifizierung verschiedener Identitäten zugreifen dürfen.

(43) Die manuelle Verifizierung verschiedener Identitäten sollte von der Behörde vorgenommen werden, die die Daten eingegeben bzw. aktualisiert hat, welche zu der Übereinstimmung geführt haben, aufgrund deren eine Verknüpfung zu in einem anderen EU-Informationssystem gespeicherten Daten angelegt wurde. Die für die manuelle Verifizierung von verschiedenen Identitäten zuständige Behörde sollte jeweils prüfen, ob Mehrfachidentitäten vorliegen, die sich in gerechtfertigter Weise oder in ungerechtfertigter Weise auf dieselbe Person beziehen. Eine derartige Prüfung sollte nach Möglichkeit im Beisein der betreffenden Person erfolgen und bei Bedarf unter Anforderung zusätzlicher Präzisierungen oder Auskünfte. Die Prüfung sollte unverzüglich und in Übereinstimmung mit den im Unionsrecht und im nationalen Recht festgelegten Anforderungen an die Genauigkeit von Informationen vorgenommen werden. Besonders an Grenzen werden die beteiligten Personen in ihrer Bewegungsfreiheit beschränkt für die Dauer der Überprüfung, die aus diesem Grunde nicht unbegrenzt dauern sollte. Die Tatsache, dass im MID eine gelbe Verknüpfung angezeigt wird, sollten nicht als solche ein Grund für die Einreiseverweigerung sein, und eine Entscheidung über die Gestattung oder Verweigerung der Einreise sollte ausschließlich auf der Grundlage der anwendbaren Bestimmungen der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates ([9]) getroffen werden.

(44) Für über das SIS generierte Verknüpfungen, die sich auf Ausschreibungen von Personen zum Zwecke der Übergabe- oder Auslieferungshaft, von Vermissten oder Schutzbedürftigen oder von im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesuchten Personen oder auf Personenausschreibungen zum Zwecke der verdeckten Kontrolle, Ermittlungsanfragen oder gezielten Kontrollen beziehen, sollte das SIRENE-Büro des Mitgliedstaats, der die Ausschreibung vorgenommen hat, für die manuelle Verifizierung verschiedener Identitäten zuständig sein. Diese Kategorien von SIS-Ausschreibungen haben einen sensiblen Charakter und sollten daher nicht notwendigerweise gegenüber den Behörden, die die damit verknüpften Daten in einem anderen EU-Informationssystem eingegeben oder aktualisiert haben, offengelegt werden. Durch die Erstellung einer Verknüpfung zu SIS-Daten sollte den nach Maßgabe der Verordnungen des Europäischen Parlaments und des Rates (EU) 2018/1860 ([10]), (EU) 2018/1861 ([11]) und (EU) 2018/1862 ([12]) zu ergreifenden Maßnahmen nicht vorgegriffen werden.

(45) Die Erstellung solcher Verknüpfungen erfordert Transparenz gegenüber den betroffenen Einzelpersonen. Um die Umsetzung der notwendigen Schutzmaßnahmen gemäß dem anwendbaren Datenschutzrecht der Union zu erleichtern, sollten Einzelpersonen, die Gegenstand einer roten Verknüpfung oder einer weißen Verknüpfung nach einer manuellen Verifizierung verschiedener Identitäten sind, unbeschadet der Einschränkungen zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass nationale Ermittlungen nicht beeinträchtigt werden, schriftlich unterrichtet werden. Diese Einzelpersonen sollten eine einmalige Kennnummer erhalten, anhand derer sie die Behörde finden können, an die sie sich zwecks Ausübung ihrer Rechte wenden sollten.

(46) Wird eine gelbe Verknüpfung erstellt, so sollte die Behörde, die für die manuelle Verifizierung verschiedener Identitäten zuständig ist, Zugang zum MID erhalten. Wenn eine rote Verknüpfung besteht, so sollten mitgliedstaatliche Behörden oder Stellen der Union, die Zugang zu mindestens einem im CIR enthaltenen EU-Informationssystem oder zum SIS haben, Zugang zum MID erhalten. Eine rote Verknüpfung sollte anzeigen, dass eine Person in ungerechtfertigter Weise verschiedene Identitäten benutzt oder dass eine Person die Identität eines anderen benutzt.

(47) Besteht eine weiße oder eine grüne Verknüpfung zwischen Daten aus zwei EU-Informationssystemen, so sollten mitgliedstaatliche Behörden und Stellen der Union Zugang zum MID erhalten, wenn die jeweilige Behörde oder Stelle Zugang zu beiden Informationssystemen hat. Ein solcher Zugang sollte zu dem alleinigen Zweck gewährt werden, dieser Behörde oder Stelle zu ermöglichen, potentielle Fälle zu ermitteln, in denen die Daten im MID, CIR und SIS falsch verknüpft oder unter Verstoß gegen diese Verordnung verarbeitet wurden, und Maßnahmen zu ergreifen, um die Situation zu bereinigen und die Verknüpfung zu aktualisieren oder zu löschen.

([9]) Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) ((ABl. L 77 vom 23.3.2016, S. 1).

([10]) Verordnung (EU) 2018/1860 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger (ABl. L 312 vom 7.12.2018, S. 1).

([11]) Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006 (ABl. L 312 vom 7.12.2018, S. 14).

([12]) Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56).

(48) Die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) sollte automatische Datenqualitätskontrollmechanismen und gemeinsame Datenqualitätsindikatoren konzipieren. Ferner sollte eu-LISA dafür verantwortlich sein, Kapazitäten für die zentrale Überwachung der Datenqualität zu entwickeln und regelmäßige Datenanalyseberichte zu erstellen, um eine bessere Kontrolle der Umsetzung der EU-Informationssysteme in den Mitgliedstaaten zu ermöglichen. Die gemeinsamen Datenqualitätsindikatoren sollten Mindestqualitätsstandards für die Datenspeicherung in den EU-Informationssystemen oder in den Interoperabilitätskomponenten einschließen. Ziel dieser Datenqualitätsstandards sollte sein, dass die EU-Informationssysteme und die Interoperabilitätskomponenten die automatische Ermittlung anscheinend falscher oder unstimmiger Dateneinträge ermöglichen und so dem Mitgliedstaat, der die Daten eingegeben hat, die Möglichkeit gegeben wird, die betreffenden Daten zu überprüfen und etwaige erforderliche Abhilfemaßnahmen zu ergreifen.

(49) Die Kommission sollte die von eu-LISA erstellten Qualitätsberichte auswerten und gegebenenfalls entsprechende Empfehlungen an die Mitgliedstaaten richten. Die Mitgliedstaaten sollten dafür verantwortlich sein, einen Aktionsplan aufzustellen, in dem Maßnahmen zur Behebung etwaiger Mängel bei der Datenqualität beschrieben werden, und regelmäßig über dabei erzielte Fortschritte Bericht erstatten.

(50) Das universelle Nachrichtenformat (Universal Message Format — im Folgenden „UMF“) sollte als Standard für den strukturierten grenzübergreifenden Informationsaustausch zwischen Informationssystemen, Behörden und/oder Organisationen im Bereich Justiz und Inneres dienen. Durch das UMF sollten ein gemeinsames Vokabular und logische Strukturen für üblicherweise ausgetauschte Informationen vorgegeben werden, damit die ausgetauschten Inhalte einheitlich und semantisch gleichwertig erstellt und gelesen werden können und somit die Interoperabilität verbessert wird.

(51) Im VIS, im SIS sowie in allen anderen bestehenden oder neuen Modellen für den grenzübergreifenden Informationsaustausch und Informationssystemen im Bereich Justiz und Inneres, die von Mitgliedstaaten entwickelt wurden oder werden, kann die Umsetzung des UMF-Standards in Betracht gezogen werden.

(52) Es sollte ein zentraler Speicher für Berichte und Statistiken (central repository for reporting and statistics — im Folgenden „CRRS“) eingerichtet werden, der die systemübergreifende Erhebung statistischer Daten und die Erstellung von Analyseberichten zu politischen und operativen Zwecken gemäß den anwendbaren Rechtsinstrumenten sowie für die Zwecke der Datenqualität ermöglicht. Der CRRS sollte von eu-LISA konzipiert, umgesetzt und an ihren technischen Standorten eingerichtet werden. Er sollte anonymisierte statistische Daten aus den EU-Informationssystemen, dem CIR, dem MID und dem gemeinsamen BMS enthalten. Die im CRRS enthaltenen Daten sollten keine Identifizierung von Einzelpersonen ermöglichen. Die Daten sollten von eu-LISA automatisch anonymisiert und als solche im CRRS gespeichert werden. Die Anonymisierung sollte automatisch erfolgen, und den Bediensteten von eu-LISA sollte kein direkter Zugang zu den in den EU-Informationssystemen oder in den Interoperabilitätskomponenten gespeicherten personenbezogenen Daten gewährt werden.

(53) Die Verordnung (EU) 2016/679 findet auf die Verarbeitung personenbezogener Daten zum Zwecke der Interoperabilität durch nationale Behörden im Rahmen dieser Verordnung Anwendung, sofern diese Verarbeitung nicht durch benannte Behörden oder zentrale Anlaufstellen der Mitgliedstaaten zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erfolgt.

(54) Wird die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten zum Zwecke der Interoperabilität gemäß der vorliegenden Verordnung von den zuständigen Behörden zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten durchgeführt, so findet die Richtlinie (EU) 2016/680 Anwendung.

(55) Die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder, sofern relevant, die Richtlinie (EU) 2016/680 gelten für jedwede Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, die gemäß der vorliegenden Verordnung erfolgen. Unbeschadet der Gründe für eine Übermittlung nach Kapitel V der Verordnung (EU) 2016/679 oder, sofern relevant, der Richtlinie (EU) 2016/680 sollte das Urteil eines Gerichts oder die Entscheidung einer Verwaltungsbehörde eines Drittlandes, durch die ein für die Verarbeitung Verantwortlicher oder Datenauftragsverarbeiter verpflichtet wird, personenbezogene Daten zu übermitteln oder offenzulegen, nur anerkannt werden oder in irgendeiner Weise durchsetzbar sein, wenn Grundlage eine internationale Übereinkunft ist, die zwischen dem anfordernden Drittland und der Union oder einem Mitgliedstaat in Kraft ist.

(56) Die einschlägigen Datenschutzbestimmungen der Verordnungen (EU) 2017/2226 ([13]), (EG) Nr. 767/2008 ([14]), (EU) 2018/1240 des Europäischen Parlaments und des Rates ([15]) und der Verordnung (EU) 2018/1861 gelten für die Verarbeitung personenbezogener Daten in den von jenen Verordnungen geregelten Systemen.

(57) Die Verordnung (EU) 2018/1725 gilt für die Verarbeitung personenbezogener Daten durch eu-LISA und andere Organe und Einrichtungen der Union bei der Wahrnehmung ihrer Aufgaben gemäß der vorliegenden Verordnung und lässt die Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates ([16]) unberührt, welche ihrerseits für die Verarbeitung personenbezogener Daten durch Europol maßgeblich ist.

(58) Die Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 oder der Richtlinie (EU) 2016/680 sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten überwachen. Der Europäische Datenschutzbeauftragte sollte die Tätigkeiten der Organe und Einrichtungen der Union bei der Verarbeitung personenbezogener Daten überwachen. Der Europäische Datenschutzbeauftragte und die Aufsichtsbehörden sollten bei der Überwachung der Verarbeitung personenbezogener Daten durch Interoperabilitätskomponenten zusammenarbeiten. Damit der Europäische Datenschutzbeauftragte die ihm gemäß dieser Verordnung übertragenen Aufgaben wahrnehmen kann, sind ausreichende Ressourcen, einschließlich personeller und finanzieller Ressourcen, erforderlich.

(59) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates ([17]) angehört und hat am 16. April 2018 eine Stellungnahme ([18]) abgegeben.

(60) Die Artikel-29-Datenschutzgruppe hat am 11. April 2018 eine Stellungnahme abgegeben.

(61) Die Mitgliedstaaten und eu-LISA sollten über Sicherheitspläne verfügen, die die Erfüllung der Sicherheitsanforderungen erleichtern und sie sollten Sicherheitsfragen gemeinsam angehen. Zudem sollte eu-LISA sicherstellen, dass zur Gewährleistung der Datenintegrität im Zusammenhang mit Konzeption, Entwicklung und Betrieb der Interoperabilitätskomponenten fortwährend auf die neuesten technologischen Entwicklungen zurückgegriffen wird. Zu den Pflichten von eu-Lisa in dieser Hinsicht sollte es gehören, die Maßnahmen zu ergreifen, die notwendig sind, um den Zugang von Unbefugten, wie etwa Personal externer Dienstleistungserbringer, zu personenbezogenen Daten zu verhindern, die über die Interoperabilitätskomponenten verarbeitet werden. Bei der Vergabe von Aufträgen für die Erbringung von Dienstleistungen sollten die Mitgliedstaaten und eu-Lisa alle Maßnahmen prüfen, die notwendig sind, um die Einhaltung der Rechts- und Verwaltungsvorschriften im Zusammenhang mit dem Schutz personenbezogener Daten und der Privatsphäre des Einzelnen bzw. dem Schutz wesentlicher Sicherheitsinteressen gemäß der Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates ([19]) und anwendbaren internationalen Übereinkommen sicherzustellen. eu-LISA sollte bei der Entwicklung der Interoperabilitätskomponenten die Grundsätze des eingebauten Datenschutzes und der datenschutzfreundlichen Grundeinstellungen anwenden.

(62) Die Implementierung der in dieser Verordnung vorgesehenen Interoperabilitätskomponenten wird Auswirkungen darauf haben, wie die Kontrollen an den Grenzübergangsstellen durchgeführt werden. Diese Auswirkungen werden das Ergebnis der Anwendung der bestehenden Vorschriften der Verordnung (EU) 2016/399 in Verbindung mit den in der vorliegenden Verordnung vorgesehenen Interoperabilitätsbestimmungen sein.

(63) Aufgrund dieser kombinierten Vorschriftenanwendung sollte das ESP die Hauptanlaufstelle für die in der Verordnung (EU) 2016/399 vorgeschriebene systematische Datenbankabfrage bei Personen an Grenzübergangsstellen bilden. Auch sollten die Identitätsdaten oder Reisedokumentendaten, aufgrund derer im MID eine rote Verknüpfung angezeigt wird, von den Grenzschutzbeamten bei der Prüfung, ob eine Person die in der

([13]) Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011 (ABl. L 327 vom 9.12.2017, S. 20).

([14]) Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (ABl. L 218 vom 13.8.2008, S. 60).

([15]) Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226 (ABl. L 236 vom 19.9.2018, S. 1).

([16]) Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).

([17]) Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

([18]) ABl. C 233 vom 4.7.2018, S. 12.

([19]) Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014 und des Beschlusses Nr. 541/2014/EU sowie zur Aufhebung der Verordnung (EU, Euratom) Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).

Verordnung (EU) 2016/399 festgelegten Einreisebedingungen erfüllt, berücksichtigt werden. Die bloße Tatsache, dass eine rote Verknüpfung angezeigt wird, sollte allerdings nicht als Ablehnungsgrund für die Einreise gelten dürfen, und die in der Verordnung (EU) 2016/399 aufgeführten möglichen Gründe für eine Ablehnung der Einreise sollten daher nicht geändert werden.

(64) Es wäre angebracht, das ausdrücklich im Leitfaden für Grenzschutzbeamte (Schengen-Handbuch) zu präzisieren.

(65) Falls bei der Abfrage des MID über das ESP eine gelbe oder eine rote Verknüpfung angezeigt wird, sollte der Grenzschutzbeamte den CIR und/oder das SIS abfragen, um die vorliegenden Informationen über die der Kontrolle unterzogene Person zu prüfen sowie um von Hand deren Identitätsdaten zu verifizieren und die Farbe der betreffenden Verknüpfung gegebenenfalls entsprechend zu ändern.

(66) Zu statistischen Zwecken und für die Berichterstattung ist es erforderlich, ermächtigten Bediensteten der in der vorliegenden Verordnung genannten zuständigen Behörden, Organe und Stellen der Union Zugang zu bestimmten Daten aus bestimmten Interoperabilitätskomponenten ohne die Möglichkeit einer Identifizierung von Einzelpersonen zu erteilen.

(67) Damit sich die mitgliedstaatlichen Behörden und Stellen der Union an die neuen Anforderungen an die Nutzung des ESP anpassen können, ist es erforderlich, einen Übergangszeitraum vorzusehen. Ebenso sollten, um ein kohärentes und optimales Funktionieren des MID zu ermöglichen, Übergangsmaßnahmen für dessen Inbetriebnahme vorgesehen werden.

(68) Da das Ziel dieser Verordnung, nämlich die Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen des Umfangs und der Wirkungen dieses Vorhabens auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(69) Die verbleibenden Mittel, die nach der Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates ([20]) für intelligente Grenzen vorgesehen sind, sollten gemäß Artikel 5 Absatz 5 Buchstabe b der Verordnung (EU) Nr. 515/2014 neu zugewiesen und auf diese Verordnung übertragen werden, um die Kosten der Entwicklung der Interoperabilitätskomponenten zu decken.

(70) Um bestimmte technische Einzelaspekte dieser Verordnung zu ergänzen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte über folgendes zu erlassen:

— die Verlängerung des Übergangszeitraums für den Einsatz des ESP;

— die Verlängerung des Übergangszeitraums für die Prüfung auf Mehrfachidentitäten durch die ETIAS-Zentralstelle;

— die Verfahren zur Bestimmung der Fälle, in denen die Identitätsdaten als gleich oder ähnlich angesehen werden können;

— die Bestimmungen für den Betrieb des CRRS, einschließlich spezifischer Sicherheitsvorkehrungen für die Verarbeitung personenbezogener Daten und Sicherheitsvorschriften für den Speicher, und

— detaillierte Bestimmungen über den Betrieb des Web-Portals.

Es ist von besonderer Bedeutung, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen in Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([21]) niedergelegt wurden. Um für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(71) Um einheitliche Bedingungen für die Durchführung dieser Verordnung zu gewährleisten, sollten der Kommission Durchführungsbefugnisse übertragen werden, um die Zeitpunkte festzulegen, ab denen das ESP, das gemeinsame BMS, das CIR, das MID und das CRRS ihren Betrieb aufnehmen

([20]) Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 zur Schaffung eines Instruments für die finanzielle Unterstützung für Außengrenzen und Visa im Rahmen des Fonds für die innere Sicherheit und zur Aufhebung der Entscheidung Nr. 574/2007/EG (ABl. L 150 vom 20.5.2014, S. 143).

([21]) ABl. L 123 vom 12.5.2016, S. 1.

(72) Zudem sollten der Kommission Durchführungsbefugnisse zum Erlass detaillierter Bestimmungen über folgende Aspekte übertragen werden: die technischen Einzelheiten der Profile von Nutzern des ESP; die Spezifikationen der technischen Lösung, die die Abfrage von EU-Informationssystemen, Europol-Daten und Interpol-Datenbanken durch das ESP erlaubt, und das Format der Antworten des ESP; die technischen Vorschriften für die Erstellung von Verknüpfungen im MID zwischen Daten aus verschiedenen EU-Informationssystemen; Inhalt und Darstellung des für die Unterrichtung der betroffenen Person zu benutzenden Formulars, wenn eine rote Verknüpfung erstellt wird; die Leistungsanforderungen und Leistungsüberwachung des gemeinsamen BMS; Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie gemeinsame Datenqualitätsindikatoren; die Entwicklung des UMF-Standards; das Verfahren zur Zusammenarbeit im Fall eines Sicherheitsvorfalls; und die Spezifikationen der technischen Lösung für die Mitgliedstaaten, um die Anträge von Nutzern auf Zugang zu verwalten. Diese Befugnisse sollten gemäß der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([22]) ausgeübt werden.

(73) Da die Interoperabilitätskomponenten die Verarbeitung einer erheblichen Menge sensibler personenbezogener Daten umfassen werden, ist es wichtig, dass Personen, deren Daten durch diese Komponenten verarbeitet werden, als Betroffene ihre Rechte gemäß der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2018/1725 wirksam ausüben können. Den betroffenen Personen sollte ein Web-Portal zur Verfügung gestellt werden, das es ihnen erleichtert, ihre Rechte auf Zugang zu ihren personenbezogenen Daten sowie auf deren Berichtigung, Löschung und Einschränkung von deren Verarbeitung auszuüben. eu-LISA sollte dieses Web-Portal einrichten und verwalten.

(74) Einer der wesentlichen Grundsätze des Datenschutzes ist die Datenminimierung: gemäß Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 muss die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Aus diesem Grund sollte bei den Interoperabilitätskomponenten nicht vorgesehen sein, dass neue personenbezogene Daten gespeichert werden, mit Ausnahme der Verknüpfungen, die im MID gespeichert werden und die das notwendige Minimum für die Zwecke dieser Verordnung darstellen.

(75) Diese Verordnung sollte klare Bestimmungen über die Haftung und das Recht auf Schadenersatz für die rechtswidrige Verarbeitung personenbezogener Daten und andere gegen diese Verordnung verstoßende Handlungen beinhalten. Diese Bestimmungen sollten das Recht auf Schadenersatz durch den für die Verarbeitung Verantwortlichen oder den Datenauftragsverarbeiter sowie deren Haftung gemäß der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2018/1725 unberührt lassen. eu-LISA sollte für jeden von ihr in ihrer Eigenschaft als Datenauftragsverarbeiter verursachten Schaden haften, wenn sie den ihr spezifisch in dieser Verordnung auferlegten Pflichten nicht nachgekommen ist oder wenn sie die rechtmäßig erteilten Anweisungen des Mitgliedstaats, der der für die Datenverarbeitung Verantwortliche ist, nicht beachtet oder gegen diese Anweisungen gehandelt hat.

(76) Diese Verordnung berührt nicht die Anwendung der Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates ([23]).

(77) Nach den Artikeln 1 und 2 des dem EUV und dem AEUV beigefügten Protokolls Nr. 22 über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Verordnung und ist weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet. Da diese Verordnung den Schengen-Besitzstand ergänzt, beschließt Dänemark gemäß Artikel 4 des genannten Protokolls innerhalb von sechs Monaten, nachdem der Rat diese Verordnung angenommen hat, ob es sie in nationales Recht umsetzt.

(78) Diese Verordnung stellt eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands dar, an denen sich das Vereinigte Königreich gemäß dem Beschluss 2000/365/EG des Rates ([24]) nicht beteiligt; das Vereinigte Königreich beteiligt sich daher nicht an der Annahme dieser Verordnung und ist weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet.

(79) Diese Verordnung stellt eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands dar, an denen sich Irland gemäß dem Beschluss 2002/192/EG des Rates ([25]) nicht beteiligt; Irland beteiligt sich daher nicht an der Annahme dieser Verordnung und ist weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet.

([22]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

([23]) Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über das Recht der Unionsbürger und ihrer Familienangehörigen, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten, zur Änderung der Verordnung (EWG) Nr. 1612/68 und zur Aufhebung der Richtlinien 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG und 93/96/EWG (ABl. L 158 vom 30.4.2004, S. 77).

([24]) Beschluss 2000/365/EG des Rates vom 29. Mai 2000 zum Antrag des Vereinigten Königreichs Großbritannien und Nordirland, einzelne Bestimmungen des Schengen-Besitzstands auf es anzuwenden (ABl. L 131 vom 1.6.2000, S. 43).

([25]) Beschluss 2002/192/EG des Rates vom 28. Februar 2002 zum Antrag Irlands auf Anwendung einzelner Bestimmungen des Schengen-Besitzstands auf Irland (ABl. L 64 vom 7.3.2002, S. 20).

(80) Für Island und Norwegen stellt diese Verordnung eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands ([26]) dar, die zu dem in Artikel 1 Buchstaben A, B und G des Beschlusses Nr. 1999/437/EG des Rates ([27]) genannten Bereich gehören.

(81) Für die Schweiz stellt diese Verordnung eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands ([28]) dar, die zu dem in Artikel 1 Buchstaben A, B und G des Beschlusses 1999/437/EG in Verbindung mit Artikel 3 des Beschlusses 2008/146/EG des Rates ([29]) genannten Bereich gehören.

(82) Für Liechtenstein stellt diese Verordnung eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands ([30]) dar, die zu dem in Artikel 1 Buchstaben A und B des Beschlusses 1999/437/EG in Verbindung mit Artikel 3 des Beschlusses 2011/350/EU des Rates ([31]) genannten Bereich gehören.

(83) Diese Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden, und sollte unter Wahrung dieser Rechte und Grundsätze angewandt werden.

(84) Damit sich diese Verordnung in den bestehenden Rechtsrahmen einfügt, sollten die Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/18/61 und die Beschlüsse 2004/512/EG des Rates ([32]) und 2008/633/JIdes Rates ([33]) entsprechend geändert werden —

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand

(1) Durch diese Verordnung und die Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates ([34]) wird ein Rahmen für die Sicherstellung der Interoperabilität zwischen dem Einreise-/Ausreisesystem (im Folgenden „EES“), dem Visa-Informationssystem (im Folgenden „VIS“), dem Europäischen Reiseinformations- und -genehmigungssystem (im Folgenden „ETIAS“), Eurodac, dem Schengener Informationssystem (im Folgenden „SIS“) und dem Europäischen Strafregisterinformationssystem für Drittstaatsangehörige (im Folgenden „ECRIS-TCN“) geschaffen.

([26]) ABl. L 176 vom 10.7.1999, S. 36.
([27]) Beschluss 1999/437/EG des Rates vom 17. Mai 1999 zum Erlass bestimmter Durchführungsvorschriften zu dem Übereinkommen zwischen dem Rat der Europäischen Union und der Republik Island und dem Königreich Norwegen über die Assoziierung dieser beiden Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen- Besitzstands (ABl. L 176 vom 10.7.1999, S. 31).
([28]) ABl. L 53 vom 27.2.2008, S. 52.
([29]) Beschluss 2008/146/EG des Rates vom 28. Januar 2008 über den Abschluss — im Namen der Europäischen Gemeinschaft — des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (ABl. L 53 vom 27.2.2008, S. 1).
([30]) ABl. L 160 vom 18.6.2011, S. 21.
([31]) Beschluss 2011/350/EU des Rates vom 7. März 2011 über den Abschluss — im Namen der Europäischen Union — des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zum Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands in Bezug auf die Abschaffung der Kontrollen an den Binnengrenzen und den freien Personenverkehr (ABl. L 160 vom 18.6.2011, S. 19).
([32]) Entscheidung 2004/512/EG des Rates vom 8. Juni 2004 zur Einrichtung des Visa-Informationssystems (VIS) (ABl. L 213 vom 15.6.2004, S. 5).
([33]) Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten (Council Decision 2008/633/JHA of 23 June 2008 concerning access for consultation of the Visa Information System (VIS) by designated authorities of Member States and by Europol for the purposes of the prevention, detection and investigation of terrorist offences and of other serious criminal offences ABl. L 218 vom 13.8.2008, S. 129).
([34]) Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen auf dem Gebiet der polizeilichen und justiziellen Zusammenarbeit, Asyl und Migration und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (siehe Seite 85 dieses Amtsblatts).

(2) Dieser Rahmen umfasst folgende Interoperabilitätskomponenten:

a) Europäisches Suchportal (European search portal im Folgenden „ESP“),

b) gemeinsamer Dienst für den Abgleich biometrischer Daten (biometric matching service — im Folgenden „gemeinsamer BMS“),

c) gemeinsamer Speicher für Identitätsdaten (common identity repository — im Folgenden „CIR“),

d) Detektor für Mehrfachidentitäten (multiple-identity detector — im Folgenden „MID“).

(3) Zudem werden in dieser Verordnung Bestimmungen über die Datenqualitätsanforderungen, ein universelles Nachrichtenformat (Universal Message Format — im Folgenden „UMF“), einen zentralen Speicher für Berichte und Statistiken (central repository for reporting and statistics — im Folgenden „CRRS“) sowie die Verantwortlichkeiten der Mitgliedstaaten und der Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) bei der Konzipierung, der Entwicklung und dem Betrieb der Interoperabilitätskomponenten festgelegt.

(4) Diese Verordnung regelt ferner die Verfahren und Bedingungen für den Zugang der benannten Behörden und der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) zum EES, zum VIS, zum ETIAS und zu Eurodac zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten.

(5) Durch diese Verordnung wird auch ein Rahmen für die Überprüfung der Identitäten von Personen und für die Identifizierung von Personen festgelegt.

Artikel 2

Ziele

(1) Durch die mittels dieser Verordnung sichergestellte Interoperabilität sollen folgende Ziele erreicht werden:

a) Verbesserung der Wirksamkeit und Effizienz der Grenzübertrittskontrollen an den Außengrenzen,

b) Beitrag zur Verhinderung und Bekämpfung illegaler Einwanderung,

c) Gewährleistung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Union einschließlich der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der inneren Sicherheit im Hoheitsgebiet der Mitgliedstaaten,

d) verbesserte Umsetzung der gemeinsamen Visumpolitik,

e) Unterstützung bei der Prüfung von Anträgen auf internationalen Schutz,

f) Beitrag zur Verhinderung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten,

g) Erleichterung der Identifizierung von unbekannten Personen, die sich nicht ausweisen können, oder von nicht identifizierten sterblichen Überresten bei Naturkatastrophen, Unfällen oder terroristischen Anschlägen.

(2) Die Ziele nach Absatz 1 sollen durch folgende Maßnahmen erreicht werden:

a) Sicherstellung der korrekten Identifizierung von Personen,

b) Beitrag zur Bekämpfung von Identitätsbetrug,

c) Verbesserung der Datenqualität und Harmonisierung der Qualitätsanforderungen an die in den EU-Informationssystemen gespeicherten Daten unter Beachtung der Datenverarbeitungsanforderungen gemäß den rechtlichen Regelungen der einzelnen Systeme sowie den Datenschutzstandards und -grundsätzen,

d) Erleichterung und Unterstützung der technischen und der operativen Umsetzung der EU-Informationssysteme durch die Mitgliedstaaten,

e) Verschärfung, Vereinfachung und Vereinheitlichung der für die einzelnen EU-Informationssysteme geltenden Bedingungen für die Sicherheit und den Schutz der Daten, ohne Auswirkungen auf den besonderen Schutz und die Garantien, die für bestimmte Kategorien von Daten vorgesehen sind,

f) Vereinheitlichung der Bedingungen für den Zugang benannter Behörden zum EES, zum VIS, zum ETIAS und zu Eurodac unter Sicherstellung der erforderlichen und verhältnismäßigen Bedingungen für diesen Zugang sowie

g) Unterstützung der Zwecke des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN.

Artikel 3

Anwendungsbereich

(1) Diese Verordnung gilt für das EES, das VIS, das ETIAS und das SIS.

(2) Diese Verordnung gilt für Personen, deren personenbezogene Daten in den in Absatz 1 genannten EU-Informationssystemen verarbeitet werden können und deren Daten für die Zwecke der Artikel 1 und 2 der Verordnung (EG) Nr. 767/2008, des Artikels 1 der Verordnung (EU) 2017/2226, der Artikel 1 und 4 der Verordnung (EU) 2018/1240, des Artikels 1 der Verordnung (EU) 2018/1860 und des Artikels 1 der Verordnung (EU) 2018/1861 erfasst werden.

Artikel 4

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Außengrenzen“ die Außengrenzen im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2016/399;
2. „Grenzübertrittskontrollen“ die Grenzübertrittskontrollen im Sinne des Artikels 2 Nummer 11 der Verordnung (EU) 2016/399;
3. „Grenzschutzbehörde“ die Grenzschutzbeamten, die nach nationalem Recht angewiesen sind, Grenzübertrittskontrollen durchzuführen;
4. „Aufsichtsbehörden“ die Aufsichtsbehörde gemäß Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 und die Aufsichtsbehörde gemäß Artikel 41 Absatz 1 der Richtlinie (EU) 2016/680;
5. „Verifizierung“ den Abgleich von Datensätzen zur Überprüfung einer Identitätsangabe (1:1-Abgleich);
6. „Identifizierung“ die Feststellung der Identität einer Person durch den Abgleich mit vielen Datensätzen in einer Datenbank (1:n-Abgleich);
7. „alphanumerische Daten“ Daten in Form von Buchstaben, Ziffern, Sonderzeichen, Leerzeichen und Satzzeichen;
8. „Identitätsdaten“ die in Artikel 27 Absatz 3 Buchstaben a bis e genannten Daten;
9. „Fingerabdruckdaten“ Fingerabdrücke und Fingerabdruckspuren, die aufgrund ihrer Einzigartigkeit und der darin enthaltenen Bezugspunkte präzise und schlüssige Abgleiche zur Identität einer Person ermöglichen;
10. „Gesichtsbild“ eine digitale Aufnahme des Gesichts einer Person;
11. „biometrische Daten“ Fingerabdruckdaten oder Gesichtsbilder oder beides;
12. „biometrisches Template“ eine mathematische Repräsentation, die mittels Merkmalsauszug aus biometrischen Daten generiert wird, welche auf die für Identifizierungs- und Verifizierungszwecke erforderlichen Merkmale begrenzt sind;
13. „Reisedokument“ einen Reisepass oder ein anderes gleichwertiges Dokument, das seinen Inhaber zum Überschreiten der Außengrenzen berechtigt und in dem ein Visum angebracht werden kann;
14. „Reisedokumentendaten“ die Art, die Nummer und das Ausstellungsland des Reisedokuments, das Datum des Ablaufs der Gültigkeitsdauer des Reisedokuments und den aus drei Buchstaben bestehenden Code des Landes, das das Reisedokument ausgestellt hat;
15. „EU-Informationssysteme“ die Systeme EES, VIS, ETIAS, Eurodac, SIS und ECRIS-TCN;
16. „Europol-Daten“ die personenbezogenen Daten, die zu den in Artikel 18 Absatz 2 Buchstaben a, b und c der Verordnung (EU) 2016/794 genannten Zwecken von Europol verarbeitet werden;
17. „Interpol-Datenbanken“ die Interpol-Datenbank für gestohlene und verlorene Reisedokumente (Stolen and Lost Travel Document database, „SLTD-Datenbank“) und die Interpol-Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (Travel Documents Associated with Notices database, „TDAWN-Datenbank“);
18. „Übereinstimmung“ eine Übereinstimmung als Ergebnis eines automatischen Abgleichs zwischen zuvor oder zeitgleich in einem Informationssystem oder in einer Datenbank erfassten personenbezogenen Daten;
19. „Polizeibehörde“ die zuständige Behörde im Sinne des Artikels 3 Nummer 7 der Richtlinie (EU) 2016/680;
20. „benannte Behörden“ die benannten mitgliedstaatlichen Behörden im Sinne von Artikel 3 Absatz 1 Nummer 26 der Verordnung (EU) 2017/2226, Artikel 2 Absatz 1 Buchstabe e des Beschlusses 2008/633/JI und Artikel 3 Absatz 1 Nummer 21 der Verordnung (EU) 2018/1240;

21. „terroristische Straftat“ eine Straftat nach nationalem Recht, die einer der in der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates ([35]) aufgeführten Straftaten entspricht oder dieser gleichwertig ist;

22. „schwere Straftat“ eine Straftat, die einer der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates ([36]) aufgeführten Straftaten entspricht oder dieser gleichwertig ist, wenn die Straftat nach dem nationalen Recht mit einer Freiheitsstrafe oder freiheitsentziehenden Maßnahme im Höchstmaß von mindestens drei Jahren bedroht ist;

23. „Einreise-/Ausreisesystem“ oder „EES“ das durch die Verordnung (EU) 2017/2226 eingerichtete Einreise-/Ausreisesystem;

24. „Visa-Informationssystem“ oder „VIS“ das durch die Verordnung (EG) Nr. 767/2008 eingerichtete Visa-Informationssystem;

25. „Europäisches Reiseinformations- und -genehmigungssystem“ oder „ETIAS“ das durch die Verordnung (EU) 2018/1240 eingerichtete Europäische Reiseinformations- und -genehmigungssystem;

26. „Eurodac“ das durch die Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates ([37]) eingerichtete Eurodac-System;

27. „Schengener Informationssystem“ oder „SIS“ das durch die Verordnungen (EU) 2018/1860, (EU) 2018/1861 und (EU) 2018/1862 eingerichtete Schengener Informationssystem;

28. „ECRIS-TCN“ das durch die Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates ([38]). eingerichtete zentralisierte System für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen vorliegen;

Artikel 5

Nichtdiskriminierung und Grundrechte

Bei der Verarbeitung personenbezogener Daten für die Zwecke dieser Verordnung dürfen keine Personen aufgrund des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, einer politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung diskriminiert werden. Die Menschenwürde und die Integrität sowie die Grundrechte der Betroffenen, darunter auch das Recht auf Achtung der Privatsphäre und auf Schutz der personenbezogenen Daten, müssen uneingeschränkt gewahrt werden. Besonderer Aufmerksamkeit bedürfen Kinder, ältere Menschen, Menschen mit Behinderungen und Menschen, die internationalen Schutz benötigen. Dem Kindeswohl ist vorrangig Rechnung zu tragen.

KAPITEL II

Europäisches Suchportal

Artikel 6

Europäisches Suchportal

(1) Es wird ein Europäisches Suchportal (European search portal, im Folgenden „ESP“) geschaffen, das den mitgliedstaatlichen Behörden und den Stellen der Union einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu den EU-Informationssystemen, den Europol-Daten und den Interpol-Datenbanken zur Wahrnehmung ihrer Aufgaben und nach Maßgabe ihrer Zugangsrechte und im Einklang mit den Zielen und Zwecken des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN erleichtern soll.

([35]) Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates (ABl. L 88 vom 31.3.2017, S. 6).

([36]) Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. L 190 vom 18.7.2002, S. 1).

([37]) Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (ABl. L 180 vom 29.6.2013, S. 1).

([38]) Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, sowie zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726 (siehe Seite 1 dieses Amtsblatts).“

(2) Das ESP umfasst

a) eine zentrale Infrastruktur einschließlich eines Suchportals, das die gleichzeitige Abfrage des EES, des VIS, des ETIAS, von Eurodac, des SIS, des ECRIS-TCN, der Europol-Daten und der Interpol-Datenbanken ermöglicht;

b) einen sicheren Kommunikationskanal zwischen dem ESP und denjenigen Mitgliedstaaten und Stellen der Union, die berechtigt sind, das ESP zu nutzen;

c) eine sichere Kommunikationsinfrastruktur zwischen dem ESP und dem EES, dem VIS, dem ETIAS, Eurodac, dem zentralen SIS, dem ECRIS-TCN, den Europol-Daten und den Interpol-Datenbanken sowie zwischen dem ESP und den zentralen Infrastrukturen des CIR und des MID.

(3) eu-LISA entwickelt das ESP und sorgt für seine technische Verwaltung.

Artikel 7

Nutzung des Europäischen Suchportals

(1) Die Nutzung des ESP ist den mitgliedstaatlichen Behörden und den Stellen der Union vorbehalten, die auf mindestens eines der EU-Informationssysteme nach Maßgabe der für diese EU-Informationssysteme geltenden Rechtsinstrumente, den CIR und den MID nach Maßgabe der vorliegenden Verordnung, Europol-Daten nach Maßgabe der Verordnung (EU) 2016/794 oder die Interpol-Datenbanken nach Maßgabe der einschlägigen Bestimmungen des Unionsrechts oder des nationalen Rechts zugreifen können.

Diese mitgliedstaatlichen Behörden und Stellen der Union dürfen nur für die Ziele und Zwecke, die in den für diese EU-Informationssysteme geltenden Rechtsinstrumenten, der Verordnung (EU) 2016/794 und in der vorliegenden Verordnung festgelegt sind, auf das ESP und die von ihm bereitgestellten Daten zurückgreifen.

(2) Die in Absatz 1 genannten mitgliedstaatlichen Behörden und Stellen der Union nutzen das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten in den Zentralsystemen des EES, des VIS und des ETIAS nach Maßgabe ihrer jeweiligen Zugangsrechte gemäß den für diese EU-Informationssysteme geltenden Rechtsinstrumenten und dem nationalen Recht. Sie nutzen das ESP zudem nach Maßgabe ihrer in dieser Verordnung festgelegten Zugangsrechte für die Abfrage des CIR für die in den Artikeln 20, 21 und 22 genannten Zwecke.

(3) Die in Absatz 1 genannten mitgliedstaatlichen Behörden können das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten im in den Verordnungen (EU) 2018/1860 und (EU) 2018/1861 genannten zentralen SIS nutzen.

(4) Wenn es nach dem Unionsrecht vorgesehen ist, können die in Absatz 1 genannten Stellen der Union das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten im zentralen SIS nutzen.

(5) Die in Absatz 1 genannten mitgliedstaatlichen Behörden und der Stellen der Union können das ESP für die Abfrage von Daten zu Reisedokumenten in den Interpol-Datenbanken nach Maßgabe ihrer jeweiligen Zugangsrechte nach dem Unionsrecht beziehungsweise nach nationalem Recht nutzen, sofern das nach Unionsrecht oder nationalem Recht vorgesehen ist.

Artikel 8

Erstellung von ESP-Nutzerprofilen

(1) Um die Nutzung des ESP zu ermöglichen, erstellt eu-LISA in Zusammenarbeit mit den Mitgliedstaaten auf der Grundlage jeder Kategorie von ESP-Nutzern und der Abfragezwecke ein Profil, das den in Absatz 2 genannten technischen Einzelheiten und Zugangsrechten Rechnung trägt. Jedes Profil enthält dabei nach Maßgabe des Unionsrechts und des nationalen Rechts folgende Informationen:

a) die für die Datenabfrage zu verwendenden Suchfelder,

b) die EU-Informationssysteme, die Europol-Daten und die Interpol-Datenbanken, die abzufragen sind, diejenigen, die abgefragt werden können und diejenigen, zu denen dem Nutzer ein Abfrageergebnis ausgeben werden muss,

c) die spezifischen Daten in den EU-Informationssystemen, den Europol-Daten und den Interpol-Datenbanken, die abgefragt werden dürfen,

d) die Kategorien von Daten, die als Abfrageergebnis ausgegeben werden dürfen.

(2) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der technischen Einzelheiten der in Absatz 1 genannten Profile gemäß der jeweiligen Zugangsrechte der ESP-Nutzer nach den geltenden Rechtsinstrumenten zur Regelung der EU-Informationssysteme und nach nationalem Recht. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

(3) Die in Absatz 1 genannten Profile werden regelmäßig und mindestens einmal pro Jahr von eu-LISA in Zusammenarbeit mit den Mitgliedstaaten überprüft sowie erforderlichenfalls aktualisiert.

Artikel 9

Abfragen

(1) Die ESP-Nutzer geben, um Abfragen vorzunehmen, alphanumerische und/oder biometrische Daten in das ESP ein. Bei einer Abfrage fragt das ESP anhand der vom Nutzer des ESP eingegebenen Daten und nach Maßgabe des jeweiligen Nutzerprofils gleichzeitig das EES, das ETIAS, das VIS, das SIS, Eurodac, das ECRIS-TCN, den CIR, die Europol-Daten und die Interpol-Datenbanken ab.

(2) Die Kategorien von Daten für die Abfrage über das ESP entsprechen den Kategorien von Daten für Personen oder Reisedokumente, die für die Abfrage der verschiedenen EU-Informationssysteme, der Europol-Daten und der Interpol-Datenbanken nach Maßgabe der für sie geltenden Rechtsinstrumente verwendet werden können.

(3) Die eu-LISA erstellt in Zusammenarbeit mit den Mitgliedstaaten für das ESP eine Dokumentation zur Schnittstellenansteuerung in dem in Artikel 38 genannten UMF.

(4) Bei einer Abfrage durch einen ESP-Nutzer werden aus dem EES, dem ETIAS, dem VIS, dem SIS, Eurodac, dem ECRIS-TCN, dem CIR, dem MID, den Europol-Daten und aus den Interpol-Datenbanken von ihnen gehaltene Daten als Antwort auf die Abfrage bereitgestellt.

Unbeschadet des Artikels 20 wird in der vom ESP erteilten Antwort angegeben, aus welchem EU-Informationssystem beziehungsweise aus welcher Datenbank die betreffenden Daten stammen.

Das ESP liefert keine Angaben zu Daten in EU-Informationssystemen, zu Europol-Daten und zu den Interpol-Datenbanken, auf die der Nutzer nach dem anwendbaren Unionsrecht und nationalen Recht nicht zugreifen darf.

(5) Über das ESP durchgeführte Abfragen der Interpol-Datenbanken erfolgen so, dass dem für die Interpol-Ausschreibung Verantwortlichen keine Informationen preisgegeben werden.

(6) Sobald Daten aus einem der EU-Informationssysteme, den Europol-Daten oder den Interpol-Datenbanken verfügbar sind, werden dem Nutzer über das ESP Antworten erteilt. Diese Antworten enthalten lediglich die Daten, auf die der Nutzer nach dem Unionsrecht und dem nationalen Recht zugreifen darf.

(7) Die Kommission erlässt einen Durchführungsrechtsakt, um das technische Verfahren für Abfragen der EU-Informationssysteme, Europol-Daten und Interpol-Datenbanken durch das ESP und das Format der vom ESP erteilten Antworten festzulegen. Dieser Durchführungsrechtsakt wird nach dem Prüfverfahren gemäß Artikel 74 Absatz 2 erlassen.

Artikel 10

Führen von Protokollen

(1) Unbeschadet des Artikels 46 der Verordnung (EU) 2017/2226, des Artikels 34 der Verordnung (EG) Nr. 767/2008, des Artikels 69 der Verordnung (EU) 2018/1240 und der Artikel 12 und 18 der Verordnung (EU) 2018/1861 führt eu-LISA Protokolle sämtlicher im ESP erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat oder Stelle der Union, der bzw. die die Abfrage vornimmt, und verwendetes ESP-Nutzerprofil,

b) Datum und Uhrzeit der Abfrage,

c) abgefragte EU-Informationssysteme und Interpol-Datenbanken.

(2) Jeder Mitgliedstaat führt Protokolle über die Abfragen, die seine zur Nutzung des ESP ordnungsgemäß ermächtigten Behörden und deren Bedienstete durchführen. Jede Stelle der Union führt Protokolle über die Abfragen, die ihre ordnungsgemäß ermächtigten Bediensteten durchführen.

(3) Die in den Absätzen 1 und 2 genannten Protokolle werden nur zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald die Protokolle nicht mehr für das Kontrollverfahren benötigt werden.

Artikel 11

Ausweichverfahren für den Fall, dass eine Nutzung des Europäischen Suchportals technisch nicht möglich ist

(1) Wenn es wegen eines Ausfalls des ESP technisch nicht möglich ist, das ESP für die Abfrage eines oder mehrerer EU-Informationssysteme oder des CIR zu nutzen, werden die ESP-Nutzer von eu-LISA automatisch entsprechend benachrichtigt.

(2) Wenn es wegen eines Ausfalls der nationalen Infrastruktur eines Mitgliedstaats technisch nicht möglich ist, das ESP für die Abfrage eines oder mehrerer EU-Informationssysteme oder des CIR zu nutzen, benachrichtigt der betroffene Mitgliedstaat eu-LISA und die Kommission automatisch.

(3) In den Fällen der Absätze 1 oder 2 des vorliegenden Artikels gilt die in Artikel 7 Absätze 2 und 4 festgelegte Pflicht nicht, bis das technische Versagen behoben ist, und die Mitgliedstaaten fragen die EU-Informationssysteme oder das CIR unmittelbar ab, wenn sie nach dem Unionsrecht oder dem nationalen Recht hierzu verpflichtet sind.

(4) Wenn es wegen eines Ausfalls der Infrastruktur einer Stelle der Union technisch nicht möglich ist, das ESP für die Abfrage eines oder mehrerer EU-Informationssysteme oder des CIR zu nutzen, benachrichtigt die betroffene Stelle eu-LISA und die Kommission automatisch.

KAPITEL III

Gemeinsamer Dienst für den Abgleich biometrischer Daten

Artikel 12

Gemeinsamer Dienst für den Abgleich biometrischer Daten

(1) Es wird ein gemeinsamer Dienst für den Abgleich biometrischer Daten (shared biometric matching service — im Folgenden „gemeinsamer BMS“) eingerichtet, der die Aufgabe hat, biometrische Templates, die aus den im CIR und im SIS gespeicherten biometrischen Daten nach Artikel 13 generiert wurden, zu speichern und die systemübergreifende Abfrage mehrerer EU-Informationssysteme anhand biometrischer Daten zu ermöglichen, um den CIR und den MID sowie die Ziele des EES, des VIS, von Eurodac, des SIS und des ECRIS-TCN zu unterstützen.

(2) Der gemeinsame BMS umfasst

a) eine zentrale Infrastruktur, die die einzelnen Zentralsysteme des EES, des VIS, des SIS, von Eurodac bzw. des ECRIS-TCN insoweit ersetzt, als in ihr biometrische Templates gespeichert werden und sie Suchen mit biometrischen Daten ermöglicht,

b) eine sichere Kommunikationsinfrastruktur zwischen dem gemeinsamen BMS, dem zentralen SIS und dem CIR.

(3) eu-LISA entwickelt den gemeinsamen BMS und sorgt für seine technische Verwaltung.

Artikel 13

Speicherung biometrischer Templates im gemeinsamen Dienst für den Abgleich biometrischer Daten

(1) Der gemeinsame BMS speichert die biometrischen Templates, die er aus folgenden biometrischen Daten generiert:

a) Daten nach Artikel 16 Absatz 1 Buchstabe d, Artikel 17 Absatz 1 Buchstaben b und c und Artikel 18 Absatz 2 Buchstaben a, b und c der Verordnung (EU) 2017/2226,

b) Daten nach Artikel 9 Nummer 6 der Verordnung (EG) Nr. 767/2008,

c) Daten nach Artikel 20 Absatz 2 Buchstabe w und x, außer Daten von Handflächenabdrücken, der Verordnung (EU) 2018/1861,

d) Daten nach Artikel 4 Absatz 1 Buchstaben u und v der Verordnung (EU) 2018/1860;

Die biometrischen Templates werden im gemeinsamen BMS logisch voneinander getrennt nach den EU-Informationssystemen, aus denen sie stammen, gespeichert.

(2) Für jeden Satz der in Absatz 1 genannten Daten fügt der gemeinsame BMS jedem biometrischen Template einen Verweis auf die EU-Informationssysteme, in denen die betreffenden biometrischen Daten gespeichert sind, und einen Verweis auf die tatsächlichen Datensätze in diesen EU-Informationssystemen hinzu.

(3) Die biometrischen Templates dürfen erst in den gemeinsamen BMS eingegeben werden, nachdem der gemeinsame BMS die einem der EU-Informationssysteme hinzugefügten biometrischen Daten einer automatischen Qualitätskontrolle unterzogen hat, um sicherzustellen, dass ein Mindestdatenqualitätsstandard eingehalten wird.

(4) Bei der Speicherung der in Absatz 1 genannten Daten sind die in Artikel 37 Absatz 2 genannten Qualitätsstandards einzuhalten.

(5) Die Kommission legt im Wege eines Durchführungsrechtsakts die Leistungsanforderungen und praktischen Vorkehrungen für die Überwachung der Leistung des gemeinsamen BMS fest, um sicherzustellen, dass die Wirksamkeit biometrischer Suchvorgänge auch bei Verfahren gewährleistet ist, bei denen die Zeit eine Rolle spielt, wie etwa Grenzkontrollen und Identifizierungen. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 14

Abfrage biometrischer Daten mithilfe des gemeinsamen Dienstes für den Abgleich biometrischer Daten

Um die im CIR und im SIS gespeicherten biometrischen Daten abzufragen, nutzen der CIR und das SIS die im gemeinsamen BMS gespeicherten biometrischen Templates. Die Abfragen anhand biometrischer Daten werden zu den Zwecken vorgenommen, die in dieser Verordnung sowie in den Verordnungen (EG) Nr. 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 und (EU) 2019/816 vorgesehen sind.

Artikel 15

Datenspeicherung im gemeinsamen Dienst für den Abgleich biometrischer Daten

Die in Artikel 13 Absätze 1 und 2 genannten Daten werden im gemeinsamen BMS nur so lange gespeichert, wie die entsprechenden biometrischen Daten im CIR beziehungsweise im SIS gespeichert werden. Die Daten werden automatisch aus dem gemeinsamen BMS gelöscht.

Artikel 16

Führen von Protokollen

1. Unbeschadet des Artikels 46 der Verordnung (EU) 2017/2226, des Artikels 34 der Verordnung (EG) Nr. 767/2008 und der Artikel 12 und 18 der Verordnung (EU) 2018/1861 führt eu-LISA Protokolle sämtlicher im gemeinsamen BMS erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat oder Stelle der Union, der bzw. die die Abfrage vornimmt,

b) Chronik der Erstellung und der Speicherung biometrischer Templates,

c) die EU-Informationssysteme, die mit den im gemeinsamen BMS gespeicherten biometrischen Templates abgefragt wurden,

d) Datum und Uhrzeit der Abfrage,

e) Art der für die Abfrage verwendeten biometrischen Daten,

f) Abfrageergebnisse sowie Datum und Uhrzeit der Ergebnisanzeige.

(2) Jeder Mitgliedstaat führt Protokolle über die Abfragen, die seine zur Nutzung des gemeinsamen BMS ordnungsgemäß ermächtigten Behörden und deren Bedienstete durchführen. Jede Stelle der Union führt Protokolle über die Abfragen, die ihre ordnungsgemäß ermächtigten Bediensteten durchführen.

(3) Die in den Absätzen 1 und 2 genannten Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald die Protokolle nicht mehr für das Kontrollverfahren benötigt werden.

KAPITEL IV

Gemeinsamer Speicher für Identitätsdaten

Artikel 17

Gemeinsamer Speicher für Identitätsdaten

(1) Es wird ein gemeinsamer Speicher für Identitätsdaten (CIR) geschaffen, in dem für jede im EES, im VIS, im ETIAS, in Eurodac oder im ECRIS-TCN erfasste Person eine individuelle Datei mit den in Artikel 18 genannten Daten angelegt wird und der dazu dient, die korrekte Identifizierung von im EES, im VIS, im ETIAS, in Eurodac und im ECRIS-TCN gemäß Artikel 20 erfassten Personen zu erleichtern und zu unterstützen, das Funktionieren des MID gemäß Artikel 21 zu unterstützen und den etwaig erforderlichen Zugang von benannten Behörden und Europol zu dem EES, dem VIS, dem ETIAS und Eurodac zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer und anderer schwerer Straftaten gemäß Artikel 22 zu erleichtern und einheitlich zu regeln.

(2) Der CIR umfasst

a) eine zentrale Infrastruktur, die die einzelnen Zentralsysteme des EES, des VIS, des ETIAS, von Eurodac und des ECRIS-TCN insoweit ersetzt, als in ihr die in Artikel 18 genannten Daten gespeichert werden,

b) einen sicheren Kommunikationskanal zwischen dem CIR und den Mitgliedstaaten und Stellen der Union, die nach dem Unionsrecht und nationalen Recht berechtigt sind, den CIR zu nutzen,

c) eine sichere Kommunikationsinfrastruktur zwischen dem CIR und dem EES, dem VIS, dem ETIAS, Eurodac und dem ECRIS-TCN sowie den zentralen Infrastrukturen des ESP, des gemeinsamen BMS und des MID.

(3) eu-LISA entwickelt den CIR und sorgt für seine technische Verwaltung.

(4) Ist es aufgrund eines Ausfalls des CIR technisch nicht möglich, den CIR zur Identifizierung einer Person gemäß Artikel 20, zur Aufdeckung von Mehrfachidentitäten gemäß Artikel 21 oder zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer und anderer schwerer Straftaten gemäß Artikel 22 zu nutzen, werden die CIR-Nutzer automatisch von eu-LISA benachrichtigt.

(5) eu-LISA erstellt in Zusammenarbeit mit den Mitgliedstaaten für den CIR eine Dokumentation zur Schnittstellenansteuerung in dem in Artikel 38 genannten UMF.

Artikel 18

Im gemeinsamen Speicher für Identitätsdaten gespeicherte Daten

(1) Im CIR werden folgende Daten logisch voneinander getrennt nach den Informationssystemen, aus denen sie stammen, gespeichert:

a) Daten nach Artikel 16 Absatz 1 Buchstaben a bis d, Artikel 17 Absatz 1 Buchstaben a, b und c und Artikel 18 Absätze 1 und 2 der Verordnung (EU) 2017/2226,

b) Daten nach Artikel 9 Nummer 4 Buchstaben a bis c sowie Nummern 5 und 6 der Verordnung (EG) Nr. 767/2008,

c) Daten nach Artikel 17 Absatz 2 Buchstaben a bis e der Verordnung (EU) 2018/1240,

(2) Für jeden Satz der in Absatz 1 genannten Daten fügt der CIR einen Verweis auf die EU-Informationssysteme hinzu, aus denen die betreffenden Daten stammen.

(3) Die Behörden, die auf das CIR zugreifen, tun das gemäß ihren jeweiligen Zugangsrechten nach den für diese EU-Informationssysteme geltenden Rechtsinstrumenten und nach dem nationalen Recht sowie nach Maßgabe ihrer in dieser Verordnung festgelegten Zugangsrechte für die Zwecke nach den Artikeln 20, 21 und 22.

(4) Für jeden Satz der in Absatz 1 genannten Daten fügt der CIR einen Verweis auf den tatsächlichen Datensatz in den EU-Informationssystemen, aus dem die Daten stammen, hinzu.

(5) Bei der Speicherung der in Absatz 1 genannten Daten sind die in Artikel 37 Absatz 2 genannten Qualitätsstandards einzuhalten.

Artikel 19

Hinzufügung, Änderung und Löschung von Daten im gemeinsamen Speicher für Identitätsdaten

(1) Bei jeder Hinzufügung, Änderung oder Löschung von Daten im EES, im VIS und im ETIAS werden die in den individuellen Dateien im CIR gespeicherten Daten nach Artikel 18 automatisch entsprechend hinzugefügt, geändert oder gelöscht.

(2) Wird im MID nach Maßgabe der Artikel 32 oder 33 eine weiße oder eine rote Verknüpfung zwischen Daten von zwei oder mehr EU-Informationssystemen, die Bestandteil des CIR sind, erstellt, werden vom CIR keine neuen individuellen Dateien angelegt, sondern die neuen Daten der individuellen Datei der verknüpften Daten hinzugefügt.

Artikel 20

Zugang zum gemeinsamen Speicher für Identitätsdaten zwecks Identifizierung

(1) Abfragen im CIR werden von einer Polizeibehörde gemäß den Absätzen 2 und 5 nur in den folgenden Situationen vorgenommen:

a) wenn eine Polizeibehörde eine Person wegen des Fehlens eines Reisedokuments oder eines anderen glaubwürdigen Dokuments zum Nachweis der Identität dieser Person nicht identifizieren kann,

b) wenn Zweifel an den von einer Person vorgelegten Identitätsdaten bestehen,

c) wenn Zweifel an der Echtheit des Reisedokuments oder eines anderen glaubwürdigen, von einer Person vorgelegten Dokuments bestehen,

d) wenn Zweifel an der Identität des Inhabers eines Reisedokuments oder eines anderen glaubwürdigen Dokuments bestehen; oder

e) wenn eine Person zu einer Zusammenarbeit nicht in der Lage ist oder sie verweigert.

Eine solche Abfrage zu Minderjährigen unter zwölf Jahren ist unzulässig, es sei denn, sie erfolgt zum Wohl des Kindes.

(2) Ist eine der in Absatz 1 aufgeführten Situationen gegeben, und wurden einer Polizeibehörde mittels nationaler Gesetzgebungsmaßnahmen die in Absatz 5 genannten Befugnisse übertragen, darf sie ausschließlich zum Zwecke der Identifizierung einer Person anhand der bei einer Identitätskontrolle direkt vor Ort erhobenen biometrischen Daten dieser Person Abfragen im CIR vornehmen, sofern das Verfahren im Beisein dieser Person eingeleitet wurde.

(3) Falls eine solche Abfrage ergibt, dass im CIR Daten zu der betreffenden Person gespeichert sind, darf die betreffende Polizeibehörde die in Artikel 18 Absatz 1 genannten Daten einsehen.

Falls die biometrischen Daten der betreffenden Person nicht verwendet werden können oder die Abfrage anhand dieser Daten nicht erfolgreich ist, ist die Abfrage anhand von Identitätsdaten dieser Person in Verbindung mit Reisedokumentendaten oder anhand der von der betreffenden Person bereitgestellten Identitätsdaten vorzunehmen.

(4) Sind einer Polizeibehörde mittels nationaler Legislativmaßnahmen die in Absatz 6 genannten Befugnisse übertragen worden, darf sie im Falle einer Naturkatastrophe, eines Unfalls oder eines Terroranschlags und ausschließlich zum Zwecke der Identifizierung unbekannter Personen, die sich nicht ausweisen können, oder nicht identifizierter menschlicher Überreste mit den biometrischen Daten dieser Personen Abfragen im CIR vornehmen.

(5) Mitgliedstaaten, die die in Absatz 2 vorgesehene Möglichkeit nutzen möchten, erlassen entsprechende nationale Gesetzgebungsmaßnahmen. Dabei berücksichtigen die Mitgliedstaaten, dass jede Diskriminierung von Drittstaatsangehörigen vermieden werden muss. Durch derartige Gesetzgebungsmaßnahmen sind die genauen Zwecke der zu den in Artikel 2 Absatz 1 Buchstaben b und c genannten Zwecken erfolgenden Identifizierung festzulegen. Durch derartige Gesetzgebungsmaßnahmen sind zudem die zuständigen Polizeibehörden zu benennen sowie die Verfahren, Bedingungen und Kriterien derartiger Kontrollen festzulegen.

(6) Mitgliedstaaten, die die in Absatz 4 vorgesehene Möglichkeit nutzen möchten, erlassen entsprechende nationale Legislativmaßnahmen, in denen die hierfür geltenden Verfahren, Bedingungen und Kriterien festgelegt sind.

Artikel 21

Zugang zum gemeinsamen Speicher für Identitätsdaten zwecks Aufdeckung etwaiger Mehrfachidentitäten

(1) Falls bei der Abfrage des CIR eine gelbe Verknüpfung gemäß Artikel 28 Absatz 4 angezeigt wird, darf die Behörde, die für die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29 zuständig ist, ausschließlich zu Verifizierungszwecken auf die im CIR gespeicherten, durch die gelbe Verknüpfung bezeichneten Daten nach Artikel 18 Absätze 1 und 2 zugreifen.

(2) Falls bei der Abfrage des CIR eine rote Verknüpfung gemäß Artikel 32 angezeigt wird, dürfen die in Artikel 26 Absatz 2 genannten Behörden ausschließlich zur Bekämpfung von Identitätsbetrug auf die im CIR gespeicherten, durch die rote Verknüpfung bezeichneten Daten nach Artikel 18 Absätze 1 und 2 zugreifen.

Artikel 22

Abfrage des gemeinsamen Speichers für Identitätsdaten zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten

(1) Gibt es in einem konkreten Einzelfall vernünftige Gründe dafür, dass die Abfrage der EU-Informationssysteme zur Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten beitragen kann, insbesondere, wenn der Verdacht besteht, dass der Verdächtige, Täter oder das Opfer einer terroristischen Straftat oder sonstiger schwerer Straftaten eine Person ist, die im EES, im VIS oder im ETIAS gespeichert ist, können die benannten Behörden und Europol den CIR abfragen, um in Erfahrung zu bringen, ob im EES, im VIS oder im ETIAS Daten zu einer spezifischen Person gespeichert sind.

(2) Wenn die Abfrage im CIR ergibt, dass im EES, im VIS oder im ETIAS Daten zu der betreffenden Person gespeichert sind, zeigt der CIR den benannten Behörden und Europol durch einen Verweis nach Artikel 18 Absatz 2 an, in welchem dieser EU-Informationssysteme die übereinstimmende Daten gespeichert sind. Alle vom CIR ausgegebenen Antworten müssen so beschaffen sein, dass die Sicherheit der Daten nicht gefährdet wird.

Die Antwort, aus der hervorgeht, dass Daten zu dieser Person in einem der in Absatz 1 genannten EU-Informationssysteme gespeichert sind, darf ausschließlich für die Zwecke der Übermittlung eines Antrags auf uneingeschränkten Zugang vorbehaltlich der Bedingungen und Verfahren, die in den einschlägigen Rechtsinstrumenten festgelegt sind, verwendet werden.

Bei einer Übereinstimmung oder mehreren Übereinstimmungen stellt die benannte Behörde oder Europol einen Antrag auf uneingeschränkten Zugang zu mindestens einem der Informationssysteme, aus dem eine Übereinstimmung generiert wurde.

Wenn ein solcher uneingeschränkter Zugang ausnahmsweise nicht beantragt wird, verzeichnet die benannte Behörde die Begründung für die Nichtbeantragung, die in der nationalen Datei rückverfolgbar sein muss. Europol verzeichnet die Begründung in der entsprechenden Datei.

(3) Der vollständige Zugang zu den im EES, im VIS oder im ETIAS gespeicherten Daten, welche für die Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erforderlich sind, unterliegt weiterhin den Bedingungen und Verfahren, die in den einschlägigen Rechtsinstrumenten festgelegt sind.

Artikel 23

Datenspeicherung im gemeinsamen Speicher für Identitätsdaten

(1) Die in Artikel 18 Absätze 1, 2 und 4 genannten Daten werden im CIR automatisch nach Maßgabe der Datenspeicherungsbestimmungen der Verordnungen (EU) 2017/2226, (EG) Nr. 767/2008 beziehungsweise (EU) 2018/1240 gelöscht.

(2) Die individuellen Dateien werden im CIR nur so lange gespeichert, wie die entsprechenden Daten in mindestens einem der EU-Informationssysteme gespeichert werden, von dem Daten im CIR enthalten sind. Durch die Erstellung einer Verknüpfung wird die Speicherfrist der einzelnen durch die Verknüpfung bezeichneten Daten nicht berührt.

Artikel 24

Führen von Protokollen

(1) Unbeschadet des Artikels 46 der Verordnung (EU) 2017/2226, des Artikels 34 der Verordnung (EG) Nr. 767/2008 und des Artikels 69 der Verordnung (EU) 2018/1240 führt eu-LISA Protokolle sämtlicher im CIR erfolgenden Datenverarbeitungsvorgänge gemäß den Absätzen 2, 3 und 4 des vorliegenden Artikels.

(2) eu-LISA führt Protokolle sämtlicher im CIR gemäß Artikel 20 erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat oder Stelle der Union, der bzw. die die Abfrage vornimmt,

b) Zweck des Zugriffs vonseiten des Nutzers, der die Abfrage über den CIR vornimmt,

c) Datum und Uhrzeit der Abfrage,

d) Art der für die Abfrage verwendeten Daten,

e) Ergebnisse der Abfrage,

(3) eu-LISA führt Protokolle sämtlicher im CIR gemäß Artikel 21 erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat oder Stelle der Union, der bzw. die die Abfrage vornimmt,

b) Zweck des Zugriffs vonseiten des Nutzers, der die Abfrage über den CIR vornimmt,

c) Datum und Uhrzeit der Abfrage,

d) falls eine Verknüpfung erstellt wird, die für die Abfrage verwendeten Daten und die Ergebnisse der Abfrage mit Angabe des EU-Informationssystems, aus dem die Daten stammen.

(4) eu-LISA führt Protokolle sämtlicher im CIR gemäß Artikel 22 erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten olgende Angaben:

a) Datum und Uhrzeit der Abfrage,

b) die für die Abfrage verwendeten Daten,

c) Ergebnisse der Abfrage,

d) Mitgliedstaat oder Stelle der Union, der bzw. die den CIR abfragen.

Die zuständige Aufsichtsbehörde nach Artikel 41 der Richtlinie (EU) 2016/680 oder der Europäische Datenschutzbeauftragte nach Artikel 43 der Verordnung (EU) 2016/794 überprüft regelmäßig, spätestens jedoch alle sechs Monate, die betreffenden Zugangsprotokolle darauf, ob die Verfahren und Bedingungen nach Artikel 22 Absätze 1 und 2 der vorliegenden Verordnung eingehalten wurden.

(5) Jeder Mitgliedstaat führt Protokolle über die Abfragen, die seine zur Nutzung des CIR ordnungsgemäß ermächtigten Behörden und die Bediensteten dieser Behörden gemäß den Artikeln 20, 21 und 22 durchführen. Jede Stelle der Union führt Protokolle über die Abfragen, die ihre ordnungsgemäß ermächtigten Bediensteten gemäß den Artikeln 21 und 21 durchführen.

Zusätzlich führt jeder Mitgliedstaat für jeden Zugang zum CIR nach Artikel 22 folgende Protokolle:

a) nationales Aktenzeichen,

b) Zugangszweck,

c) nach Maßgabe der nationalen Vorschriften die eindeutige Nutzerkennung des Beamten, der die Abfrage vorgenommen hat, und des Beamten, der die Abfrage angeordnet hat.

(6) Gemäß der Verordnung (EU) 2016/794 führt Europol für jeden Zugang zum CIR nach Artikel 22 der vorliegenden Verordnung Protokolle der eindeutigen Nutzerkennung des Beamten, der die Abfrage vorgenommen hat, und des Beamten, der die Abfrage angeordnet hat.

(7) Die in den Absätzen 2 bis 6 genannten Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald die Protokolle nicht mehr für das Kontrollverfahren benötigt werden.

(8) eu-LISA speichert die Protokolle über die Chronik der Daten in individuellen Dateien. eu-LISA löscht solche Protokolle automatisch, sobald die Daten gelöscht werden.

KAPITEL V

Detektor für Mehrfachidentitäten

Artikel 25

Detektor für Mehrfachidentitäten

(1) Zur Unterstützung des Funktionierens des CIR und der Ziele des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN wird ein Detektor für Mehrfachidentitäten (MID) eingerichtet, der Identitätsbestätigungsdateien nach Artikel 34 erstellt und speichert, die Verknüpfungen zwischen in den EU-Informationssystemen einschließlich des CIR und des SIS enthaltenen Daten enthält und die Aufdeckung von Mehrfachidentitäten ermöglicht, mit dem doppelten Ziel, Identitätsprüfungen zu vereinfachen und Identitätsbetrug zu bekämpfen.

(2) Der MID umfasst

a) eine zentrale Infrastruktur, die Verknüpfungen und Angaben zu EU-Informationssystemen speichert;

b) eine sichere Kommunikationsinfrastruktur, über die der MID mit dem SIS und den zentralen Infrastrukturen des ESP und des CIR verbunden ist.

(3) eu-LISA entwickelt den MID und sorgt für seine technische Verwaltung.

Artikel 26

Zugriff auf den Detektor für Mehrfachidentitäten

(1) Für die Zwecke der manuellen Verifizierung verschiedener Identitäten nach Artikel 29 erhalten folgende Stellen Zugriff auf die im MID gespeicherten Daten nach Artikel 34:

a) die gemäß Artikel 9 Absatz 2 der Verordnung (EU) 2017/2226 benannten zuständigen Behörden beim Anlegen oder Aktualisieren eines persönlichen Dossiers im EES gemäß Artikel 14 der genannten Verordnung;

b) die in Artikel 6 Absatz 1 der Verordnung (EG) Nr. 767/2008 genannten Visumbehörden bei der Erstellung oder Aktualisierung eines Antragsdatensatzes im VIS gemäß der genannten Verordnung;

c) die ETIAS-Zentralstelle und die nationalen ETIAS-Stellen bei der Durchführung der Bearbeitung gemäß den Artikeln 22 und 26 der Verordnung (EU) 2018/1240;

d) das SIRENE-Büro des Mitgliedstaats, der eine SIS-Ausschreibung gemäß den Verordnungen (EU) 2018/1860 und (EU) 2018/1861 eingibt oder aktualisiert.

(2) Die mitgliedstaatlichen Behörden und die Stellen der Union, die Zugang zu mindestens einem in den CIR integrierten EU-Informationssystem oder zum SIS haben, erhalten über rote Verknüpfungen nach Artikel 32 Zugang zu den in Artikel 34 Buchstaben a und b genannten Daten.

(3) Die mitgliedstaatlichen Behörden und die Stellen der Union haben Zugang zu weißen Verknüpfungen nach Artikel 33, wenn sie Zugang zu den beiden EU-Informationssystemen haben, die die Daten enthalten, zwischen denen die weiße Verknüpfung erstellt wurde.

(4) Die mitgliedstaatlichen Behörden und die Stellen der Union haben Zugang zu grünen Verknüpfungen nach Artikel 31, wenn sie Zugang zu den beiden EU-Informationssystemen haben, die die Daten enthalten, zwischen denen die grüne Verknüpfung erstellt wurde, und eine Abfrage dieser Informationssysteme eine Übereinstimmung bei den beiden verknüpften Datensätzen ergeben hat.

Artikel 27

Prüfung auf Mehrfachidentitäten

(1) Im CIR und im SIS wird eine Prüfung auf Mehrfachidentitäten eingeleitet, wenn

a) im EES ein persönliches Dossier nach Artikel 14 der Verordnung (EU) 2017/2226 angelegt oder aktualisiert wird;

b) im VIS nach der Verordnung (EG) Nr. 767/2008 ein Antragsdatensatz erstellt oder aktualisiert wird;

c) im ETIAS nach Artikel 19 der Verordnung (EU) 2018/1240 ein Antragsdatensatz erstellt oder aktualisiert wird;

d) im SIS nach Artikel 3 der Verordnung (EU) 2018/1860 und Kapitel V der Verordnung (EU) 2018/1861 eine Ausschreibung zu einer Person erstellt oder aktualisiert wird.

(2) Wenn die in einem EU-Informationssystem enthaltenen Daten nach Absatz 1 biometrische Daten umfassen, nutzen der CIR und das zentrale SIS den gemeinsamen BMS für die Prüfung auf Mehrfachidentitäten. Der gemeinsame BMS vergleicht die aus neuen biometrischen Daten generierten biometrischen Templates mit den bereits im gemeinsamen BMS vorhandenen biometrischen Templates, um zu überprüfen, ob die zu derselben Person gehörenden Daten bereits im CIR oder im zentralen SIS gespeichert sind.

(3) Zusätzlich zu dem in Absatz 2 genannten Vorgang nutzen der CIR und das zentrale SIS das ESP, um anhand der folgenden Daten die im zentralen SIS bzw. im CIR gespeicherten Daten zu durchsuchen:

a) Nachname (Familienname), Vorname oder Vornamen, Geburtsdatum, Staatsangehörigkeit oder Staatsangehörigkeiten und Geschlecht gemäß Artikel 16 Absatz 1 Buchstabe a, Artikel 17 Absatz 1 und Artikel 18 Absatz 1 der Verordnung (EU) 2017/2226;

b) Nachname (Familienname), Vorname oder Vornamen, Geburtstdatum, Geschlecht, Ort und Land der Geburt und Staatsangehörigkeiten gemäß Artikel 9 Nummer 4 Buchstaben a und aa der Verordnung (EG) Nr. 767/2008;

c) Nachname (Familienname), Vorname(n), Geburtsname, Aliasname(n), Geburtsdatum, Geburtsort, Geschlecht und derzeitige Staatsangehörigkeit(en) gemäß Artikel 17 Absatz 2 der Verordnung (EU) 2018/1240;

d) Nachnamen; Vornamen, Geburtsnamen, früher verwendete Namen und Aliasnamen, Geburtsort, Geburtsdatum, Geschlecht und sämtliche Staatsangehörigkeiten gemäß Artikel 20 Absatz 2 der Verordnung (EU) 2018/1861;

e) Nachnamen, Vornamen, Geburtsnamen, frühere Namen und Aliasnamen, Geburtsort, Geburtsdatum, Geschlecht und sämtliche Staatsangehörigkeiten gemäß Artikel 4 der Verordnung (EU) 2018/1860.

(4) Zusätzlich zu dem in den Absätzen 2 und 3 genannten Vorgang nutzen der CIR und das zentrale SIS das ESP, um anhand der Reisedokumentendaten die im zentralen SIS bzw. im CIR gespeicherten Daten zu durchsuchen.

(5) Die Prüfung auf Mehrfachidentitäten wird nur durchgeführt, um Daten, die in einem EU-Informationssystem vorhanden sind, mit Daten, die in anderen EU-Informationssystemen vorhanden sind, zu vergleichen.

Artikel 28

Ergebnisse der Prüfung auf Mehrfachidentitäten

(1) Wenn die Abfragen nach Artikel 27 Absätze 2, 3 und 4 keine Übereinstimmung ergeben, werden die in Artikel 27 Absatz 1 genannten Verfahren gemäß den einschlägigen Rechtsinstrumenten fortgesetzt.

(2) Wenn die Abfrage nach Artikel 27 Absätze 2, 3 und 4 eine oder mehrere Übereinstimmungen ergibt, erstellen der CIR und gegebenenfalls das SIS eine Verknüpfung zwischen den für die Abfrage verwendeten Daten und den Daten, die zu der Übereinstimmung geführt haben.

Wenn mehrere Übereinstimmungen gemeldet werden, wird eine Verknüpfung zwischen allen Daten, die zu der Übereinstimmung geführt haben, erstellt. Wenn die Daten bereits verknüpft waren, wird die bestehende Verknüpfung auf die zur Abfrage verwendeten Daten ausgeweitet.

(3) Wenn die Abfrage nach Artikel 27 Absätze 2, 3 und 4 eine oder mehrere Übereinstimmungen ergibt und die Identitätsdaten der verknüpften Dateien gleich oder ähnlich sind, wird eine weiße Verknüpfung nach Artikel 33 erstellt.

(4) Wenn die Abfrage nach Artikel 27 Absätze 2, 3 und 4 eine oder mehrere Übereinstimmungen ergibt und die Identitätsdaten der verknüpften Dateien nicht als ähnlich angesehen werden können, wird eine gelbe Verknüpfung nach Artikel 30 erstellt, und das Verfahren nach Artikel 29 gelangt zur Anwendung.

(5) Die Kommission erlässt gemäß Artikel 73 delegierte Rechtsakte zur Festlegung der Verfahren für die Bestimmung der Fälle, in denen Identitätsdaten als identisch oder ähnlich angesehen werden können.

(6) Die Verknüpfungen werden in der Identitätsbestätigungsdatei gemäß Artikel 34 gespeichert.

(7) Die Kommission legt in Zusammenarbeit mit eu-LISA die technischen Vorschriften für die Erstellung von Verknüpfungen zwischen Daten aus unterschiedlichen EU-Informationssystemen im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 29

Manuelle *Verifizierung verschiedener Identitäten* und zuständige Behörden

(1) Unbeschadet von Absatz 2 sind für die manuelle Verifizierung verschiedener Identitäten folgende Behörden zuständig:

a) die gemäß Artikel 9 Absatz 2 der Verordnung (EU) 2017/2226 benannte Behörde, die für Übereinstimmungen zuständig ist, die beim Anlegen oder Aktualisieren eines persönlichen Dossiers im EES im Sinne der genannten Verordnung erzielt wurden;

b) die in Artikel 6 Absatz 1 der Verordnung (EG) Nr. 767/2008 genannten Visumbehörden, die für Übereinstimmungen zuständig sind, die bei der Erstellung oder Aktualisierung eines Antragsdatensatzes im VIS gemäß jener Verordnung erzielt wurden;

c) die ETIAS-Zentralstelle und die nationalen ETIAS-Stellen bei Übereinstimmungen, die bei der Erstellung oder Aktualisierung eines Antragsdatensatzes gemäß der Verordnung (EU) 2018/1240 erzielt wurden;

d) das SIRENE-Büro des Mitgliedstaats bei Übereinstimmungen, die bei der Eingabe oder Aktualisierung einer SIS-Ausschreibung gemäß den Verordnungen (EU) 2018/1860 und (EU) 2018/1861 erzielt wurden.

Der MID gibt die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde in der Identitätsbestätigungsdatei an.

(2) Die für die manuelle Verifizierung verschiedener Identitäten in der Identitätsbestätigungsdatei zuständige Behörde ist das SIRENE-Büro des Mitgliedstaats, der die Ausschreibung eingegeben hat, wenn eine Verknüpfung zu Daten erstellt wird, die in einer Ausschreibung

a) von Personen zum Zwecke der Übergabe- oder Auslieferungshaft nach Artikel 26 der Verordnung (EU) 2018/1862 enthalten sind;

b) von Vermissten oder schutzbedürftigen Personen nach Artikel 32 der Verordnung (EU) 2018/1862 enthalten sind;

c) von Personen, die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht werden, nach Artikel 34 der Verordnung (EU) 2018/1862 enthalten sind;

d) von Personen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielte Kontrollen nach Artikel 36 der Verordnung (EU) 2018/1862 enthalten sind;

(3) Die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde erhält unbeschadet des Absatzes 4 dieses Artikels Zugriff auf die in der betreffenden Identitätsbestätigungsdatei enthaltenen verknüpften Daten und auf die im CIR und gegebenenfalls im SIS verknüpften Identitätsdaten. Sie prüft die verschiedenen Identitäten unverzüglich. Sobald die Prüfung abgeschlossen ist, aktualisiert sie die Verknüpfung gemäß den Artikeln 31, 32 und 33 und fügt diese unverzüglich zur Identitätsbestätigungsdatei hinzu.

(4) Wenn die für die manuelle Verifizierung verschiedener Identitäten in der Identitätsbestätigungsdatei zuständige Behörde die gemäß Artikel 9 Absatz 2 der Verordnung (EU) 2017/2226 benannte zuständige Behörde ist, die im EES ein persönliches Dossier nach Artikel 14 der genannten Verordnung anlegt oder aktualisiert, und wenn eine gelbe Verknüpfung erstellt wird, führt diese Behörde zusätzliche Überprüfungen durch. Diese Behörde erhält nur für diesen Zweck Zugriff auf die in der betreffenden Identitätsbestätigungsdatei enthaltenen einschlägigen Daten. Sie prüft die verschiedenen Identitäten, aktualisieren die Verknüpfung gemäß den Artikeln 31, 32 und 33 der vorliegenden Verordnung und fügt diese unverzüglich zur Identitätsbestätigungsdatei hinzu.

Diese manuelle Verifizierung verschiedener Identitäten wird im Beisein der betroffenen Person eingeleitet, die Gelegenheit erhält, die Umstände der zuständigen Behörde zu erläutern, die diese Erläuterungen zu berücksichtigen hat.

Wenn die manuelle Verifizierung verschiedener Identitäten an der Grenze erfolgt, wird sie möglichst innerhalb von zwölf Stunden nach der Erstellung einer gelben Verknüpfung gemäß Artikel 28 Absatz 4 vorgenommen.

(5) Wenn mehr als eine Verknüpfung erstellt wird, prüft die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde jede Verknüpfung gesondert.

(6) Wenn Daten, die zu einer Übereinstimmung geführt haben, bereits verknüpft sind, berücksichtigt die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde die bestehenden Verknüpfungen bei der Prüfung, ob neue Verknüpfungen erstellt werden müssen.

Artikel 30

Gelbe Verknüpfung

(1) Wurde noch keine manuelle Verifizierung verschiedener Identitäten vorgenommen, wird eine Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen in folgenden Fällen als gelb klassifiziert:

a) Die verknüpften Daten enthalten dieselben biometrischen Daten, aber ähnliche oder unterschiedliche Identitätsdaten;

b) die verknüpften Daten enthalten unterschiedliche Identitätsdaten aber dieselben Reisedokumentendaten, und mindestens eines der EU-Informationssysteme enthält keine biometrischen Daten zu der betroffenen Person;

c) die verknüpften Daten enthalten dieselben Identitätsdaten, aber unterschiedliche biometrische Daten;

d) die verknüpften Daten enthalten ähnliche oder unterschiedliche Identitätsdaten, dieselben Reisedokumentendaten, aber unterschiedliche biometrische Daten.

(2) Wenn eine Verknüpfung gemäß Absatz 1 als gelb klassifiziert wird, gelangt das Verfahren nach Artikel 29 zur Anwendung.

Artikel 31

Grüne Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen wird als grün klassifiziert, wenn

a) die verknüpften Daten unterschiedliche biometrische Daten, aber dieselben Identitätsdaten enthalten und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde festgestellt hat, dass sich die verknüpften Daten auf zwei unterschiedliche Personen beziehen;

b) die verknüpften Daten unterschiedliche biometrische Daten, ähnliche oder unterschiedliche Identitätsdaten und dieselben Reisedokumentendaten enthalten und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde festgestellt hat, dass sich die verknüpften Daten auf zwei unterschiedliche Personen beziehen;

c) die verknüpften Daten unterschiedliche Identitätsdaten, aber dieselben Reisedokumentendaten enthalten, mindestens eines der EU-Informationssysteme keine biometrischen Daten zu der betroffenen Person enthält und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde festgestellt hat, dass sich die verknüpften Daten auf zwei unterschiedliche Personen beziehen.

(2) Wenn eine Abfrage im CIR oder im SIS durchgeführt wird und eine grüne Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen besteht, zeigt der MID an, dass die Identitätsdaten der verknüpften Daten nicht ein und dieselbe Person bezeichnen.

(3) Wenn eine mitgliedstaatliche Behörde Belege hat, aus denen hervorgeht, dass eine grüne Verknüpfung im MID unrichtig erfasst wurde, dass eine grüne Verknüpfung nicht dem neuesten Stand entspricht oder dass mit der Verarbeitung der Daten im MID oder den EU-Informationssystemen gegen diese Verordnung verstoßen wurde, muss sie die betreffenden im CIR und im SIS gespeicherten Daten überprüfen und die Verknüpfung gegebenenfalls unverzüglich berichtigen oder aus dem MID löschen. Diese mitgliedstaatliche Behörde setzt unverzüglich den für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaat in Kenntnis.

Artikel 32

Rote Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen wird in folgenden Fällen als rot klassifiziert:

a) Die verknüpften Daten enthalten dieselben biometrischen Daten, aber ähnliche oder unterschiedliche Identitätsdaten, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten in ungerechtfertigter Weise auf ein und dieselbe Person beziehen;

b) die verknüpften Daten enthalten dieselben, ähnliche oder unterschiedliche Identitätsdaten und die gleichen Reisedokumentendaten, aber unterschiedliche biometrische Daten, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten auf zwei unterschiedliche Personen beziehen, von denen mindestens eine dasselbe Reisedokument in ungerechtfertigter Weise benutzt;

c) die verknüpften Daten enthalten dieselben Identitätsdaten, aber unterschiedliche biometrischen Daten und unterschiedliche oder keine Reisedokumentendaten, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten in ungerechtfertigter Weise auf zwei unterschiedliche Personen beziehen;

d) die verknüpften Daten enthalten unterschiedliche Identitätsdaten, aber dieselben Reisedokumentendaten, mindestens eines der EU-Informationssysteme enthält keine biometrischen Daten zu der betreffenden Person, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten in ungerechtfertigter Weise auf ein und dieselbe Person beziehen.

(2) Wenn eine Abfrage im CIR oder im SIS durchgeführt wird und eine rote Verknüpfung zwischen Daten in zwei oder mehr EU-Informationssystemen besteht, zeigt der MID die in Artikel 34 genannten Daten an. Bei etwaigen Folgemaßnahmen zu einer roten Verknüpfung sind die einschlägigen Bestimmungen des Unionsrechts und des nationalen Rechts einzuhalten, wobei sich etwaige rechtliche Folgen für die betroffene Person nur auf die einschlägigen Daten zu dieser Person gründen dürfen. Aufgrund der bloßen Existenz einer roten Verknüpfung entstehen für die betroffene Person keine rechtlichen Folgen.

(3) Wenn eine rote Verknüpfung zwischen Daten im EES, im VIS, im ETIAS, in Eurodac oder im ECRIS-TCN erstellt wird, wird die im CIR gespeicherte individuelle Datei gemäß Artikel 19 Absatz 2 aktualisiert.

(4) Unbeschadet der Bestimmungen für die Handhabung von Ausschreibungen im SIS in den Verordnungen (EU) 2018/1860, (EU) 2018/1861 und (EU) 2018/1862 und unbeschadet der erforderlichen Einschränkungen zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass bei der Erstellung einer roten Verknüpfung keine nationalen Ermittlungen beeinträchtigt werden, teilt die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde der betroffenen Person mit, dass illegale Mehrfachidentitätsdaten vorliegen, und teilt der Person die einmalige Kennnummer gemäß Artikel 34 Buchstabe c der vorliegenden Verordnung, die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde gemäß Artikel 34 Buchstabe d der vorliegenden Verordnung und die Adresse des nach Artikel 49 der vorliegenden Verordnung eingerichteten Web-Portals mit.

(5) Die in Absatz 4 genannten Informationen werden von der für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde schriftlich anhand eines Standardformulars zur Verfügung gestellt. Die Kommission legt den Inhalt und die Darstellung dieses Formulars im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

(6) Wenn eine rote Verknüpfung erstellt wird, unterrichtet der MID automatisch die Behörden, die für die verknüpften Daten zuständig sind.

(7) Wenn eine Behörde eines Mitgliedstaates oder eine Stelle der Union mit Zugriff auf den CIR oder das SIS Belege dafür hat, dass eine rote Verknüpfung im MID unrichtig erfasst wurde oder dass mit der Verarbeitung der Daten im MID, im CIR oder im SIS gegen diese Verordnung verstoßen wurde, muss die Behörde oder Stelle die betreffenden im CIR und im SIS gespeicherten Daten überprüfen und,

a) wenn sich die Verknüpfung auf eine der SIS-Ausschreibungen gemäß Artikel 29 Absatz 2 bezieht, umgehend das zuständige SIRENE-Büro des Mitgliedstaats informieren, das die SIS-Ausschreibung erstellt hat;

b) in allen anderen Fällen die Verknüpfung umgehend entweder berichtigen oder aus dem MID löschen.

Wird ein SIRENE-Büro gemäß Unterabsatz 1 Buchstabe a kontaktiert, verifiziert es die von der mitgliedstaatlichen Behörde oder Stelle der Union vorgelegten Belege unverzüglich und berichtigt gegebenenfalls umgehend die Verknüpfung oder löscht diese aus dem MID.

Die mitgliedstaatliche Behörde, die die Belege erhält, informiert unverzüglich die Behörde des Mitgliedstaats, die für die manuelle Verifizierung verschiedener Identitäten zuständig ist, über jegliche Berichtigung oder Löschung einer roten Verknüpfung.

Artikel 33

Weiße Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen wird in folgenden Fällen als weiß klassifiziert:

a) Die verknüpften Daten enthalten dieselben biometrischen Daten und dieselben oder ähnliche Identitätsdaten;

b) die verknüpften Daten enthalten dieselben oder ähnliche Identitätsdaten, dieselben Reisedokumentendaten und in mindestens einem der EU-Informationssysteme liegen keine biometrischen Daten zu der betroffenen Person vor;

c) die verknüpften Daten enthalten dieselben biometrischen Daten, dieselben Reisedokumentendaten, und ähnliche Identitätsdaten;

d) die verknüpften Daten enthalten dieselben biometrischen Daten, aber ähnliche oder unterschiedliche Identitätsdaten, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten in gerechtfertigter Weise auf ein und dieselbe Person beziehen.

(2) Wenn eine Abfrage im CIR oder im SIS durchgeführt wird und eine weiße Verknüpfung zwischen Daten in zwei oder mehr EU-Informationssystemen besteht, zeigt der MID an, dass die Identitätsdaten der verknüpften Daten ein und dieselbe Person bezeichnen. In der Antwort der abgefragten EU-Informationssysteme werden gegebenenfalls alle verknüpften Daten zu der Person angezeigt, wodurch eine Übereinstimmung auf Basis der Daten, die durch die weiße Verknüpfung verknüpft sind, erfolgt, soweit die Behörde, welche die Abfrage durchführt, nach dem Unionsrecht oder nationalem Recht Zugriff auf die verknüpften Daten hat.

(3) Wenn eine weiße Verknüpfung zwischen Daten im EES, im VIS, im ETIAS, in Eurodac oder im ECRIS-TCN erstellt wird, wird die im CIR gespeicherte individuelle Datei gemäß Artikel 19 Absatz 2 aktualisiert.

(4) Wenn nach einer manuellen Verifizierung von verschiedener Identitäten eine weiße Verknüpfung erstellt wird, teilt die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde der betreffenden Person unbeschadet der Bestimmungen für die Handhabung von Ausschreibungen im SIS in den Verordnungen (EU) 2018/1860, (EU) 2018/1861 und (EU) 2018/1862 und unbeschadet der erforderlichen Einschränkungen zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass keine nationalen Ermittlungen beeinträchtigt werden, mit, dass ähnliche oder unterschiedliche Identitätsdaten vorliegen, und teilt der Person die einmalige Kennnummer gemäß Artikel 34 Buchstabe c der vorliegenden Verordnung, die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde gemäß Artikel 34 Buchstabe d der vorliegenden Verordnung und die Adresse des nach Artikel 49 der vorliegenden Verordnung eingerichteten Web-Portals mit.

(5) Wenn eine mitgliedstaatliche Behörde Belege hat, aus denen hervorgeht, dass eine weiße Verknüpfung im MID unrichtig erfasst wurde, dass eine weiße Verknüpfung nicht dem neuesten Stand entspricht oder dass mit der Verarbeitung der Daten im MID oder in den EU-Informationssystemen gegen diese Verordnung verstoßen wurde, muss sie die betreffenden im CIR und im SIS gespeicherten Daten überprüfen und die Verknüpfung gegebenenfalls unverzüglich berichtigen oder aus dem MID löschen. Diese mitgliedstaatliche Behörde setzt unverzüglich den für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaat in Kenntnis.

(6) Die in Absatz 4 genannten Informationen werden von der für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde schriftlich anhand eines Standardformulars zur Verfügung gestellt. Die Kommission legt den Inhalt und die Darstellung dieses Formulars im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 34

Identitätsbestätigungsdatei

Die Identitätsbestätigungsdatei enthält folgende Daten:

a) die in den Artikeln 30 bis 33 genannten Verknüpfungen;

b) eine Angabe der EU-Informationssysteme, in denen die verknüpften Daten gespeichert sind;

c) eine einmalige Kennnummer, die das Abrufen der verknüpften Daten aus den entsprechenden EU-Informationssystemen ermöglicht;

d) eine Angabe der für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde;

e) das Datum der Erstellung oder jeder Aktualisierung der Verknüpfung.

Artikel 35

Datenspeicherung im Detektor für Mehrfachidentitäten

Die Identitätsbestätigungsdateien und die in ihnen enthaltenen Daten einschließlich der Verknüpfungen werden im MID nur so lange gespeichert, wie die verknüpften Daten in zwei oder mehr EU-Informationssystemen gespeichert werden. Sie werden automatisch aus dem MID gelöscht.

Artikel 36

Führen von Protokollen

(1) eu-LISA führt Protokolle über alle Datenverarbeitungsvorgänge im MID. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat, der die Abfrage vornimmt;

b) Zweck des Zugriffs des Nutzers;

c) Datum und Uhrzeit der Abfrage;

d) Art der für die Abfrage verwendeten Daten;

e) Verweis auf die verknüpften Daten;

f) Chronik der Identitätsbestätigungsdatei.

(2) Jeder Mitgliedstaat führt Protokolle über die Abfragen, die seine zur Nutzung des MID ordnungsgemäß ermächtigten Behörden und deren Bedienstete durchführen. Jede Stelle der Union führt Protokolle über die Abfragen, die ihre ordnungsgemäß ermächtigten Behörden durchführen.

(3) Die in den Absätzen 1 und 2 genannten Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald die Protokolle nicht mehr für das Kontrollverfahren benötigt werden.

KAPITEL VI

Maßnahmen zur Unterstützung der Interoperabilität

Artikel 37

Datenqualität

(1) Unbeschadet der Verantwortlichkeiten der Mitgliedstaaten für die Qualität der in die Systeme eingegebenen Daten führt eu-LISA für die im EES, im VIS, im ETIAS, im SIS, im gemeinsamer BMS und im CIR gespeicherten Daten Mechanismen und Verfahren für die automatische Datenqualitätskontrolle ein.

(2) eu-LISA setzt Mechanismen für die Bewertung der Richtigkeit des gemeinsamen BMS, gemeinsame Datenqualitätsindikatoren und die Mindestqualitätsstandards für die Speicherung von Daten im EES, im VIS, im ETIAS, im SIS, im gemeinsamen BMS und im CIR um.

Nur Daten, die den Mindestqualitätsstandards genügen, dürfen in das EES, das VIS, das ETIAS, das SIS, den gemeinsamen BMS, den CIR und den MID eingegeben werden.

(3) eu-LISA legt den Mitgliedstaaten regelmäßig Berichte über die Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie die gemeinsamen Datenqualitätsindikatoren vor. Ferner legt eu-LISA der Kommission regelmäßig Berichte über die festgestellten Probleme und die betroffenen Mitgliedstaaten vor. eu-LISA legt diese Berichte auf Anfrage auch dem Europäischen Parlament und dem Rat vor. Keiner der in diesem Absatz genannten Berichte darf personenbezogene Daten enthalten.

(4) Die Einzelheiten der Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie der gemeinsamen Datenqualitätsindikatoren und der Mindestqualitätsstandards für die Speicherung von Daten im EES, im VIS, im ETIAS, im SIS und im gemeinsamen BMS und im CIR, insbesondere bei biometrischen Daten, werden in Durchführungsrechtsakten festgelegt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

(5) Ein Jahr nach der Einführung der Mechanismen und Verfahren für die automatische Datenqualitätskontrolle, der gemeinsamen Datenqualitätsindikatoren und der Mindestdatenqualitätsstandards und danach jedes Jahr evaluiert die Kommission die Umsetzung der Datenqualität durch die Mitgliedstaaten und gibt erforderlichenfalls Empfehlungen ab. Die Mitgliedstaaten legen der Kommission einen Aktionsplan zur Beseitigung etwaiger im Evaluierungsbericht festgestellter Mängel und insbesondere zur Lösung von Problemen bei der Datenqualität, die sich aus fehlerhaften Daten in EU-Informationssystemen ergeben, vor. Die Mitgliedstaaten erstatten der Kommission regelmäßig Bericht über die Fortschritte bei der Umsetzung dieses Aktionsplans, bis dieser vollständig umgesetzt ist.

Die Kommission übermittelt den Evaluierungsbericht dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten, dem Europäischen Datenschutzausschuss und der durch die Verordnung (EG) Nr. 168/2007 des Rates ([39]) eingerichteten Agentur der Europäischen Union für Grundrechte.

Artikel 38

Universelles Nachrichtenformat

(1) Das universelle Nachrichtenformat (UMF) wird eingeführt. Mit dem UMF werden Standards für bestimmte inhaltliche Elemente des grenzüberschreitenden Informationsaustauschs zwischen Informationssystemen, Behörden und/oder Organisationen im Bereich Justiz und Inneres festgelegt.

(2) Der UMF-Standard ist bei der Entwicklung des EES, des ETIAS, des ESP, des CIR und des MID sowie gegebenenfalls bei der Entwicklung neuer Modelle für den Informationsaustausch und neuer Informationssysteme im Bereich Justiz und Inneres durch eu-LISA oder eine andere Stelle der Union zu verwenden.

(3) Die Kommission erlässt einen Durchführungsrechtsakt zur Festlegung und Entwicklung des in Absatz 1 dieses Artikels genannten UMF-Standards. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 39

Zentraler Speicher für Berichte und Statistiken

(1) Es wird ein zentraler Speicher für Berichte und Statistiken (CRRS) eingerichtet, um die Ziele des EES, des VIS, des ETIAS sowie des SIS gemäß den entsprechenden geltenden Rechtsinstrumenten zu unterstützen und systemübergreifende statistische Daten und analytische Berichte für politische und operative Zwecke sowie für die Zwecke der Datenqualität bereitzustellen.

(2) eu-LISA sorgt an ihren technischen Standorten für die Einrichtung, die Implementierung und das Hosting des CRRS, das logisch nach den EU-Informationssystemen getrennt die Daten und Statistiken nach Artikel 63 der Verordnung (EU) 2017/2226, Artikel 17 der Verordnung (EG) Nr. 767/2008, Artikel 84 der Verordnung (EU) 2018/1240 und Artikel 60 der Verordnung (EU) 2018/1861 sowie Artikel 16 der Verordnung (EU) 2018/1860 enthält. Der Zugang zum CRRS erfolgt in Form eines kontrollierten, gesicherten Zugangs und spezifischen Nutzerprofilen und wird den in Artikel 63 der Verordnung (EU) 2017/2226, Artikel 17 der Verordnung (EG) Nr. 767/2008, Artikel 84 der Verordnung (EU) 2018/1240 und Artikel 60 der Verordnung (EU) 2018/1861 genannten Behörden ausschließlich zu Berichterstattungs- und Statistikzwecken gewährt.

(3) eu-LISA anonymisiert die Daten und speichert diese anonymisierten Daten im CRRS. Die Anonymisierung der Daten erfolgt nach einem automatisierten Verfahren.

Die im CRRS enthaltenen Daten dürfen keine Identifizierung von Einzelpersonen ermöglichen.

(4) Der CRRS umfasst

a) die für die Anonymisierung von Daten notwendigen Instrumente;

b) eine zentrale Infrastruktur, die aus einem Datenregister anonymisierter Daten besteht;

c) eine sichere Kommunikationsinfrastruktur, über die der CRRS mit dem EES, dem VIS, dem ETIAS und dem SIS sowie den zentralen Infrastrukturen des gemeinsamen BMS, des CIR und des MID verbunden ist.

(5) Die Kommission erlässt einen delegierten Rechtsakt gemäß Artikel 73, um detaillierte Bestimmungen über den Betrieb des CRRS, einschließlich spezifischer Garantien für die Verarbeitung personenbezogener Daten gemäß den Absätzen 2 und 3 des vorliegenden Artikels und der für den Speicher geltenden Sicherheitsvorschriften festzulegen.

([39]) Verordnung (EG) Nr. 168/2007 des Rates vom 15. Februar 2007 zur Errichtung einer Agentur der Europäischen Union für Grundrechte (ABl. L 53 vom 22.2.2007, S. 1).

KAPITEL VII

Datenschutz

Artikel 40

Für die Verarbeitung Verantwortlicher

(1) Für die Verarbeitung von Daten im gemeinsamen BMS sind die mitgliedstaatlichen Behörden, die jeweils für die Verarbeitung im EES, im VIS und im SIS verantwortlich sind, Verantwortliche im Sinne des Artikels 4 Nummer 7 der Verordnung (EU) 2016/679 oder des Artikels 3 Nummer 8 der Richtlinie (EU) 2016/680 für die aus den in Artikel 13 der vorliegenden Verordnung genannten Daten generierten biometrischen Templates, die sie in die zugrunde liegenden Systeme eingeben, und tragen die Verantwortung für die Verarbeitung der biometrischen Templates im gemeinsamen BMS.

(2) Für die Verarbeitung von Daten im CIR sind die mitgliedstaatlichen Behörden, die jeweils für die Verarbeitung im EES, im VIS und im ETIAS verantwortlich sind, Verantwortliche im Sinne des Artikels 4 Nummer 7 der Verordnung (EU) 2016/679 für die in Artikel 18 der vorliegenden Verordnung genannten Daten, die sie in die zugrunde liegenden Systeme eingeben, und tragen die Verantwortung für die Verarbeitung dieser personenbezogenen Daten im CIR.

(3) Für die Verarbeitung von Daten im MID

a) ist die Europäische Agentur für die Grenz- und Küstenwache ein für die Verarbeitung Verantwortlicher im Sinne des Artikels 3 Nummer 8 der Verordnung (EU) 2018/1725 für die Verarbeitung personenbezogener Daten durch die ETIAS-Zentralstelle;

b) sind die mitgliedstaatlichen Behörden, die Daten in der Identitätsbestätigungsdatei hinzufügen oder ändern, Verantwortliche im Sinne des Artikels 4 Nummer 7 der Verordnung (EU) 2016/679 oder des Artikels 3 Nummer 8 der Richtlinie (EU) 2016/680 und tragen die Verantwortung für die Verarbeitung personenbezogener Daten im MID.

(4) Zum Zwecke der datenschutzrechtlichen Kontrolle, einschließlich zur Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung, haben die für die Verarbeitung Verantwortlichen Zugang zu den Protokollen nach den Artikeln 10, 16, 24 und 36 für die Eigenkontrolle nach Artikel 44.

Artikel 41

Datenauftragsverarbeiter

Für die Verarbeitung personenbezogener Daten im gemeinsamen BMS, im CIR und im MID ist eu-LISA Datenauftragsverarbeiter im Sinne des Artikels 3 Nummer 12 Buchstabe a der Verordnung (EU) 2018/1725.

Artikel 42

Sicherheit der Verarbeitung

(1) eu-LISA, die ETIAS-Zentralstelle, Europol und die mitgliedstaatlichen Behörden gewährleisten die Sicherheit der Verarbeitung personenbezogener Daten nach Maßgabe dieser Verordnung. Bei der Erfüllung sicherheitsbezogener Aufgaben arbeiten eu-LISA, die ETIAS-Zentralstelle, Europol und die mitgliedstaatlichen Behörden zusammen.

(2) Unbeschadet des Artikels 33 der Verordnung (EU) 2018/1725 ergreift eu-LISA die erforderlichen Maßnahmen, um die Sicherheit der Interoperabilitätskomponenten und der mit ihnen verbundenen Kommunikationsinfrastruktur sicherzustellen.

(3) Insbesondere trifft eu-LISA die erforderlichen Maßnahmen, einschließlich der Annahme eines Sicherheitsplans, eines Betriebskontinuitätsplans und eines Notfallwiederherstellungsplans, um

a) die Daten physisch zu schützen, unter anderem durch Aufstellung von Notfallplänen für den Schutz kritischer Infrastrukturen;

b) Unbefugten den Zugang zu Datenverarbeitungseinrichtungen und -anlagen zu verwehren;

c) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden;

d) die unbefugte Dateneingabe sowie die unbefugte Kenntnisnahme, Änderung oder Löschung gespeicherter personenbezogener Daten zu verhindern;

e) die unbefugte Datenverarbeitung sowie das unbefugte Kopieren, Ändern oder Löschen von Daten zu verhindern;

f) zu verhindern, dass automatisierte Datenverarbeitungssysteme mithilfe von Datenübertragungseinrichtungen von Unbefugten genutzt werden;

g) sicherzustellen, dass die zum Zugang zu den Interoperabilitätskomponenten berechtigten Personen nur mittels einer persönlichen Benutzerkennung und vertraulicher Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können;

h) sicherzustellen, dass überprüft und festgestellt werden kann, welchen Stellen personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden können;

i) sicherzustellen, dass überprüft und festgestellt werden kann, welche Daten wann, von wem und zu welchem Zweck in den Interoperabilitätskomponenten verarbeitet wurden;

j) das unbefugte Lesen, Kopieren, Ändern oder Löschen von personenbezogenen Daten während der Übermittlung personenbezogener Daten an die oder aus den Interoperabilitätskomponenten oder während des Transports von Datenträgern zu verhindern, insbesondere durch geeignete Verschlüsselungstechniken;

k) sicherzustellen, dass eingesetzte Systeme im Störungsfall für den Normalbetrieb wiederhergestellt werden können;

l) die Zuverlässigkeit sicherzustellen, indem dafür Sorge getragen wird, dass alle Funktionsstörungen der Interoperabilitätskomponenten ordnungsgemäß gemeldet werden;

m) die Wirksamkeit der in diesem Absatz genannten Sicherheitsmaßnahmen zu überwachen, die erforderlichen organisatorischen Maßnahmen für die interne Überwachung zu treffen, um die Einhaltung dieser Verordnung sicherzustellen, und diese Sicherheitsmaßnahmen vor dem Hintergrund neuer technologischer Entwicklungen zu bewerten.

(4) Die Mitgliedstaaten, Europol und die ETIAS-Zentralstelle treffen für die Verarbeitung personenbezogener Daten durch die Behörden, die das Recht auf Zugang zu Interoperabilitätskomponenten haben, Sicherheitsmaßnahmen, die den in Absatz 3 genannten entsprechen.

Artikel 43

Sicherheitsvorfälle

(1) Jedes Ereignis, das sich auf die Sicherheit der Interoperabilitätskomponenten auswirkt oder auswirken kann und darin gespeicherte Daten beschädigen oder ihren Verlust herbeiführen kann, ist als Sicherheitsvorfall anzusehen; das gilt insbesondere, wenn möglicherweise ein unbefugter Datenzugriff erfolgt ist oder die Verfügbarkeit, die Integrität und die Vertraulichkeit von Daten tatsächlich oder möglicherweise nicht mehr gewährleistet war.

(2) Sicherheitsvorfällen ist durch eine rasche, wirksame und angemessene Reaktion zu begegnen.

(3) Unbeschadet der Meldung und Mitteilung einer Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 der Verordnung (EU) 2016/679, Artikel 30 der Richtlinie (EU) 2016/680 oder beiden Artikeln unterrichten die Mitgliedstaaten die Kommission, eu-LISA, die zuständigen Aufsichtsbehörden und den Europäischen Datenschutzbeauftragten unverzüglich über etwaige Sicherheitsvorfälle.

Unbeschadet der Artikel 34 und 35 der Verordnung (EU) 2018/1725 und Artikel 34 der Verordnung (EU) 2016/794 unterrichten die ETIAS-Zentralstelle und Europol die Kommission, eu-LISA und den Europäischen Datenschutzbeauftragten unverzüglich über etwaige Sicherheitsvorfälle.

Im Falle eines Sicherheitsvorfalls in Verbindung mit der zentralen Infrastruktur der Interoperabilitätskomponenten unterrichtet eu-LISA die Kommission und den Europäischen Datenschutzbeauftragten unverzüglich.

(4) Informationen über einen Sicherheitsvorfall, der sich auf den Betrieb der Interoperabilitätskomponenten oder die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten auswirkt oder auswirken kann, werden den Mitgliedstaaten, der ETIAS-Zentralstelle und Europol unverzüglich bereitgestellt und nach Maßgabe des von eu-LISA bereitzustellenden Plans für die Bewältigung von Sicherheitsvorfällen gemeldet.

(5) Die betroffenen Mitgliedstaaten, die ETIAS-Zentralstelle, Europol und eu-LISA arbeiten im Falle eines Sicherheitsvorfalls zusammen. Die Kommission legt die genauen Modalitäten dieser Zusammenarbeit im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 44

Eigenkontrolle

Die Mitgliedstaaten und die zuständigen Stellen der Union stellen sicher, dass jede zum Zugriff auf die Interoperabilitätskomponenten berechtigte Behörde die erforderlichen Maßnahmen zur Überwachung der Einhaltung dieser Verordnung trifft und erforderlichenfalls mit der Aufsichtsbehörde zusammenarbeitet.

Die für die Verarbeitung Verantwortlichen im Sinne des Artikels 40 treffen die erforderlichen Maßnahmen, um die Ordnungsgemäßheit der Datenverarbeitung gemäß dieser Verordnung zu überwachen, unter anderem durch häufige Überprüfung der Protokolle gemäß den Artikeln 10, 16, 24 und 36, und arbeiten erforderlichenfalls mit den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten zusammen.

Artikel 45

Sanktionen

Die Mitgliedstaaten stellen sicher, dass jeder Missbrauch von Daten, jede Verarbeitung von Daten oder jeder Austausch von Daten, die dieser Verordnung zuwiderläuft, gemäß nationalem Recht geahndet werden können. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

Artikel 46

Haftung

(1) Unbeschadet des Anspruchs auf Schadenersatz durch den für die Verarbeitung Verantwortlichen oder den Datenauftragsverarbeiter und unbeschadet ihrer Haftung gemäß der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2018/1725

a) hat jede Person oder jeder Mitgliedstaat, der/dem durch eine rechtswidrige Verarbeitung personenbezogener Daten oder durch andere gegen diese Verordnung verstoßende Handlungen seitens eines Mitgliedstaats ein materieller oder immaterieller Schaden entsteht, das Recht, von diesem Mitgliedstaat Schadenersatz zu verlangen;

b) hat jede Person oder jeder Mitgliedstaat, der/dem durch eine gegen diese Verordnung verstoßende Handlung seitens Europol, der Europäischen Agentur für die Grenz- und Küstenwache oder eu-LISA ein materieller oder immaterieller Schaden entsteht, das Recht, von der betreffenden Stelle Schadenersatz zu verlangen.

Der betreffende Mitgliedstaat, Europol, die Europäische Agentur für die Grenz- und Küstenwache oder eu-LISA werden vollständig oder teilweise von ihrer Haftung nach Unterabsatz 1 befreit, wenn sie nachweisen, dass sie für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich sind.

(2) Verursacht eine Verletzung der in dieser Verordnung festgelegten Pflichten durch einen Mitgliedstaat einen Schaden an den Interoperabilitätskomponenten, haftet dieser Mitgliedstaat für den entstandenen Schaden, sofern und soweit es eu-LISA oder ein anderer durch diese Verordnung gebundener Mitgliedstaat nicht versäumt haben, angemessene Maßnahmen zur Verhinderung des Schadens oder zur Verringerung seiner Auswirkungen zu ergreifen.

(3) Die Geltendmachung von Schadenersatzansprüchen nach den Absätzen 1 und 2 gegen einen Mitgliedstaat unterliegt dem nationalen Recht des beklagten Mitgliedstaats. Die Geltendmachung von Schadenersatzansprüchen nach den Absätzen 1 und 2 gegen den für die Verarbeitung Verantwortlichen oder eu-LISA unterliegt den in den Verträgen vorgesehenen Voraussetzungen.

Artikel 47

Recht auf Information

(1) Die Behörde, die die personenbezogenen Daten erfasst, die im gemeinsamen BMS, im CIR oder im MID zu speichern sind, stellt den Personen, deren Daten erfasst werden, die Informationen zur Verfügung, die nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679, den Artikeln 12 und 13 der Richtlinie (EU) 2016/680 und den Artikeln 15 und 16 der Verordnung (EU) 2018/1725 vorgeschrieben sind. Die Behörde stellt die Informationen zum Zeitpunkt der Datenerfassung zur Verfügung.

(2) Alle Informationen werden in einer in klarer und einfacher Sprache verfassten Sprachfassung, die die betreffende Person versteht oder von der vernünftigerweise angenommen werden darf, dass sie sie versteht, bereitgestellt. Die Informationen müssen für Minderjährige auch in einer dem Alter angemessenen Weise bereitgestellt werden.

(3) Personen, deren Daten im EES, im VIS oder im ETIAS gespeichert sind, werden über die Verarbeitung personenbezogener Daten für die Zwecke dieser Verordnung gemäß Absatz 1 informiert, wenn

a) im EES ein persönliches Dossier nach Artikel 14 der Verordnung (EU) 2017/2226 angelegt oder aktualisiert wird;

b) im VIS nach Artikel 8 der Verordnung (EG) Nr. 767/2008 ein Antragsdatensatz erstellt oder aktualisiert wird;

c) im ETIAS nach Artikel 19 der Verordnung (EU) 2018/1240 ein Antragsdatensatz erstellt oder aktualisiert wird.

Artikel 48

Recht auf Auskunft, Berichtigung und Löschung von im MID gespeicherten personenbezogenen Daten sowie auf Einschränkung ihrer Verarbeitung

(1) Personen, die von ihren Rechten nach den Artikeln 15 bis 18 der Verordnung (EU) 2016/679, den Artikeln 17 bis 20 der Verordnung (EU) 2018/1725 und den Artikeln 14, 15 und 16 der Richtlinie (EU) 2016/680 Gebrauch machen möchten, können sich an die zuständige Behörde eines beliebigen Mitgliedstaats wenden, der den Antrag prüft und beantwortet.

(2) Der Mitgliedstaat, der einen solchen Antrag prüft, antwortet unverzüglich, in jedem Fall jedoch innerhalb von 45 Tagen nach Antragseingang. Diese Frist kann um weitere 15 Tage verlängert werden, wenn das unter Berücksichtigung der Komplexität und der Zahl der Anträge erforderlich ist. Der Mitgliedstaat, der den Antrag prüft, unterrichtet die betroffene Person innerhalb von 45 Tagen nach Antragseingang über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Die Mitgliedstaaten können entscheiden, dass die Antworten von Zentralstellen zu erteilen sind.

(3) Wird ein Antrag auf Berichtigung oder Löschung personenbezogener Daten bei einem anderen Mitgliedstaat als dem für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaat gestellt, so kontaktiert der Mitgliedstaat, an den der Antrag gerichtet wurde, innerhalb von sieben Tagen die Behörden des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats. Der für die manuelle Verifizierung verschiedener Identitäten zuständige Mitgliedstaat überprüft die Richtigkeit der Daten und die Rechtmäßigkeit der Datenverarbeitung unverzüglich, in jedem Fall jedoch innerhalb von 30 Tagen nach der Kontaktaufnahme. Diese Frist kann um weitere 15 Tage verlängert werden, wenn das unter Berücksichtigung der Komplexität und der Zahl der Anträge erforderlich ist. Der für die manuelle Verifizierung verschiedener Identitäten zuständige Mitgliedstaat unterrichtet den Mitgliedstaat, der ihn kontaktiert hat, von jeder solchen Fristverlängerung und nennt die Gründe für die Verzögerung. Der Mitgliedstaat, der die Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats kontaktiert hat, informiert die betroffene Person über das weitere Verfahren.

(4) Wird ein Antrag auf Berichtigung oder Löschung personenbezogener Daten bei einem Mitgliedstaat gestellt, in dem die ETIAS-Zentralstelle für die manuelle Verifizierung verschiedener Identitäten zuständig war, so kontaktiert der Mitgliedstaat, an den der Antrag gerichtet wurde, die ETIAS-Zentralstelle innerhalb von sieben Tagen, um sie darum zu ersuchen, eine Stellungnahme abzugeben. Die ETIAS-Zentralstelle gibt ihre Stellungnahme unverzüglich, in jedem Fall jedoch innerhalb von 30 Tagen nach der Kontaktaufnahme ab. Diese Frist kann um weitere 15 Tage verlängert werden, wenn das unter Berücksichtigung der Komplexität und der Zahl der Anträge erforderlich ist. Die betroffene Person wird von dem Mitgliedstaat, der die ETIAS-Zentralstelle kontaktiert hat, über das weitere Verfahren informiert.

(5) Falls bei einer Prüfung festgestellt wird, dass die im MID gespeicherten Daten unrichtig sind oder unrechtmäßig erfasst wurden, werden diese Daten vom für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaat oder, wenn kein Mitgliedstaat für die manuelle Verifizierung verschiedener Identitäten zuständig war oder wenn die ETIAS-Zentralstelle für die manuelle Verifizierung verschiedener Identitäten zuständig war, von dem Mitgliedstaat, an den der Antrag gerichtet wurde, unverzüglich berichtigt oder gelöscht. Die betroffene Person wird schriftlich darüber informiert, dass ihre Daten berichtigt oder gelöscht worden sind.

(6) Falls im MID gespeicherte Daten während ihrer Speicherfrist von einem Mitgliedstaat geändert werden, nimmt dieser Mitgliedstaat die Verarbeitung nach Artikel 27 und gegebenenfalls die Verarbeitung nach Artikel 29 vor, um zu ermitteln, ob die geänderten Daten verknüpft werden müssen. Ergibt sich bei der Verarbeitung keine Übereinstimmung, so löscht dieser Mitgliedstaat die Daten aus der Identitätsbestätigungsdatei. Falls bei der automatisierten Verarbeitung ein oder mehrere Übereinstimmungen gemeldet werden, erstellt oder aktualisiert dieser Mitgliedstaat die betreffende Verknüpfung gemäß den einschlägigen Bestimmungen dieser Verordnung.

(7) Ist der für die manuelle Verifizierung verschiedener Identitäten zuständige Mitgliedstaat oder gegebenenfalls der Mitgliedstaat, an den der Antrag gerichtet wurde, nicht der Ansicht, dass die im MID gespeicherten Daten unrichtig sind oder unrechtmäßig gespeichert wurden, so erlässt er eine Verwaltungsentscheidung, in der er der betroffenen Person unverzüglich schriftlich erläutert, warum er nicht zu einer Berichtigung oder Löschung der sie betreffenden Daten bereit ist.

(8) In der Entscheidung gemäß Absatz 7 wird die betroffene Person zudem darüber belehrt, dass sie die Entscheidung über ihren Antrag auf Auskunft über personenbezogene Daten bzw. Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten anfechten und wie sie gegebenenfalls bei den zuständigen Gerichten oder Behörden Klage erheben oder Beschwerde einlegen kann, einschließlich diesbezüglicher Hilfe, auch der Aufsichtsbehörden.

(9) Jeder Antrag auf Auskunft über personenbezogene Daten bzw. Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten enthält die zur Identifizierung der betroffenen Person notwendigen Informationen. Diese Informationen werden ausschließlich dazu verwendet, die Wahrnehmung der in diesem Artikel genannten Rechte zu ermöglichen, und anschließend unverzüglich gelöscht.

(10) Der für die manuelle Verifizierung verschiedener Identitäten zuständige Mitgliedstaat oder gegebenenfalls der Mitgliedstaat, an den der Antrag gerichtet wurde, führt eine schriftliche Aufzeichnung darüber, dass ein Antrag auf Auskunft über personenbezogene Daten bzw. Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten gestellt und wie dieser bearbeitet wurde, und stellt diese Aufzeichnung unverzüglich den Aufsichtsbehörden zur Verfügung.

(11) Dieser Artikel gilt unbeschadet etwaiger Beschränkungen und Einschränkungen der in diesem Artikel festgelegten Rechte gemäß der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680.

Artikel 49

Web-Portal

(1) Um die Ausübung der Rechte auf Auskunft über personenbezogene Daten bzw. Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten zu erleichtern, wird ein Web-Portal eingerichtet.

(2) Das Web-Portal enthält Informationen über die Rechte und Verfahren nach den Artikeln 47 und 48 und eine Benutzerschnittstelle, die es Personen, deren Daten im MID verarbeitet werden und die davon unterrichtet wurden, dass eine rote Verknüpfung nach Artikel 32 Absatz 4 angezeigt wurde, ermöglicht, die Kontaktinformationen der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats zu erhalten.

(3) Um die Kontaktinformationen der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats zu erhalten, sollte die Person, deren Daten im MID verarbeitet werden, die Angaben zu der für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde nach Artikel 34 Buchstabe d eingeben. Das Web-Portal benutzt diese Angaben, um die Kontaktinformationen der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats abzurufen. Das Web-Portal umfasst auch eine E-Mail-Vorlage, um die Kommunikation zwischen dem Portalnutzer und der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats zu erleichtern. Diese E-Mail enthält ein Eingabefeld für die einmalige Kennnummer nach Artikel 34 Buchstabe c, um der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats zu ermöglichen, die betreffenden Daten zu identifizieren.

(4) Die Mitgliedstaaten stellen eu-LISA die Kontaktdaten aller Behörden zur Verfügung, die für die Prüfung und Beantwortung von Anträgen nach den Artikeln 47 und 48 zuständig sind, und überprüfen regelmäßig, ob diese Kontaktdaten aktuell sind.

(5) eu-LISA entwickelt das Web-Portal und sorgt für seine technische Verwaltung.

(6) Die Kommission erlässt einen delegierten Rechtsakt gemäß Artikel 73, um detaillierte Bestimmungen über den Betrieb des Web-Portals festzulegen, einschließlich der Benutzerschnittstelle, der Sprachen, in denen das Web-Portal zur Verfügung stehen soll, und der E-Mail-Vorlage.

Artikel 50

Übermittlung personenbezogener Daten an Drittstaaten, internationale Organisationen und private Stellen

Unbeschadet des Artikels 65 der Verordnung (EU) 2018/1240, der Artikel 25 und 26 der Verordnung (EU) 2016/794, des Artikels 41 der Verordnung (EU) 2017/2226, des Artikels 31 der Verordnung (EG) Nr. 767/2008 und der Abfrage von Interpol-Datenbanken durch das ESP gemäß Artikel 9 Absatz 5 der vorliegenden Verordnung, die gemäß den Bestimmungen des Kapitels V der Verordnung (EU) 2018/1725 und des Kapitels V der Verordnung (EU) 2016/679 stehen, dürfen personenbezogene Daten, die in den Interoperabilitätskomponenten gespeichert sind, verarbeitet werden oder auf die über die Interoperabilitätskomponenten zugegriffen wird, nicht an Drittstaaten, internationale Organisationen oder private Stellen übermittelt oder diesen zur Verfügung gestellt werden.

Artikel 51

Überwachung durch die Aufsichtsbehörden

(1) Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörden die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung durch den betreffenden Mitgliedstaat, einschließlich der Übermittlung an die und von den Interoperabilitätskomponenten, unabhängig überwachen.

(2) Jeder Mitgliedstaat trägt dafür Sorge, dass die gemäß der Richtlinie (EU) 2016/680 erlassenen nationalen Rechts- und Verwaltungsvorschriften gegebenenfalls auch für den Zugang von Polizeibehörden und benannten Behörden zu den Interoperabilitätskomponenten gelten, auch hinsichtlich der Rechte der Personen, auf deren Daten auf diese Weise zugegriffen wird.

(3) Die Aufsichtsbehörden stellen sicher, dass mindestens alle vier Jahre die durch die zuständigen nationalen Behörden erfolgenden Verarbeitungsvorgänge von personenbezogenen Daten für die Zwecke der vorliegenden Verordnung nach den einschlägigen internationalen Prüfungsstandards überprüft werden.

Die Aufsichtsbehörden veröffentlichen jährlich die Zahl der Anträge auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung personenbezogener Daten, die getroffenen Folgemaßnahmen und die Zahl der Berichtigungen, Löschungen und Einschränkungen der Verarbeitung, die auf Antrag der betroffenen Personen vorgenommen wurden.

(4) Die Mitgliedstaaten stellen sicher, dass ihre Aufsichtsbehörden über ausreichende Ressourcen und Fachkenntnisse zur Wahrnehmung der Aufgaben verfügen, die ihnen gemäß dieser Verordnung übertragen werden.

(5) Die Mitgliedstaaten stellen alle Informationen, die von einer in Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörde angefordert werden, zur Verfügung, insbesondere Informationen zu den Tätigkeiten, die entsprechend ihren Verantwortlichkeiten gemäß der vorliegenden Verordnung durchgeführt werden. Die Mitgliedstaaten gewähren den in Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden Zugang zu ihren Protokollen nach den Artikeln 10, 16, 24 und 36 der vorliegenden Verordnung sowie zu den Begründungen nach Artikel 22 Absatz 2 der vorliegenden Verordnung und gestatten ihnen jederzeit Zutritt zu allen ihren für Interoperabilitätszwecke genutzten Räumlichkeiten.

Artikel 52

Prüfungen durch den Europäischen Datenschutzbeauftragten

Der Europäische Datenschutzbeauftragte trägt dafür Sorge, dass die durch eu-LISA, die ETIAS-Zentralstelle und Europol für die Zwecke der vorliegenden Verordnung erfolgenden Verarbeitungsvorgänge von personenbezogenen Daten mindestens alle vier Jahre nach den einschlägigen internationalen Prüfungsstandards überprüft werden. Der Prüfbericht wird dem Europäischen Parlament, dem Rat, eu-LISA, der Kommission, den Mitgliedstaaten und der betreffenden Stelle der Union übermittelt. eu-LISA, die ETIAS-Zentralstelle und Europol erhalten vor der Annahme des Berichts Gelegenheit zur Stellungnahme.

eu-LISA, die ETIAS-Zentralstelle und Europol liefern die vom Europäischen Datenschutzbeauftragten angeforderten Informationen, gewähren dem Europäischen Datenschutzbeauftragten Zugang zu allen von ihm angeforderten Dokumenten und zu ihren Protokollen nach den Artikeln 10, 16, 24 und 36 und gestatten dem Europäischen Datenschutzbeauftragten jederzeit Zutritt zu allen ihren Räumlichkeiten.

Artikel 53

Zusammenarbeit zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten

(1) Die Aufsichtsbehörden und der Europäische Datenschutzbeauftragte arbeiten — jeweils innerhalb ihres Kompetenzbereichs — im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammen und sorgen für eine koordinierte Aufsicht der Nutzung der Interoperabilitätskomponenten und der Anwendung anderer Bestimmungen dieser Verordnung, insbesondere wenn der Europäische Datenschutzbeauftragte oder eine Aufsichtsbehörde größere Diskrepanzen zwischen den Verfahrensweisen der Mitgliedstaaten feststellt oder möglicherweise unrechtmäßige Übermittlungen über die Kommunikationskanäle der Interoperabilitätskomponenten bemerkt.

(2) In den in Absatz 1 dieses Artikels genannten Fällen wird eine koordinierte Aufsicht gemäß Artikel 62 der Verordnung (EU) 2018/1725 sichergestellt.

(3) Bis zum 12. Juni 2021 und danach alle zwei Jahre übermittelt der Europäische Datenschutzausschuss einen gemeinsamen Bericht über seine Tätigkeiten im Rahmen dieses Artikels an das Europäische Parlament, den Rat, die Kommission, Europol, die Europäische Agentur für die Grenz- und Küstenwache und eu-LISA. Dieser Bericht enthält für jeden Mitgliedstaat ein Kapitel, das von der Aufsichtsbehörde des betreffenden Mitgliedstaats erstellt wird.

KAPITEL VIII

Verantwortlichkeiten

Artikel 54

Verantwortlichkeiten von eu-LISA während der Konzept- und Entwicklungsphase

(1) eu-LISA stellt sicher, dass die zentralen Infrastrukturen der Interoperabilitätskomponenten gemäß dieser Verordnung betrieben werden.

(2) Die Interoperabilitätskomponenten werden an den technischen Standorten von eu-LISA betrieben und bieten die in dieser Verordnung vorgesehenen Funktionen gemäß den in Artikel 55 Absatz 1 festgelegten Bedingungen für die Sicherheit, Verfügbarkeit, Qualität und Leistung.

(3) eu-LISA ist verantwortlich für die Entwicklung der Interoperabilitätskomponenten sowie für jegliche Anpassungen, die erforderlich sind, um die Interoperabilität zwischen den Zentralsystemen des EES, des VIS, des ETIAS, des SIS, von Eurodac, dem ECRIS-TCN, dem ESP, dem BMS, dem CIR, dem MID und dem CRRS herzustellen.

Unbeschadet des Artikels 66 hat eu-LISA keinen Zugang zu den personenbezogenen Daten, die über das ESP, den gemeinsamen BMS, den CIR oder den MID verarbeitet werden.

eu-LISA konzipiert die Architektur der Interoperabilitätskomponenten einschließlich ihrer Kommunikationsinfrastrukturen, legt ihre technischen Spezifikationen fest und bestimmt ihre Weiterentwicklung in Bezug auf die zentrale Infrastruktur und die sichere Kommunikationsinfrastruktur, die vom Verwaltungsrat vorbehaltlich einer befürwortenden Stellungnahme der Kommission angenommen werden. eu-LISA nimmt zudem etwaige erforderliche Anpassungen am EES, VIS, ETIAS oder SIS vor, die für die Herstellung der Interoperabilität notwendig und in dieser Verordnung vorgesehen sind.

eu-LISA entwickelt und implementiert die Interoperabilitätskomponenten so bald wie möglich nach dem Inkrafttreten dieser Verordnung und nach Erlass der in Artikel 8 Absatz 2, Artikel 9 Absatz 7, Artikel 28 Absätze 5 und 7, Artikel 37 Absatz 4, Artikel 38 Absatz 3, Artikel 39 Absatz 5, Artikel 43 Absatz 5 und Artikel 78 Absatz 10 vorgesehenen Maßnahmen durch die Kommission.

Die Entwicklung umfasst die Ausarbeitung und Umsetzung der technischen Spezifikationen, die Erprobung und die gesamte Projektverwaltung und -koordination.

(4) Während der Konzept- und Entwicklungsphase wird ein Programmverwaltungsrat eingerichtet, der aus höchstens zehn Mitgliedern besteht. Dem Programmverwaltungsrat gehören sieben Mitglieder, die vom Verwaltungsrat von eu-LISA aus dem Kreis seiner Mitglieder oder stellvertretenen Mitglieder ernannt werden, der Vorsitzende der Beratergruppe für Interoperabilität gemäß Artikel 75, ein vom Exekutivdirektor ernannter Vertreter von eu-LISA sowie ein von der Kommission ernanntes Mitglied an. Die vom Verwaltungsrat von eu-LISA ernannten Mitglieder werden ausschließlich aus dem Kreis derjenigen Mitgliedstaaten gewählt, die nach dem Unionsrecht in vollem Umfang durch die Rechtsinstrumente gebunden sind, welche für die Entwicklung, die Errichtung, den Betrieb und die Nutzung aller EU-Informationssysteme gelten, und die sich an den Interoperabilitätskomponenten beteiligen werden.

(5) Der Programmverwaltungsrat tritt regelmäßig, mindestens jedoch dreimal pro Quartal zusammen. Er stellt die angemessene Verwaltung der Konzept- und Entwicklungsphase der Interoperabilitätskomponenten sicher.

Der Programmverwaltungsrat legt dem Verwaltungsrat von eu-LISA monatlich schriftliche Berichte über den Fortschritt des Projekts vor. Der Programmverwaltungsrat hat keine Entscheidungsbefugnis und kein Mandat zur Vertretung der Mitglieder des Verwaltungsrats von eu-LISA.

(6) Der Verwaltungsrat von eu-LISA legt die Geschäftsordnung des Programmverwaltungsrats fest, in der insbesondere Folgendes geregelt ist:

a) der Vorsitz,

b) die Sitzungsorte,

c) die Vorbereitung von Sitzungen,

d) die Zulassung von Sachverständigen zu den Sitzungen,

e) Kommunikationspläne, die gewährleisten, dass nicht teilnehmende Mitglieder des Verwaltungsrats lückenlos unterrichtet werden.

Den Vorsitz übernimmt ein Mitgliedstaat, der nach dem Unionsrecht in vollem Umfang durch die Rechtsinstrumente gebunden ist, die für die Entwicklung, die Errichtung, den Betrieb und die Nutzung aller EU-Informationssysteme gelten, und die sich an den Interoperabilitätskomponenten beteiligen werden.

Sämtliche Reise- und Aufenthaltskosten, die den Mitgliedern des Programmverwaltungsrats entstehen, werden von eu-LISA erstattet, wobei Artikel 10 der Geschäftsordnung von eu-LISA sinngemäß gilt. eu-LISA stellt das Sekretariat des Programmverwaltungsrats.

Die in Artikel 75 genannte Beratergruppe für Interoperabilität tritt bis zur Inbetriebnahme der Interoperabilitätskomponenten regelmäßig zusammen. Nach jeder Sitzung erstattet sie dem Programmverwaltungsrat Bericht. Sie stellt den technischen Sachverstand für die Unterstützung des Programmverwaltungsrats bei seinen Aufgaben bereit und überwacht den Stand der Vorbereitung in den Mitgliedstaaten.

Artikel 55

Verantwortlichkeiten von eu-LISA nach der Inbetriebnahme

(1) Nach der Inbetriebnahme der einzelnen Interoperabilitätskomponenten übernimmt eu-LISA die technische Verwaltung der zentralen Infrastruktur der Interoperabilitätskomponenten, einschließlich ihrer Wartung und von Technologieentwicklungen. In Zusammenarbeit mit den Mitgliedstaaten stellt eu-LISA sicher, dass vorbehaltlich einer Kosten-Nutzen-Analyse die beste verfügbare Technologie eingesetzt wird. eu-LISA ist zudem für die technische Verwaltung der in den Artikeln 6, 12, 17, 25 und 39 genannten Kommunikationsinfrastruktur verantwortlich.

Die technische Verwaltung der Interoperabilitätskomponenten umfasst alle Aufgaben und technischen Lösungen, die erforderlich sind, um die Interoperabilitätskomponenten gemäß dieser Verordnung betriebsbereit zu halten und um den Mitgliedstaaten und den Stellen der Union 24 Stunden am Tag und 7 Tage in der Woche ununterbrochene Dienste zu erbringen. Dazu gehören die Wartungsarbeiten und technischen Anpassungen, die erforderlich sind, um sicherzustellen, dass die Komponenten gemäß den technischen Spezifikationen und insbesondere bei der Reaktionszeit bei Abfragen der zentralen Infrastrukturen mit zufriedenstellender technischer Qualität arbeiten.

Alle Interoperabilitätskomponenten werden so entwickelt und verwaltet, dass ein schneller, unterbrechungsfreier, effizienter und kontrollierter Zugang, die volle, ununterbrochene Verfügbarkeit der Komponenten und der im MID, im gemeinsamen BMS und im CIR gespeicherten Daten sowie eine Reaktionszeit entsprechend den operativen Erfordernissen der mitgliedstaatlichen Behörden und der Stellen der Union sichergestellt sind.

(2) Unbeschadet des Artikels 17 des Statuts der Beamten der Europäischen Union wendet eu-LISA angemessene Regeln zur Gewährleistung der beruflichen Schweigepflicht oder einer anderen vergleichbaren Geheimhaltungspflicht auf ihre Bediensteten an, die mit in den Interoperabilitätskomponenten gespeicherten Daten arbeiten. Diese Pflicht besteht auch nach dem Ausscheiden dieser Bediensteten aus dem Amt oder Dienstverhältnis oder der Beendigung ihrer Tätigkeit weiter.

Unbeschadet des Artikels 66 hat eu-LISA keinen Zugang zu den personenbezogenen Daten, die über das ESP, den gemeinsamen BMS, den CIR und den MID verarbeitet werden.

(3) eu-LISA entwickelt und pflegt einen Mechanismus und Verfahren für die Durchführung von Qualitätskontrollen der im gemeinsamen BMS und im CIR gespeicherten Daten gemäß Artikel 37.

(4) eu-LISA nimmt zudem Aufgaben im Zusammenhang mit Schulungen zur technischen Nutzung der Interoperabilitätskomponenten wahr.

Artikel 56

Zuständigkeiten der Mitgliedstaaten

(1) Jeder Mitgliedstaat ist zuständig für

a) die Anbindung an die Kommunikationsinfrastruktur des ESP und des CIR;

b) die Integration der bestehenden nationalen Systeme und Infrastrukturen in das ESP, den CIR und den MID;

c) die Organisation, die Verwaltung, den Betrieb und die Wartung seiner bestehenden nationalen Infrastruktur und deren Anbindung an die Interoperabilitätskomponenten;

d) die Verwaltung und die Regelung des Zugangs der dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen nationalen Behörden zum ESP, zum CIR und zum MID gemäß dieser Verordnung und für die Erstellung und regelmäßige Aktualisierung eines Verzeichnisses dieser Bediensteten und ihrer Profile;

e) den Erlass der in Artikel 20 Absätze 5 und 6 genannten Gesetzgebungsmaßnahmen zur Regelung des Zugriffs auf den CIR zu Identifizierungszwecken;

f) die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29;

g) die Einhaltung der durch das Unionsrecht aufgestellten Datenqualitätsanforderungen;

h) die Einhaltung der Regeln jedes EU-Informationssystems für die Sicherheit und die Integrität personenbezogener Daten;

i) die Beseitigung etwaiger Mängel, die im Evaluierungsbericht der Kommission über die Datenqualität nach Artikel 37 Absatz 5 festgestellt wurden.

(2) Jeder Mitgliedstaat verbindet seine benannten Behörden mit dem CIR.

Artikel 57

Zuständigkeiten der ETIAS-Zentralstelle

Die ETIAS-Zentralstelle ist zuständig für

a) die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29;

b) die Prüfung der im EES, im VIS, in Eurodac und im SIS gespeicherten Daten auf Mehrfachidentitäten gemäß Artikel 69.

KAPITEL IX

Änderungen anderer Rechtsakte der Union

Artikel 58

Änderung der Verordnung (EG) Nr. 767/2008

Die Verordnung (EG) Nr. 767/2008 wird wie folgt geändert:

1. In Artikel 1 wird folgender Absatz angefügt:

„Durch die Speicherung von Identitätsdaten, Reisedokumentendaten und biometrischen Daten in dem durch Artikel 17 Absatz 1 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates (*) eingerichteten gemeinsamen Speicher für Identitätsdaten (CIR) trägt das VIS zur Erleichterung und Unterstützung bei der korrekten Identifizierung von im VIS erfassten Personen unter den Voraussetzungen und im Hinblick auf die Zwecke des Artikels 20 der genannten Verordnung bei.

(*) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27).“.

2. In Artikel 4 werden die folgenden Nummern angefügt:

„12. „VIS-Daten“: sämtliche Daten, die gemäß den Artikeln 9 bis 14 im Zentralsystem des VIS und im CIR gespeichert sind;

13. „Identitätsdaten“: die in Artikel 9 Absatz 4 Buchstaben a und aa genannten Daten;

14. „Fingerabdruckdaten“: die Daten zu den fünf Fingerabdrücken des Zeigefingers, Mittelfingers, Ringfingers, kleinen Fingers und des Daumens der rechten sowie der linken Hand, soweit vorhanden;“

3. In Artikel 5 wird folgender Absatz eingefügt:

„(1a) Der CIR enthält die in Artikel 9 Absatz 4 Buchstaben a bis c, Absatz 5 und Absatz 6 genannten Daten. Die übrigen VIS-Daten werden im Zentralsystem des VIS gespeichert.“;

4. Artikel 6 Absatz 2 erhält folgende Fassung:

„(2) Der Zugang zum VIS zum Zwecke der Datenabfrage ist ausschließlich den dazu ermächtigten Bediensteten der nationalen Behörden der einzelnen Mitgliedstaaten, die für die in den Artikeln 15 bis 22 aufgeführten Zwecke zuständig sind, und den dazu ermächtigten Bediensteten der nationalen Behörden der einzelnen Mitgliedstaaten und der Stellen der Union, die für die in den Artikeln 20 und 21 der Verordnung (EU) 2019/817 aufgeführten Zwecke zuständig sind, vorbehalten. Dieser Zugang ist auf das Maß beschränkt, in dem die Daten für die Wahrnehmung ihrer Aufgaben zu diesen Zwecken erforderlich sind, und steht in einem angemessenen Verhältnis zu den verfolgten Zielen.“

5. Artikel 9 Absatz 4 Buchstaben a bis c erhalten folgende Fassung:

„a) Nachname (Familienname), Vorname(n), Geburtsdatum, Geschlecht,

aa) Geburtsnamen (frühere(r) Nachname(n)) Geburtsort und -land, derzeitige Staatsangehörigkeit und Staatsangehörigkeit zum Zeitpunkt der Geburt;

b) Art und Nummer des Reisedokuments oder der Reisedokumente sowie der aus drei Buchstaben bestehende Code des ausstellenden Staates;

c) Datum des Ablaufs der Gültigkeitsdauer des Reisedokuments oder der Reisedokumente;

ca) Behörde, die das Reisedokument ausgestellt hat, und das Ausstellungsdatum."

Artikel 59

Änderung der Verordnung (EU) 2016/399

In Artikel 8 wird folgender Absatz eingefügt:

„(4a) Falls bei der Ein- oder Ausreise eine Abfrage der einschlägigen Datenbanken, einschließlich des Detektors für Mehrfachidentitäten, durch das Europäische Suchportal, die mit Artikel 25 Absatz 1 bzw. Artikel 6 Absatz 1 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates (*) eingerichtet wurden, eine gelbe oder rote Verknüpfung anzeigt, führt der Grenzschutzbeamte eine Abfrage im gemeinsamen Speicher für Identitätsdaten gemäß Artikel 17 Absatz 1 der genannten Verordnung oder im SIS oder in beidem durch, um die Unterschiede bei den verknüpften Identitätsdaten oder Reisedokumentendaten zu prüfen. Der Grenzschutzbeamte führt sämtliche zusätzlichen Überprüfungen durch, die für eine Entscheidung über den Status und die Farbe der Verknüpfung erforderlich sind.

Gemäß Artikel 69 Absatz 1 der Verordnung (EU) 2019/817 gilt dieser Absatz ab dem Zeitpunkt der Inbetriebnahme des Detektors für Mehrfachidentitäten nach Artikel 72 Absatz 4 der genannten Verordnung.

(*) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, der (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27).".

Artikel 60

Änderung der Verordnung (EU) 2017/2226

Die Verordnung (EU) 2017/2226 wird wie folgt geändert:

1. In Artikel 1 wird folgender Absatz angefügt:

„(3) Durch die Speicherung von Identitätsdaten, Reisedokumentendaten und biometrischen Daten in dem durch Artikel 17 Absatz 1 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates (*) eingerichteten gemeinsamen Speicher für Identitätsdaten (CIR) trägt das EES zur Erleichterung und Unterstützung bei der korrekten Identifizierung von im EES erfassten Personen unter den Voraussetzungen und im Hinblick auf die Zwecke des Artikels 20 der genannten Verordnung bei."

(*) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27).".

2. Artikel 3 Absatz 1 wird wie folgt geändert:

a) Nummer 22 erhält folgende Fassung:

„22. „EES-Daten" sämtliche Daten, die gemäß den Artikeln 15 bis 20 im Zentralsystem des EES und im CIR gespeichert sind;";

b) Folgende Nummer wird eingefügt:

„22a. „Identitätsdaten" die in Artikel 16 Absatz 1 Buchstabe a genannten Daten sowie die einschlägigen Daten nach Artikel 17 Absatz 1 und Artikel 18 Absatz 1;";

c) Folgende Nummern werden eingefügt:

„32. „ESP" das durch Artikel 6 Absatz 1 der Verordnung (EU) 2019/817 geschaffene Europäische Suchportal;

33. „CIR" den durch Artikel 17 Absatz 1 der Verordnung (EU) 2019/817 eingerichteten gemeinsamen Speicher für Identitätsdaten."

3. In Artikel 6 Absatz 1 wird folgender Buchstabe angefügt:

„j) Sicherstellung der korrekten Identifizierung von Personen."

4. Artikel 7 wird wie folgt geändert:

a) Absatz 1 wird wie folgt geändert:

i) Folgender Buchstabe wird eingefügt:

„aa) der zentralen Infrastruktur des CIR im Sinne des Artikels 17 Absatz 2 Buchstabe a der Verordnung (EU) 2019/817;"

ii) Buchstabe f erhält folgende Fassung:

„f) einer sicheren Kommunikationsinfrastruktur zwischen dem Zentralsystem des EES und den zentralen Infrastrukturen des ESP und des CIR."

b) Folgender Absatz wird eingefügt:

„(1a) Der CIR enthält die in Artikel 16 Absatz 1 Buchstaben a bis d, Artikel 17 Absatz 1 Buchstaben a, b und c und Artikel 18 Absätze 1 und 2 genannten Daten. Die übrigen EES-Daten werden im Zentralsystem des EES gespeichert."

5. In Artikel 9 wird folgender Absatz angefügt:

„(4) Der Zugang zu den im CIR gespeicherten EES-Daten ist ausschließlich dem ordnungsgemäß befugten Personal der nationalen mitgliedstaatlichen Behörden und dem ordnungsgemäß befugten Personal der Stellen der Union vorbehalten, die für die in den Artikeln 20 und 21 der Verordnung (EU) 2019/817 genannten Aufgaben zuständig sind. Dieser Zugang ist auf das Maß beschränkt, wie die Daten zur Wahrnehmung ihrer Aufgaben für diese Zwecke erforderlich sind, und steht in einem angemessenen Verhältnis zu den verfolgten Zielen."

6. Artikel 21 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Wenn es technisch nicht möglich ist, Daten in das Zentralsystem des EES oder den CIR einzugeben, oder bei einem Ausfall des Zentralsystems des EES oder des CIR werden die in den Artikeln 16 bis 20 genannten Daten vorübergehend in der einheitlichen nationalen Schnittstelle gespeichert. Ist das nicht möglich, so werden die Daten vorübergehend in einem elektronischen Format lokal gespeichert. In beiden Fällen werden die Daten in das Zentralsystem des EES oder den CIR eingegeben, sobald das technisch wieder möglich ist beziehungsweise der Ausfall behoben wurde. Die Mitgliedstaaten ergreifen entsprechende Maßnahmen und stellen die erforderliche Infrastruktur und Ausrüstung sowie die nötigen Ressourcen zur Verfügung, um zu gewährleisten, dass eine solche vorübergehende lokale Speicherung jederzeit und an allen Grenzübergangsstellen vorgenommen werden kann."

b) Absatz 2 Unterabsatz 1 erhält folgende Fassung:

„(2) Unbeschadet der Verpflichtung zur Durchführung von Grenzübertrittskontrollen gemäß der Verordnung (EU) 2016/399 nimmt die Grenzbehörde in Ausnahmesituationen, in denen die Eingabe von Daten in das Zentralsystem des EES, in den CIR oder in die einheitliche nationale Schnittstelle oder die vorübergehende lokale Speicherung in einem elektronischen Format technisch nicht möglich ist, eine manuelle Speicherung der Daten gemäß den Artikeln 16 bis 20 der vorliegenden Verordnung vor, mit Ausnahme der biometrischen Daten, und bringt einen Ein- oder Ausreisestempel im Reisedokument des Drittstaatsangehörigen an. Diese Daten werden in das Zentralsystem des EES und den CIR eingegeben, sobald das technisch möglich ist."

7. Artikel 23 wird wie folgt geändert:

a) Folgender Absatz wird eingefügt:

„(2a) Für die Zwecke der Verifizierungen gemäß Absatz 1 dieses Artikels nimmt die Grenzbehörde eine Abfrage über das ESP vor, um die Daten zu dem Drittstaatsangehörigen mit den einschlägigen Daten im EES und im VIS abzugleichen."

b) Absatz 4 Unterabsatz 1 erhält folgende Fassung:

„(4) Wenn die Suchabfrage anhand der alphanumerischen Daten nach Absatz 2 dieses Artikels ergibt, dass keine Daten über den Drittstaatsangehörigen im EES gespeichert sind, wenn die Verifizierung des Drittstaatsangehörigen gemäß Absatz 2 nicht erfolgreich ist oder wenn Zweifel an der Identität des Drittstaatsangehörigen bestehen, erhalten die Grenzbehörden Zugang zu Daten zwecks Identifizierung gemäß Artikel 27 der vorliegenden Verordnung, um ein persönliches Dossier nach Artikel 14 anzulegen oder zu aktualisieren."

8. In Artikel 32 wird folgender Absatz eingefügt:

„(1a) Wenn die benannten Behörden eine Abfrage im CIR gemäß Artikel 22 der Verordnung (EU) 2019/817 durchgeführt haben und aus der erhaltenen Antwort gemäß Artikel 22 Absatz 2 der Verordnung (EU) 2019/817 hervorgeht, dass Daten im EES gespeichert sind, dürfen sie zum Zwecke von Abfragen auf das EES zugreifen, wenn die im vorliegenden Artikel festgelegten Bedingungen erfüllt sind."

9. In Artikel 33 wird folgender Absatz eingefügt:

„(1a) Wenn Europol eine Abfrage im CIR gemäß Artikel 22 der Verordnung (EU) 2019/817 durchgeführt hat und aus der erhaltenen Antwort gemäß Artikel 22 Absatz 2 der Verordnung (EU) 2019/817 hervorgeht, dass Daten im EES gespeichert sind, darf Europol zum Zwecke von Abfragen auf das EES zugreifen, wenn die im vorliegenden Artikel festgelegten Bedingungen erfüllt sind."

10. Artikel 34 wird wie folgt geändert:

a) In den Absätzen 1 und 2 werden die Wörter „im Zentralsystem des EES" durch die Wörter „im CIR und im Zentralsystem des EES" ersetzt.

b) In Absatz 5 werden die Wörter „aus dem Zentralsystem des EES" durch die Wörter „aus dem Zentralsystem des EES und aus dem CIR" ersetzt.

11. Artikel 35 Absatz 7 erhält folgende Fassung:

„(7) Das Zentralsystem des EES und der CIR informieren alle Mitgliedstaaten unverzüglich über die Löschung von EES- oder CIR-Daten und entfernen sie gegebenenfalls aus der in Artikel 12 Absatz 3 genannten Liste der ermittelten Personen."

12. In Artikel 36 werden die Wörter „des Zentralsystems des EES" durch die Wörter „des Zentralsystem des EES und des CIR" ersetzt.

13. Artikel 37 wird wie folgt geändert:

a) Absatz 1 Unterabsatz 1 erhält folgende Fassung:

„(1) eu-LISA ist zuständig für die Entwicklung des Zentralsystems des EES, und des CIR, der einheitlichen nationalen Schnittstellen, der Kommunikationsinfrastruktur sowie des sicheren Kommunikationskanals zwischen dem Zentralsystem des EES und dem Zentralsystem des VIS. eu-LISA ist zudem zuständig für die Entwicklung des in Artikel 13 genannten Web-Dienstes gemäß den detaillierten Regeln des Artikels 13 Absatz 7 sowie den Spezifikationen und Bedingungen, die gemäß Artikel 36 Absatz 1 Buchstaben h erlassen werden, und für die Entwicklung des in Artikel 63 Absatz 2 genannten Datenregisters."

b) Absatz 3 Unterabsatz 1 erhält folgende Fassung:

„(3) eu-LISA ist zuständig für das Betriebsmanagement des Zentralsystems des EES und des CIR, der einheitlichen nationalen Schnittstellen und des sicheren Kommunikationskanals zwischen dem Zentralsystem des EES und dem Zentralsystem des VIS. In Zusammenarbeit mit den Mitgliedstaaten gewährleistet die Agentur, dass vorbehaltlich einer Kosten-Nutzen-Analyse jederzeit die beste verfügbare Technologie für das Zentralsystem des EES und des CIR, die einheitlichen nationalen Schnittstellen, die Kommunikationsinfrastruktur, den sicheren Kommunikationskanal zwischen dem Zentralsystem des EES und dem Zentralsystem des VIS, den Web-Dienst gemäß Artikel 13 und das Datenregister gemäß Artikel 63 Absatz 2 eingesetzt wird. eu-LISA ist zudem für das Betriebsmanagement der Kommunikationsinfrastruktur zwischen dem Zentralsystem des EES und den einheitlichen nationalen Schnittstellen, für den Web-Dienst gemäß Artikel 13 und das Datenregister gemäß Artikel 63 Absatz 2 zuständig."

14. In Artikel 46 Absatz 1 wird folgender Buchstabe angefügt:

„f) einen Verweis auf die Nutzung des ESP zur Abfrage des EES gemäß Artikel 7 Absatz 2 der Verordnung (EU) 2019/817."

15. Artikel 63 wird wie folgt geändert:

a) Absatz 2 erhält folgende Fassung:

„(2) Für die Zwecke von Absatz 1 dieses Artikels speichert eu-LISA die Daten nach jenem Absatz in dem zentralen Speicher für Berichte und Statistiken nach Artikel 39 der Verordnung (EU) 2019/817."

b) In Absatz 4 wird folgender Unterabsatz angefügt:

„Die täglichen Statistiken werden im zentralen Speicher für Berichte und Statistiken gespeichert."

Artikel 61

Änderung der Verordnung (EU) 2018/1240

Die Verordnung (EU) 2018/1240 wird wie folgt geändert:

1. In Artikel 1 wird folgender Absatz angefügt:

„(3) Durch die Speicherung von Identitätsdaten und Reisedokumentendaten in dem durch Artikel 17 Absatz 1 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates (*) eingerichteten gemeinsamen Speicher für Identitätsdaten (CIR) trägt das ETIAS zur Erleichterung und Unterstützung bei der korrekten Identifizierung von im ETIAS erfassten Personen unter den Voraussetzungen und im Hinblick auf die Zwecke des Artikels 20 der genannten Verordnung bei."

(*) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27)."

2. In Artikel 3 Absatz 1 werden die folgenden Nummern angefügt:

„(23) „CIR" den durch Artikel 17 Absatz 1 der Verordnung (EU) 2019/817 eingerichteten gemeinsamen Speicher für Identitätsdaten;

(24) „ESP" das durch Artikel 6 Absatz 1 der Verordnung (EU) 2019/817 geschaffene Europäische Suchportal;

(25) „ETIAS-Zentralsystem" das Zentralsystem im Sinne des Artikels 6 Absatz 2 Buchstabe a zusammen mit dem CIR, soweit der CIR die in Artikel 6 Absatz 2 Buchstabe a genannten Daten enthält;

(26) „Identitätsdaten" die in Artikel 17 Absatz 2 Buchstaben a, b und c genannten Daten;

(27) „Reisedokumentendaten" die in Artikel 17 Absatz 2 Buchstaben d und e genannten Daten sowie den aus drei Buchstaben bestehenden Code des Landes, das das Reisedokument ausgestellt hat, im Sinne des Artikels 19 Absatz 3 Buchstabe c;"

3. In Artikel 4 wird folgender Buchstabe angefügt:

„g) einen Beitrag zur korrekten Identifizierung von Personen."

4. Artikel 6 wird wie folgt geändert:

a) Absatz 2 wird wie folgt geändert:

i) Buchstabe a erhält folgende Fassung:

„a) einem Zentralsystem, das die ETIAS-Überwachungsliste nach Artikel 34 enthält;"

ii) Folgender Buchstabe wird eingefügt:

„aa) dem CIR;"

iii) Buchstabe d erhält folgende Fassung:

„d) einer sicheren Kommunikationsinfrastruktur zwischen dem Zentralsystem und den zentralen Infrastrukturen des ESP und des CIR;"

b) Folgender Absatz wird eingefügt:

„(2a) Der CIR enthält die Identitäts- und Reisedokumentendaten. Die übrigen Daten werden im Zentralsystem gespeichert."

5. Artikel 13 wird wie folgt geändert:

a) Folgender Absatz wird eingefügt:

„(4a) Der Zugang zu den im CIR gespeicherten ETIAS-Identitäts- und Reisedokumentendaten ist zudem ausschließlich den dazu ordnungsgemäß ermächtigten Bediensteten der nationalen mitgliedstaatlichen Behörden und den dazu ordnungsgemäß ermächtigten Bediensteten der Stellen der Union vorbehalten, die für die in den Artikeln 20 und 21 der Verordnung (EU) 2019/817 genannten Aufgaben zuständig sind. Dieser Zugang ist auf das Maß beschränkt, wie die Daten zur Wahrnehmung ihrer Aufgaben für diese Zwecke erforderlich sind und steht in einem angemessenen Verhältnis zu den verfolgten Zielen."

b) Absatz 5 erhält folgende Fassung:

„(5) Jeder Mitgliedstaat benennt die zuständigen nationalen Behörden gemäß den Absätzen 1, 2, 4 und 4a des vorliegenden Artikels und übermittelt unverzüglich gemäß Artikel 87 Absatz 2 eine Liste dieser Behörden an eu-LISA. In dieser Liste wird angegeben, zu welchem Zweck die dazu ordnungsgemäß ermächtigten Bediensteten jeder Behörde gemäß den Absätzen 1, 2, 4 und 4a des vorliegenden Artikels Zugriff auf die Daten im ETIAS-Informationssystem erhalten."

6. Artikel 17 Absatz 2 wird wie folgt geändert:

a) Buchstabe a erhält folgende Fassung:

„a) Nachname (Familienname), Vorname(n), Geburtsname, Geburtsdatum, Geburtsort, Geschlecht, derzeitige Staatsangehörigkeit;"

b) Folgender Buchstabe wird eingefügt:

„aa) Geburtsland, Vorname(n) der Eltern des Antragstellers;"

7. In Artikel 19 Absatz 4 werden die Wörter „Artikel 17 Absatz 2 Buchstabe a" durch die Wörter „Artikel 17 Absatz 2 Buchtstaben a und aa" ersetzt.

8. Artikel 20 wird wie folgt geändert:

a) Absatz 2 Unterabsatz 1 erhält folgende Fassung:

„(2) Das ETIAS-Zentralsystem führt über das ESP eine Abfrage durch, um die in Artikel 17 Absatz 2 Buchstaben a, aa, b, c, d, f, g, j, k und m sowie die in Artikel 17 Absatz 8 genannten einschlägigen Daten mit den vorhandenen Daten in den Dossiers, Datensätzen oder Ausschreibungen in einem Antragsdatensatz abzugleichen, die im ETIAS-Zentralsystem, im SIS, im EES, im VIS, in Eurodac, in den Europol-Daten sowie in den Interpol-SLTD und Interpol-TDAWN Datenbanken erfasst sind."

b) In Absatz 4 werden die Wörter „Artikel 17 Absatz 2 Buchstaben a, b, c, d, f, g, j, k und m" durch die Wörter „Artikel 17 Absatz 2 Buchstaben a, aa, b, c, d, f, g, j, k und m" ersetzt.

c) In Absatz 5 werden die Wörter „Artikel 17 Absatz 2 Buchstaben a, c, f, h und i " durch die Wörter „Artikel 17 Absatz 2 Buchstaben a, aa, c, f, h und i " ersetzt.

9. Artikel 23 Absatz 1 erhält folgende Fassung:

„(1) Das ETIAS-Zentralsystem führt über das ESP eine Abfrage durch, um die in Artikel 17 Absatz 2 Buchstaben a, aa, b und d genannten einschlägigen Daten mit den Daten im SIS abzugleichen, damit ermittelt werden kann, ob zu dem Antragsteller eine der folgenden Ausschreibungen vorliegt:

a) eine Ausschreibung von Vermissten;

b) eine Ausschreibung von Personen, die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht werden;

c) eine Ausschreibung von Personen zum Zwecke der verdeckten oder der gezielten Kontrolle."

10. In Artikel 52 wird folgender Absatz eingefügt:

„(1a) Wenn die benannten Behörden eine Abfrage im CIR gemäß Artikel 22 der Verordnung (EU) 2019/817 durchgeführt haben und aus der erhaltenen Antwort gemäß Artikel 22 Absatz 2 der Verordnung (EU) 2019/817 hervorgeht, dass Daten in den im ETIAS-Zentralsystem gespeicherten Antragsdatensätzen gespeichert sind, dürfen sie nach dem vorliegenden Artikel zum Zwecke von Abfragen auf die im ETIAS-Zentralsystem gespeicherten Antragsdatensätze zugreifen."

11. In Artikel 53 wird folgender Absatz eingefügt:

„(1a) Wenn Europol eine Abfrage im CIR gemäß Artikel 22 der Verordnung (EU) 2019/817 durchgeführt haben und aus der erhaltenen Antwort gemäß Artikel 22 Absatz 2 der Verordnung (EU) 2019/817 hervorgeht, dass Daten in den im ETIAS-Zentralsystem gespeicherten Antragsdatensätzen gespeichert sind, dürfen sie nach den vorliegenden Artikel zum Zwecke von Abfragen auf die im ETIAS-Zentralsystem gespeicherten Antragsdatensätze zugreifen."

12. In Artikel 65 Absatz 3 Unterabsatz 5 werden die Wörter „Artikel 17 Absatz 2 Buchstaben a, b, d, e und f" durch die Wörter „Artikel 17 Absatz 2 Buchstaben a, aa, b, d, e und f" ersetzt.

13. In Artikel 69 Absatz 1 wird folgender Buchstabe eingefügt:

„ca) gegebenenfalls einen Verweis auf die Nutzung des ESP zur Abfrage des ETIAS-Zentralsystems gemäß Artikel 7 Absatz 2 der Verordnung (EU) 2019/817;"

14. In Artikel 73 Absatz 2 werden die Wörter „des zentralen Datenregisters" durch die Wörter „des zentralen Speichers für Berichte und Statistiken nach Artikel 39 der Verordnung (EU) 2019/817, soweit dieser Daten enthält, die gemäß Artikel 84 der vorliegenden Verordnung aus dem ETIAS-Zentralsystem abgerufen wurden" ersetzt.

15. Artikel 74 Absatz 1 Unterabsatz 1 erhält folgende Fassung:

„1. Nach der Inbetriebnahme des ETIAS übernimmt eu-LISA die technische Verwaltung des ETIAS-Zentralsystems und der einheitlichen nationalen Schnittstellen. Außerdem ist die Agentur für technische Prüfungen zuständig, die zur Erstellung und Aktualisierung der ETIAS-Überprüfungsregeln erforderlich sind. In Zusammenarbeit mit den Mitgliedstaaten gewährleistet die Agentur, dass vorbehaltlich einer Kosten-Nutzen-Analyse jederzeit die beste verfügbare Technologie eingesetzt wird. eu-LISA ist zudem für die technische Verwaltung der Kommunikationsinfrastruktur zwischen dem ETIAS-Zentralsystem und den einheitlichen nationalen Schnittstellen, die öffentliche Website, die Anwendung für Mobilgeräte, den E-Mail-Dienst, den Dienst für sichere Konten, das Überprüfungsinstrument für Antragsteller, das Einwilligungsinstrument für Antragsteller, das Bewertungsinstrument für die ETIAS-Überwachungsliste, den Zugang für Beförderungsunternehmen, den Web-Dienst und die Software für die Antragsbearbeitung zuständig."

16. Artikel 84 Absatz 2 Unterabsatz 1 erhält folgende Fassung:

„(2) Für die Zwecke von Absatz 1 dieses Artikels speichert eu-LISA die Daten nach jenem Absatz in dem in Artikel 39 der Verordnung (EU) 2019/817 genannten zentralen Speicher für Berichte und Statistiken. Nach Artikel 39 Absatz 1 der genannten Verordnung werden die systemübergreifende Erhebung statistischer Daten und die Erstellung von Analyseberichten den in Absatz 1 des vorliegenden Artikels genannten Behörden ermöglichen, anpassbare Berichte und Statistiken zu erhalten, die Umsetzung der ETIAS-Überprüfungsregeln im Sinne des Artikels 33 zu unterstützen, die Bewertung der Risiken im Zusammenhang mit der Sicherheit und der illegalen Einwanderung sowie hoher Epidemierisiken zu verbessern, die Effizienz von Grenzübertrittskontrollen zu steigern und die ETIAS-Zentralstelle und die nationalen ETIAS-Stellen bei der Bearbeitung von Anträgen auf Erteilung einer Reisegenehmigung zu unterstützen."

17. Dem Artikel 84 Absatz 4 wird folgender Unterabsatz angefügt:

„Die täglichen Statistiken werden in dem in Artikel 39 der Verordnung (EU) 2019/817 genannten zentralen Speicher für Berichte und Statistiken gespeichert."

Artikel 62

Änderung der Verordnung (EU) 2018/1726

Die Verordnung (EU) 2018/1726 wird wie folgt geändert:

1. Artikel 12 erhält folgende Fassung:

„*Artikel 12*

Datenqualität

(1) Unbeschadet der Verantwortung der Mitgliedstaaten für die in die Systeme unter der betrieblichen Verantwortung der Agentur eingegebenen Daten führt die Agentur unter enger Einbeziehung ihrer Beratergruppen für alle Systeme, die in die betriebliche Zuständigkeit der Agentur fallen, Mechanismen und Verfahren für die automatische Datenqualitätskontrolle, gemeinsame Datenqualitätsindikatoren und Mindestqualitätsstandards für die Speicherung von Daten gemäß den einschlägigen Rechtsinstrumenten der für diese Informationssysteme geltenden Rechtsinstrumente und des Artikels 37 der Verordnungen (EU) 2019/817 (*) und (EU) 2019/818 des Europäischen Parlaments und des Rates (**) ein.

(2) Die Agentur richtet gemäß Artikel 39 der Verordnungen (EU) 2019/817 und (EU) 2019/818 einen zentralen Speicher für Berichte und Statistiken, der nur anonymisierte Daten enthält und für den spezifische Bestimmungen in den Rechtsinstrumenten zur Regelung der Entwicklung, der Errichtung, des Betriebs und der Nutzung von von der Agentur verwalteten IT-Großsystemen gelten, ein."

(*) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27).

(**) Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (ABl. L 135 vom 22.5.2019, S. 85)"

2. Artikel 19 Absatz 1 wird wie folgt geändert:

a) Folgender Buchstabe wird eingefügt:

„eea) die Berichte über den Stand der Entwicklung der Interoperabilitätskomponenten nach Artikel 78 Absatz 2 der Verordnung (EU) 2019/817 und Artikel 74 Absatz 2 der Verordnung (EU) 2019/818 anzunehmen."

b) Buchstabe ff erhält folgende Fassung:

„ff) die Berichte über die technische Funktionsweise des SIS nach Artikel 60 Absatz 7 der Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates (*) und Artikel 74 Absatz 8 der Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates (**), des VIS nach Artikel 50 Absatz 3 der Verordnung (EG) Nr. 767/2008 und Artikel 17 Absatz 3 des Beschlusses 2008/633/JI, des EES nach Artikel 72 Absatz 4 der Verordnung (EU) 2017/2226, des ETIAS nach Artikel 92 Absatz 4 der Verordnung (EU) 2018/1240, des ECRIS-TCN und der ECRIS-Referenzimplementierung nach Artikel 36 Absatz 8 der Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates (***) und der Interoperabilitätskomponenten nach Artikel 78 Absatz 3 der Verordnung (EU) 2019/817 und Artikel 74 Absatz 3 der Verordnung (EU) 2019/818 anzunehmen;

(*) Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006 (ABl. L 312 vom 7.12.2018, S. 14).

(**) Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56).

(***) Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, sowie zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) 2018/1726 (ABl. L 135 vom 22.5.2019, S. 1).“

c) Buchstabe hh erhält folgende Fassung:

„hh) förmliche Stellungnahmen zu den Berichten des Europäischen Datenschutzbeauftragten über seine Überprüfungen nach Artikel 56 Absatz 2 der Verordnung (EU) 2018/1861 Artikel 42 Absatz 2 der Verordnung (EG) Nr. 767/2008 und Artikel 31 Absatz 2 der Verordnung (EU) Nr. 603/2013, Artikel 56 Absatz 2 der Verordnung (EU) 2017/2226, Artikel 67 der Verordnung (EU) 2018/1240, Artikel 29 Absatz 2 der Verordnung (EU) 2019/816 und Artikel 52 der Verordnungen (EU) 2019/817 und (EU) 2019/818 anzunehmen und für geeignete Folgemaßnahmen zu diesen Überprüfungen zu sorgen;“

d) Buchstabe mm erhält folgende Fassung:

„mm) die jährliche Veröffentlichung folgender Auflistungen sicherzustellen: der Liste der zuständigen Behörden, die nach Artikel 41 Absatz 8 der Verordnung (EU) 2018/1861 und Artikel 56 Absatz 7 der Verordnung (EU) 2018/1862 berechtigt sind, die im SIS gespeicherten Daten unmittelbar abzufragen, zusammen mit einer Liste der Stellen der nationalen Systeme des SIS (N.SIS -Stellen) und der SIRENE-Büros nach Artikel 7 Absatz 3 der Verordnung (EU) 2018/1861 bzw. Artikel 7 Absatz 3 der Verordnung (EU) 2018/1862 und der Liste der zuständigen Behörden nach Artikel 65 Absatz 2 der Verordnung (EU) 2017/2226, der Liste der zuständigen Behörden nach Artikel 87 Absatz 2 der Verordnung (EU) 2018/1240, der Liste der Zentralbehörden nach Artikel 34 Absatz 2 der Verordnung (EU) 2019/816 sowie der Liste der Behörden nach Artikel 71 Absatz 1 der Verordnung (EU) 2019/817 und Artikel 67 Absatz 1 der Verordnung (EU) 2019/818.“

3. Artikel 22 Absatz 4 erhält folgende Fassung:

„(4) Europol und Eurojust können an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine SIS II betreffende Angelegenheit im Zusammenhang mit der Anwendung des Beschlusses 2007/533/JI auf der Tagesordnung steht.

Die Europäische Agentur für die Grenz- und Küstenwache kann an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine das SIS betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) 2016/1624 auf der Tagesordnung steht.

Europol kann an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine das VIS betreffende Angelegenheit im Zusammenhang mit der Anwendung des Beschlusses 2008/633/JI oder eine Eurodac betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) Nr. 603/2013 auf der Tagesordnung steht.

Europol kann an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine das EES betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) 2017/2226 oder eine ETIAS betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) 2018/1240 auf der Tagesordnung steht.

Die Europäische Agentur für die Grenz- und Küstenwache kann an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine ETIAS betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) 2018/1240 auf der Tagesordnung steht.

Eurojust, Europol und die die Europäische Staatsanwaltschaft können an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine die Verordnung (EU) 2019/816 betreffende Angelegenheit auf der Tagesordnung steht.

Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache können an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine die Verordnungen (EU) 2019/817 und (EU) 2019/818 betreffende Angelegenheit auf der Tagesordnung steht.

Der Verwaltungsrat kann weitere Personen, deren Stellungnahme von Interesse sein könnte, als Beobachter zu seinen Sitzungen einladen."

4. Artikel 24 Absatz 3 Buchstabe p erhält folgende Fassung:

„p) unbeschadet des Artikels 17 des Beamtenstatuts Geheimhaltungsvorschriften festzulegen, um Artikel 17 der Verordnung (EG) Nr. 1987/2006, Artikel 17 des Beschlusses 2007/533/JI, Artikel 26 Absatz 9 der Verordnung (EG) Nr. 767/2008, Artikel 4 Absatz 4 der Verordnung (EU) Nr. 603/2013, Artikel 37 Absatz 4 der Verordnung (EU) 2017/2226, Artikel 74 Absatz 2 der Verordnung (EU) 2018/1240, Artikel 11 Absatz 16 der Verordnung (EU) 2019/816 und Artikel 55 Absatz 2 der Verordnungen (EU) 2019/817 und (EU) 2019/818 nachzukommen;"

5. Artikel 27 wird wie folgt geändert:

a) In Absatz 1 wird folgender Buchstabe eingefügt:

„da) die Beratergruppe für Interoperabilität;"

b) Absatz 3 erhält folgende Fassung:

„(3) Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache können je einen Vertreter in die SIS-II-Beratergruppe entsenden.

Europol kann auch einen Vertreter in die VIS- und die Eurodac- sowie die EES-ETIAS-Beratergruppe entsenden.

Die Europäische Agentur für die Grenz- und Küstenwache kann auch einen Vertreter in die EES-ETIAS-Beratergruppe entsenden.

Eurojust, Europol und die Europäische Staatsanwaltschaft können je einen Vertreter in die ECRIS-TCN-Beratergruppe entsenden.

Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache können je einen Vertreter in die Beratergruppe für Interoperabilität entsenden."

Artikel 63

Änderung der Verordnung (EU) 2018/1861

Die Verordnung (EU) 2018/1861 wird wie folgt geändert:

1. In Artikel 3 werden die folgenden Nummern angefügt:

„22. „ESP" das durch Artikel 6 Absatz 1 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates (*) geschaffene Europäische Suchportal.

23. „gemeinsamer BMS" den durch Artikel 12 Absatz 1 der Verordnung (EU) 2019/817 eingerichteten gemeinsamen Dienst für den Abgleich biometrischer Daten.

24. „CIR" den durch Artikel 17 Absatz 1 der Verordnung (EU) 2019/817 eingerichteten gemeinsamen Speicher für Identitätsdaten;

25. „MID" den durch Artikel 25 Absatz 1 der Verordnung (EU) 2019/817 eingerichteten Detektor für Mehrfachidentitäten."

(*) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27)."

2. Artikel 4 wird wie folgt geändert:

a) Absatz 1 Buchstaben b und c erhalten folgende Fassung:

„b) einem nationalen System (im Folgenden „N.SIS“) in jedem einzelnen Mitgliedstaat, das aus den nationalen, mit dem zentralen SIS kommunizierenden Datensystemen besteht, einschließlich mindestens einem nationalen oder gemeinsamen Back-up-N.SIS;

c) einer Kommunikationsinfrastruktur zwischen der CS-SIS, der Back-up-CS-SIS und der NI-SIS (im Folgenden „Kommunikationsinfrastruktur“), die ein verschlüsseltes virtuelles Netz speziell für SIS-Daten und den Austausch von Daten zwischen SIRENE-Büros nach Artikel 7 Absatz 2 zur Verfügung stellt, und

d) einer sicheren Kommunikationsinfrastruktur zwischen der CS-SIS und den zentralen Infrastrukturen des ESP, des gemeinsamen BMS und des MID.“

b) Folgende Absätze werden angefügt:

„(8) Unbeschadet der Absätze 1 bis 5 können SIS-Daten auch über das ESP abgefragt werden.

(9) Unbeschadet der Absätze 1 bis 5 können SIS-Daten auch über die sichere Kommunikationsinfrastruktur gemäß Absatz 1 Buchstabe d übermittelt werden. Diese Übermittlungen sind auf das Maß beschränkt, in dem die Daten für die in der Verordnung (EU) 2019/817 genannten Zwecke erforderlich sind.“

3. In Artikel 7 wird folgender Absatz eingefügt:

„(2a) Die SIRENE-Büros gewährleisten außerdem die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29 der Verordnung (EU) 2019/817. In dem für die Erfüllung dieser Aufgabe erforderlichem Maße können die SIRENE-Büros für die in den Artikeln 21 und 26 der Verordnung (EU) 2019/817 genannten Zwecke auf die im CIR und im MID gespeicherten Daten zugreifen.“

4. Artikel 12 Absatz 1 erhält folgende Fassung:

„(1) Die Mitgliedstaaten stellen sicher, dass jeder Zugriff auf personenbezogene Daten und jeder Austausch solcher Daten mit der CS-SIS in ihrem N.SIS protokolliert werden, damit die Rechtmäßigkeit der Abfrage und der Datenverarbeitung kontrolliert, eine Eigenkontrolle durchgeführt und das einwandfreie Funktionieren des N.SIS gewährleistet werden können, sowie für die Zwecke der Datenintegrität und -sicherheit. Diese Anforderung gilt nicht für die in Artikel 4 Absatz 6 Buchstaben a, b und c genannten automatisierten Prozesse.

Die Mitgliedstaaten stellen sicher, dass jeder Zugriff auf personenbezogene Daten über das ESP ebenfalls protokolliert wird, damit die Rechtmäßigkeit der Abfrage und die Rechtmäßigkeit der Datenverarbeitung kontrolliert und eine Eigenkontrolle durchgeführt sowie die Datenintegrität und -sicherheit gewährleistet werden kann.“

5. In Artikel 34 Absatz 1 wird folgender Buchstabe angefügt:

„g) die Verifizierung verschiedener Identitäten und die Bekämpfung von Identitätsbetrug gemäß Kapitel V der Verordnung (EU) 2019/817.“

6. Artikel 60 Absatz 6 erhält folgende Fassung:

„(6) „Für die Zwecke des Artikels 15 Absatz 4 und der Absätze 3, 4 und 5 des vorliegenden Artikels speichert eu-LISA die Daten nach Artikel 15 Absatz 4 und nach Absatz 3 des vorliegenden Artikels in dem in Artikel 39 der Verordnung (EU) 2019/817 genannten zentralen Speicher für Berichte und Statistiken; dies darf eine Identifizierung einzelner Personen nicht ermöglichen.

eu-LISA gestattet der Kommission und den Stellen nach Absatz 5 des vorliegenden Artikels, maßgeschneiderte Berichte und Statistiken zu erhalten. Auf Anfrage gewährt eu-LISA den Mitgliedstaaten, der Kommission, Europol und der Europäischen Agentur für die Grenz- und Küstenwache Zugang zu dem zentralen Speicher für Berichte und Statistiken gemäß Artikel 39 der Verordnung (EU) 2019/817.“

Artikel 64

Änderung der Entscheidung 2004/512/EG

Artikel 1 Absatz 2 der Entscheidung 2004/512/EG zur Einrichtung des Visa-Informationssystems (VIS) erhält folgende Fassung:

„(2) Das Visa-Informationssystem verfügt über eine zentralisierte Architektur und besteht aus

a) der zentralen Infrastruktur des gemeinsamen Speichers für Identitätsdaten (CIR) im Sinne des Artikels 17 Absatz 2 Buchstabe a der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates (*);

b) einem zentralen Informationssystem, nachstehend „das zentrale Visa-Informationssystem“ (CS-VIS) genannt,

c) einer Schnittstelle in jedem Mitgliedstaat, nachstehend „die nationale Schnittstelle“ (NI-VIS) genannt, um die Verbindung zu der betreffenden zentralen nationalen Behörde des jeweiligen Mitgliedstaats herzustellen,

d) einer Kommunikationsinfrastruktur zwischen dem zentralen Visa-Informationssystem und den nationalen Schnittstellen,

e) einem sicheren Kommunikationskanal zwischen dem Zentralsystem des EES und dem CS-VIS,

f) einer sicheren Kommunikationsinfrastruktur zwischen dem Zentralsystem des VIS und der zentralen Infrastruktur des durch Artikel 6 Absatz 1 der Verordnung (EU) 2019/817 geschaffenen Europäischen Suchportals und des durch Artikel 17 Absatz 1 der Verordnung (EU) 2019/817 geschaffenen gemeinsamen Speichers für Identitätsdaten.“

(*) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27).“

Artikel 65

Änderung des Beschlusses 2008/633/JI

Der Beschluss 2008/633/JI wird wie folgt geändert:

1. In Artikel 5 wird folgender Absatz eingefügt:

„(1a) Wenn die benannten Behörden eine Abfrage im gemeinsamen Speicher für Identitätsdaten (CIR) gemäß Artikel 22 der Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates (*) durchgeführt haben und aus der erhaltenen Antwort gemäß Artikel 22 Absatz 2 der genannten Verordnung hervorgeht, dass Daten im VIS gespeichert sind, dürfen sie zum Zwecke von Abfragen auf das VIS zugreifen, wenn die in dem vorliegenden Artikel festgelegten Zugangsbedingungen erfüllt sind.“

(*) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27).“

2. In Artikel 7 wird folgender Absatz eingefügt:

„(1a) Wenn Europol eine Abfrage im CIR gemäß Artikel 22 der Verordnung (EU) 2019/817 durchgeführt hat und aus der erhaltenen Antwort gemäß Artikel 22 Absatz 2 der genannten Verordnung hervorgeht, dass Daten im VIS gespeichert sind, darf Europol zum Zwecke von Abfragen auf das VIS zugreifen, wenn die in dem vorliegenden Artikel festgelegten Zugangsbedingungen erfüllt sind.“

KAPITEL X

Schlussbestimmungen

Artikel 66

Berichte und Statistiken

(1) Die folgenden Daten zum ESP dürfen von dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen mitgliedstaatlichen Behörden, der Kommission und von eu-LISA ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden:

a) Zahl der Abfragen pro ESP-Nutzerprofil;

b) Zahl der Abfragen in den einzelnen Interpol-Datenbanken.

Die Identifizierung einzelner Personen auf der Grundlage der Daten darf nicht möglich sein.

(2) Die folgenden Daten zum CIR dürfen von dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen mitgliedstaatlichen Behörden, der Kommission und von eu-LISA ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden:

a) Zahl der Abfragen für die Zwecke der Artikel 20, 21 und 22;

b) Staatsangehörigkeit, Geschlecht und Geburtsjahr der Person;

c) Art des Reisedokuments und aus drei Buchstaben bestehender Code des ausstellenden Staates;

d) Zahl der Abfragen mit und ohne biometrische Daten.

Die Identifizierung einzelner Personen auf der Grundlage der Daten darf nicht möglich sein.

(3) Die folgenden Daten zum MID dürfen von dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen mitgliedstaatlichen Behörden, der Kommission und von eu-LISA ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden:

a) Zahl der Abfragen mit und ohne biometrische Daten;

b) Zahl der Verknüpfungen, aufgeschlüsselt nach Verknüpfungsart, und die EU-Informationssysteme, die die verknüpften Daten enthalten;

c) Zeitraum, für den eine gelbe und rote Verknüpfung im System verblieben ist.

Die Identifizierung einzelner Personen auf der Grundlage der Daten darf nicht möglich sein.

(4) Die ordnungsgemäß ermächtigten Bediensteten der Europäischen Agentur für die Grenz- und Küstenwache können zur Durchführung von Risikoanalysen und Schwachstellenbeurteilungen nach den Artikeln 11 und 13 der Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates ([40]) auf die in den Absätzen 1, 2 und 3 des vorliegenden Artikels genannten Daten zugreifen.

(5) Die ordnungsgemäß ermächtigten Bediensteten von Europol können auf die in den Absätzen 2 und 3 des vorliegenden Artikels genannten Daten zur Durchführung von strategischen, themenbezogenen und operativen Analysen nach Artikel 18 Absatz 2 Buchstaben b und c der Verordnung (EU) 2016/794 zugreifen.

(6) Für die Zwecke der Absätze 1, 2 und 3 speichert eu-LISA die in diesen Absätzen genannten Daten im CRRS. Die Identifizierung einzelner Personen auf der Grundlage der im CRRS enthaltenen Daten darf nicht möglich sein, jedoch müssen die Daten den in den Absätzen 1, 2 und 3 genannten Behörden die Möglichkeit geben, anpassbare Berichte und Statistiken abzurufen, um die Effizienz von Grenzübertrittskontrollen zu steigern, Behörden bei der Bearbeitung von Visumanträgen zu unterstützen und eine faktengestützte Gestaltung der Migrations- und Sicherheitspolitik der Union zu fördern.

(7) Auf Anfrage werden der Agentur der Europäischen Union für Grundrechte relevante Informationen von der Kommission zur Verfügung gestellt, damit sie die Auswirkungen dieser Verordnung auf die Grundrechte bewerten kann.

Artikel 67

Übergangszeitraum für die Nutzung des Europäischen Suchportals

(1) Während eines Zeitraums von zwei Jahren nach dem Datum der Inbetriebnahme des ESP gelten die Pflichten nach Artikel 7 Absätze 2 und 4 nicht, und die Benutzung des ESP ist fakultativ.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 73 einen delegierten Rechtsakt zur Änderung dieser Verordnung zu erlassen, durch die der in Absatz 1 des vorliegenden Artikels genannte Zeitraum einmal um höchstens ein Jahr verlängert wird, wenn eine Bewertung der Umsetzung des ESP ergeben hat, dass eine solche Verlängerung insbesondere angesichts der Auswirkungen, die die Inbetriebnahme des ESP auf die Organisation und die Dauer der Grenzübertrittskontrollen hätte, notwendig ist.

Artikel 68

Übergangszeit für die Bestimmungen über den Zugriff auf den gemeinsamen Speicher für Identitätsdaten zu Zwecken der Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten

Artikel 22, Artikel 60 Nummern 8 und 9, Artikel 61 Nummern 10 und 11 und Artikel 65 gelten ab dem Tag der Inbetriebnahme des CIR gemäß Artikel 72 Absatz 3.

([40]) Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates vom 14. September 2016 über die Europäische Grenz- und Küstenwache und zur Änderung der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Verordnung (EG) Nr. 863/2007 des Europäischen Parlaments und des Rates, der Verordnung (EG) Nr. 2007/2004 des Rates und der Entscheidung des Rates 2005/267/EG (ABl. L 251 vom 16.9.2016, S. 1).

Artikel 69

Übergangszeitraum für die Prüfung auf Mehrfachidentitäten

(1) Für die Dauer eines Jahres, nachdem eu-LISA den Abschluss des Tests des MID nach Artikel 72 Absatz 4 Buchstabe b mitgeteilt hat, und vor der Inbetriebnahme des MID ist die ETIAS-Zentralstelle für die Prüfung der im EES, im VIS, in Eurodac und im SIS gespeicherten Daten auf Mehrfachidentitäten zuständig. Die Prüfungen auf Mehrfachidentitäten werden ausschließlich anhand biometrischer Daten durchgeführt.

(2) Wenn die Abfrage eine oder mehrere Übereinstimmungen ergibt und die Identitätsdaten der verknüpften Dateien gleich oder ähnlich sind, wird eine weiße Verknüpfung nach Artikel 33 erstellt.

Wenn die Abfrage eine oder mehrere Übereinstimmungen ergibt und die Identitätsdaten der verknüpften Dateien nicht als ähnlich angesehen werden können, wird eine gelbe Verknüpfung nach Artikel 30 erstellt, und das Verfahren nach Artikel 29 gelangt zur Anwendung.

Wenn mehrere Übereinstimmungen gemeldet werden, wird zwischen jedem Datenelement, das zu einer Übereinstimmung geführt hat, eine Verknüpfung erstellt.

(3) Wenn eine gelbe Verknüpfung erstellt wird, gewährt der MID der ETIAS-Zentralstelle Zugang zu den in den verschiedenen EU-Informationssystemen gespeicherten Identitätsdaten.

(4) Wenn eine Verknüpfung zu einer Ausschreibung im SIS erstellt wird, bei der es sich nicht um eine Ausschreibung nach Artikel 3 der Verordnung (EU) 2018/1860, den Artikeln 24 und 25 der Verordnung (EU) 2018/1861 oder Artikel 38 der Verordnung (EU) 2018/1862 handelt, gewährt der MID dem SIRENE-Büro des Mitgliedstaats, der die Ausschreibung eingegeben hat, Zugang zu den in den verschiedenen Informationssystemen gespeicherten Identitätsdaten.

(5) Die ETIAS-Zentralstelle beziehungsweise - in den in Absatz 4 dieses Artikels genannten Fällen - das SIRENE-Büro des Mitgliedstaats, der die Ausschreibung eingegeben hat, greift auf die in der Identitätsbestätigungsdatei enthaltenen Daten zu, prüft die verschiedenen Identitäten, aktualisiert die Verknüpfung gemäß den Artikeln 31, 32 und 33 und fügt diese zur Identitätsbestätigungsdatei hinzu.

(6) Die ETIAS-Zentralstelle unterrichtet die Kommission gemäß Artikel 71 Absatz 3 erst, sobald alle gelben Verknüpfungen manuell überprüft und deren Status entweder in grüne, weiße oder rote Verknüpfungen aktualisiert worden sind.

(7) Die Mitgliedstaaten unterstützen die ETIAS-Zentralstelle gegebenenfalls bei der Prüfung auf Mehrfachidentitäten gemäß diesem Artikel.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 73 einen delegierten Rechtsakt zur Änderung dieser Verordnung zu erlassen, durch die der in Absatz 1 dieses Artikels genannte Zeitraum um sechs Monate verlängert wird, wobei zweimal eine weitere Verlängerung um jeweils sechs Monate möglich ist. Eine solche Verlängerung wird nur gewährt, wenn eine Bewertung der geschätzten Zeit für den Abschluss der Prüfung auf Mehrfachidentitäten nach diesem Artikel ergibt, dass die Prüfung auf Mehrfachidentitäten aus Gründen, auf die die ETIAS-Zentralstelle keinen Einfluss hat, nicht vor Ende des Zeitraums gemäß Absatz 1 dieses Artikels oder einer laufenden Verlängerung abgeschlossen werden kann, und dass keine korrektiven Maßnahmen getroffen werden können. Die Bewertung wird spätestens drei Monate vor Auslaufen eines solchen Zeitraums oder einer solchen laufenden Verlängerung durchgeführt.

Artikel 70

Kosten

(1) Die Kosten im Zusammenhang mit der Einrichtung und dem Betrieb des ESP, des gemeinsamen BMS, des CIR und des MID gehen zulasten des Gesamthaushaltsplans der Union.

(2) Die Kosten im Zusammenhang mit der Integration der bestehenden nationalen Infrastrukturen, deren Anbindung an die einheitlichen nationalen Schnittstellen und dem Hosting der einheitlichen nationalen Schnittstellen gehen zulasten des Gesamthaushaltsplans der Union.

Hiervon ausgenommen sind die Kosten für

a) die Projektverwaltungsstelle der Mitgliedstaaten (Sitzungen, Dienstreisen, Büroräume),

b) das Hosting nationaler IT-Systeme (Räume, Implementierung, Stromversorgung, Kühlung),

c) den Betrieb nationaler IT-Systeme (Betreiber- und Unterstützungsverträge),

d) Konzipierung, Entwicklung, Implementierung, Betrieb und Wartung nationaler Kommunikationsnetze.

(3) Unbeschadet der Zuweisung weiterer Finanzierungsmittel für diesen Zweck aus anderen Quellen des Gesamthaushaltsplans der Union werden 32 077 000 EUR aus der Dotation von 791 000 000 EUR mobilisiert, die gemäß Artikel 5 Absatz 5 Buchstabe b der Verordnung (EU) Nr. 515/2014 vorgesehen ist, um die Kosten für die Umsetzung dieser Verordnung abzudecken, wie das in den Absätzen 1 und 2 des vorliegenden Artikels vorgesehen ist.

(4) Von der in Absatz 3 genannten Dotation werden 22 861 000 EUR eu-LISA, 9 072 000 EUR Europol und 144 000 EUR der Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) zugewiesen, um diese Stellen bei der Wahrnehmung ihrer jeweiligen Aufgaben nach dieser Verordnung zu unterstützen. Die Umsetzung erfolgt im Wege der indirekten Mittelverwaltung.

(5) Die Kosten im Zusammenhang mit den benannten Behörden gehen zulasten der jeweils benennenden Mitgliedstaaten. Die Kosten für die Anbindung jeder benannten Behörde an den CIR gehen zulasten der einzelnen Mitgliedstaaten.

Die Kosten, die Europol entstehen, einschließlich der Kosten für die Anbindung an den CIR, gehen zulasten von Europol.

Artikel 71

Mitteilungen

(1) Die Mitgliedstaaten teilen eu-LISA die Behörden gemäß den Artikeln 7, 20, 21 und 26 mit, die das ESP, den CIR beziehungsweise den MID nutzen dürfen oder Zugang zum ESP, zum CIR beziehungsweise zum MID haben.

Innerhalb von drei Monaten nach dem Datum, an dem die einzelnen Interoperabilitätskomponenten gemäß Artikel 72 ihren Betrieb aufgenommen haben, wird eine konsolidierte Liste dieser Behörden im *Amtsblatt der Europäischen Union* veröffentlicht. Werden Änderungen an der Liste vorgenommen, so veröffentlicht eu-LISA einmal im Jahr eine aktualisierte konsolidierte Liste.

(2) eu-LISA teilt der Kommission den erfolgreichen Abschluss der Tests nach Artikel 72 Absatz 1 Buchstabe b, Absatz 2 Buchstabe b, Absatz 3 Buchstabe b, Absatz 4 Buchstabe b. Absatz 5 Buchstabe b und Absatz 6 Buchstabe b mit.

(3) Die ETIAS-Zentralstelle teilt der Kommission den erfolgreichen Abschluss des Übergangszeitraums nach Artikel 69 mit.

(4) Die Kommission stellt den Mitgliedstaaten und der Öffentlichkeit die gemäß Absatz 1 mitgeteilten Informationen über eine fortlaufend aktualisierte öffentliche Website bereit.

Artikel 72

Aufnahme des Betriebs

(1) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt das ESP seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 8 Absatz 2, Artikel 9 Absatz 7 und Artikel 43 Absatz 5 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des ESP festgestellt, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden und den Stellen der Union, die das ESP nutzen können, durchgeführt hat;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 8 Absatz 1 validiert und der Kommission mitgeteilt;

Abfragen der Interpol-Datenbanken über das ESP erfolgen erst, wenn die technischen Vorkehrungen die Einhaltung des Artikels 9 Absatz 5 ermöglichen. Eine Unmöglichkeit der Einhaltung von Artikel 9 Absatz 5 führt dazu, dass eine Abfrage der Interpol-Datenbanken über das ESP unterbleibt, die Aufnahme des Betriebs des ESP wird aber nicht verzögert.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(2) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt der gemeinsame BMS seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 13 Absatz 5 und Artikel 43 Absatz 5 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des gemeinsamen BMS, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden durchgeführt hat, festgestellt;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 13 validiert und der Kommission mitgeteilt;

d) eu-LISA hat den erfolgreichen Abschluss des Tests nach Absatz 5 Buchstabe b festgestellt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(3) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt der CIR seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 43 Absatz 5 und Artikel 78 Absatz 10 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des CIR, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden durchgeführt hat, festgestellt;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 18 validiert und der Kommission mitgeteilt;

d) eu-LISA hat den erfolgreichen Abschluss des Tests nach Absatz 5 Buchstabe b festgestellt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(4) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt der MID seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 28 Absätze 5 und 7, Artikel 32 Absatz 6, Artikel 33 Absatz 5, Artikel 43 Absatz 5 und Artikel 49 Absatz 6 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des MID, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden und der ETIAS-Zentralstelle durchgeführt hat, festgestellt;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 34 validiert und der Kommission mitgeteilt;

d) die ETIAS-Zentralstelle hat ihre Mitteilung an die Kommission gemäß Artikel 71 Absatz 3 getätigt;

e) eu-LISA hat den erfolgreichen Abschluss der Tests nach Absatz 1 Buchstabe b, Absatz 2 Buchstabe b, Absatz 3 Buchstabe b und Absatz 5 Buchstabe b festgestellt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(5) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, ab welchem Zeitpunkt die Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie die gemeinsamen Datenqualitätsindikatoren und die Mindestqualitätsstandards für Daten zu nutzen sind, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 37 Absatz 4 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests der Mechanismen und Verfahren für die automatische Datenqualitätskontrolle, der gemeinsamen Datenqualitätsindikatoren und der Mindestqualitätsstandards für Daten, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden durchgeführt hat, festgestellt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(6) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt der CRRS seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 39 Absatz 5 und Artikel 43 Absatz 5 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des CRRS, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden durchgeführt hat, festgestellt;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 39 validiert und der Kommission mitgeteilt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(7) Die Kommission unterrichtet das Europäische Parlament und den Rat über die Ergebnisse der gemäß Absatz 1 Buchstabe b, Absatz 2 Buchstabe b, Absatz 3 Buchstabe b, Absatz 4 Buchstabe b, Absatz 5 Buchstabe b und Absatz 6 Buchstabe b durchgeführten Tests.

(8) Die Mitgliedstaaten, die ETIAS-Zentraleinheit und Europol beginnen mit der Nutzung der einzelnen Interoperabilitätskomponenten ab dem von der Kommission gemäß den Absätzen 1, 2, 3 bzw. 4 jeweils festgelegten Zeitpunkt.

Artikel 73

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 28 Absatz 5, Artikel 39 Absatz 5, Artikel 49 Absatz 6, Artikel 67 Absatz 2 und Artikel 69 Absatz 8 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 11. Juni 2019 übertragen. Die Kommission erstellt spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

(3) Die Befugnisübertragung gemäß Artikel 28 Absatz 5, Artikel 39 Absatz 5, Artikel 49 Absatz 6, Artikel 67 Absatz 2 und Artikel 69 Absatz 8 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnisse. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen, im Einklang mit den in der Interinstitutionellen Vereinbarung über bessere Rechtsetzung vom 13. April 2016 festgelegten Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 28 Absatz 5, Artikel 39 Absatz 5, Artikel 49 Absatz 6, Artikel 67 Absatz 2 und Artikel 69 Absatz 8 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 74

Ausschussverfahren

1. Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

2. Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

Gibt der Ausschuss keine Stellungnahme ab, so erlässt die Kommission den Durchführungsrechtsakt nicht, und Artikel 5 Absatz 4 Unterabsatz 3 der Verordnung (EU) Nr. 182/2011 findet Anwendung.

Artikel 75

Beratergruppe

eu-LISA setzt eine Beratergruppe für Interoperabilität ein. Während der Konzept- und Entwicklungsphase der Interoperabilitätskomponenten findet Artikel 54 Absätze 4, 5 und 6 Anwendung.

Artikel 76

Schulung

eu-LISA nimmt Aufgaben im Zusammenhang mit Schulungen in der technischen Nutzung der Interoperabilitätskomponenten gemäß der Verordnung (EU) 2018/1726 wahr.

Die mitgliedstaatlichen Behörden und die Stellen der Union stellen ihren Bediensteten, die zur Verarbeitung von Daten mittels der Interoperabilitätskomponenten ermächtigt sind, ein geeignetes Schulungsprogramm zu Datensicherheit, Datenqualität, Datenschutzvorschriften, Datenverarbeitungsverfahren und den Informationspflichten gemäß Artikel 32 Absatz 4, Artikel 33 Absatz 4 und Artikel 47 zur Verfügung.

Gegebenenfalls werden auf Unionsebene gemeinsame Schulungskurse zu diesen Themen organisiert, um die Zusammenarbeit und den Austausch bewährter Verfahren zwischen den Bediensteten der mitgliedstaatlichen Behörden und der Stellen der Union, die zur Verarbeitung von Daten mittels der Interoperabilitätskomponenten ermächtigt sind, zu verbessern. Besonderes Augenmerk gilt dem Verfahren der Prüfung auf Mehrfachidentitäten, einschließlich der manuellen Verifizierung verschiedener Identitäten und der damit einhergehenden Notwendigkeit, angemessene Schutzmechanismen für Grundrechte beizubehalten.

Artikel 77

Handbuch

Die Kommission stellt in enger Zusammenarbeit mit den Mitgliedstaaten, eu-LISA und anderen zuständigen Stellen der Union ein Handbuch für die Umsetzung und den Betrieb der Interoperabilitätskomponenten zur Verfügung. Das Handbuch enthält technische und operative Leitlinien, Empfehlungen und bewährte Verfahren. Die Kommission nimmt dieses Handbuch in Form einer Empfehlung an.

Artikel 78

Überwachung und Bewertung

(1) eu-LISA stellt sicher, dass Verfahren vorhanden sind, um die Entwicklung der Interoperabilitätskomponenten und ihrer Anbindung an die einheitliche nationale Schnittstelle anhand von Zielen für Planung und Kosten sowie die Funktionsweise der Interoperabilitätskomponenten anhand von Zielen für die technische Leistung, Kostenwirksamkeit, Sicherheit und Qualität des Dienstes zu überwachen.

(2) Bis zum 12. Dezember 2019 und danach alle sechs Monate während der Entwicklungsphase der Interoperabilitätskomponenten übermittelt eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über den Stand der Entwicklung der Interoperabilitätskomponenten und ihrer Anbindung an die einheitliche nationale Schnittstelle. Sobald die Entwicklung abgeschlossen ist, wird dem Europäischen Parlament und dem Rat ein Bericht übermittelt, in dem detailliert dargelegt wird, wie die Ziele, insbesondere für die Planung und die Kosten, erreicht wurden, und in dem etwaige Abweichungen begründet werden.

(3) Vier Jahre nach Inbetriebnahme der einzelnen Interoperabilitätskomponenten gemäß Artikel 72 und danach alle vier Jahre übermittelt eu-LISA dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise der Interoperabilitätskomponenten einschließlich ihrer Sicherheit.

(4) Ferner erstellt die Kommission ein Jahr nach jedem Bericht von eu-LISA eine Gesamtbewertung der Interoperabilitätskomponenten, die Folgendes beinhaltet:

a) eine Beurteilung der Anwendung dieser Verordnung;

b) eine Analyse der Ergebnisse, gemessen an den Zielen dieser Verordnung und ihrer Auswirkungen auf die Grundrechte, einschließlich insbesondere einer Bewertung der Auswirkungen der Interoperabilitätskomponenten auf das Recht auf Nichtdiskriminierung;

c) eine Bewertung des Funktionierens des Web-Portals, einschließlich Zahlen zur Nutzung des Web-Portals und der Zahl von Anfragen, denen entsprochen wurde;

d) eine Beurteilung, ob die grundlegenden Prinzipien der Interoperabilitätskomponenten weiterhin Gültigkeit haben;

e) eine Beurteilung der Sicherheit der Interoperabilitätskomponenten;

f) eine Beurteilung der Nutzung des CIR zu Zwecken der Identifizierung;

g) eine Beurteilung der Nutzung des CIR zu Zwecken der Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten;

h) eine Beurteilung etwaiger Auswirkungen, auch etwaiger unverhältnismäßiger Auswirkungen auf den Verkehrsfluss an den Grenzübergangsstellen, und der Auswirkungen auf den Gesamthaushalt der Union;

i) eine Beurteilung der Abfrage der Interpol-Datenbanken über das ESP, einschließlich Informationen über die Zahl der Übereinstimmungen in Interpol-Datenbanken und Informationen zu allen festgestellten Problemen.

Die Gesamtbewertung gemäß Unterabsatz 1 dieses Absatzes schließt etwaige erforderliche Empfehlungen ein. Die Kommission übermittelt den Bewertungsbericht dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten und der Agentur der Europäischen Union für Grundrechte.

(5) Die Kommission übermittelt dem Europäischen Parlament und dem Rat bis zum 12. Juni 2020 und danach jedes Jahr, bis die Durchführungsrechtsakte der Kommission nach Artikel 72 erlassen wurden, einen Bericht über den Stand der Vorbereitungen für die vollumfängliche Durchführung dieser Verordnung. Dieser Bericht enthält auch genaue Angaben über die angefallenen Kosten und Informationen über sämtliche Risiken, die Auswirkungen auf die Gesamtkosten haben könnten.

(6) Zwei Jahre nach Inbetriebnahme des MID gemäß Artikel 72 Absatz 4 nimmt die Kommission eine Analyse der Auswirkungen des MID auf das Recht auf Nichtdiskriminierung vor. Nach diesem ersten Bericht ist die Analyse der Auswirkungen des MID auf das Recht auf Nichtdiskriminierung Teil der in Absatz 4 Buchstabe b des vorliegenden Artikels genannten Analyse.

(7) Die Mitgliedstaaten und Europol stellen eu-LISA und der Kommission die für die Ausarbeitung der Berichte nach den Absätzen 3 bis 6 erforderlichen Informationen zur Verfügung. Diese Informationen dürfen nicht zu einer Beeinträchtigung der Arbeitsverfahren führen oder Angaben enthalten, die Rückschlüsse auf Quellen, Bedienstete oder Ermittlungen der benannten Behörden ermöglichen.

(8) eu-LISA stellt der Kommission die Informationen zur Verfügung, die zur Durchführung der in Absatz 4 genannten Gesamtbewertung erforderlich sind.

(9) Die Mitgliedstaaten und Europol erstellen unter Einhaltung der nationalen Rechtsvorschriften über die Veröffentlichung von sensiblen Informationen und unbeschadet der erforderlichen Einschränkungen zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass keine nationalen Ermittlungen beeinträchtigt werden, Jahresberichte über die Wirksamkeit des Zugangs zu im CIR gespeicherten Daten zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten; diese Berichte enthalten Informationen und Statistiken über

a) den genauen Zweck der Abfrage, einschließlich über die Art der terroristischen Straftaten oder sonstigen schweren Straftaten;

b) die hinreichenden Anhaltspunkte für den begründeten Verdacht, dass ein Verdächtige, ein Täter oder ein Opfer unter die Verordnung (EU) 2017/2226, die Verordnung (EG) Nr. 767/2008 oder die Verordnung (EU) 2018/1240 fällt;

c) die Zahl der Anträge auf Zugang zum CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten;

d) die Anzahl und die Art von Fällen, in denen die Identität einer Person festgestellt werden konnte;

e) die Notwendigkeit für und die Anwendung des Dringlichkeitsverfahrens in Ausnahmefällen, darunter in Fällen, in denen bei der nachträglichen Überprüfung durch die zentrale Zugangsstelle festgestellt wurde, dass das Dringlichkeitsverfahren nicht gerechtfertigt war.

Die Jahresberichte der Mitgliedstaaten und von Europol werden der Kommission bis zum 30. Juni des Folgejahres vorgelegt.

(10) Zur Verwaltung von Anträgen der Nutzer auf Zugang gemäß Artikel 22 und zur Erleichterung der Erhebung der in den Absätzen 7 und 9 des vorliegenden Artikels aufgeführten Informationen für die Zwecke der Erstellung der in jenen Absätzen genannten Berichte und Statistiken wird den Mitgliedstaaten eine technische Lösung bereitgestellt. Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Spezifikationen der technischen Lösung. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 74 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 79

Inkrafttreten und Anwendbarkeit

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Die Bestimmungen dieser Verordnung über das ESP gelten ab dem von der Kommission gemäß Artikel 72 Absatz 1 bestimmtem Zeitpunkt.

Die Bestimmungen dieser Verordnung über den gemeinsamen BMS gelten ab dem von der Kommission gemäß Artikel 72 Absatz 2 bestimmtem Zeitpunkt.

Die Bestimmungen dieser Verordnung über den CIR gelten ab dem von der Kommission gemäß Artikel 72 Absatz 3 bestimmtem Zeitpunkt.

Die Bestimmungen dieser Verordnung über den MID gelten ab dem von der Kommission gemäß Artikel 72 Absatz 4 bestimmtem Zeitpunkt.

Die Bestimmungen dieser Verordnung über die Mechanismen und Verfahren für die automatische Datenqualitätskontrolle, die gemeinsamen Datenqualitätsindikatoren und die Mindestqualitätsstandards gelten ab dem von der Kommission gemäß Artikel 72 Absatz 5 bestimmtem Zeitpunkt.

Die Bestimmungen dieser Verordnung über den CRRS gelten ab dem von der Kommission gemäß Artikel 72 Absatz 6 bestimmtem Zeitpunkt.

Die Artikel 6, 12, 17, 25, 38, 42, 54, 56, 57, 70, 71, 73, 74, 75, 77 und Artikel 78 Absatz 1 gelten ab dem 11. Juni 2019.

Diese Verordnung gilt für Eurodac ab dem Tag der Anwendbarkeit der Neufassung der Verordnung (EU) Nr. 603/2013.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß den Verträgen unmittelbar in den Mitgliedstaaten.

Geschehen zu Brüssel am 20. Mai 2019.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
A. TAJANI	G. CIAMBA

VERORDNUNG (EU) 2019/818 DES EUROPÄISCHEN PARLAMENTS UND DES RATES

vom 20. Mai 2019

zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816

DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —

gestützt auf den Vertrag zur Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16 Absatz 2, Artikel 74, Artikel 78 Absatz 2 Buchstabe e, Artikel 79 Absatz 2 Buchstabe c, Artikel 82 Absatz 1 Buchstabe d, Artikel 85 Absatz 1, Artikel 87 Absatz 2 Buchstabe a und Artikel 88 Absatz 2,

auf Vorschlag der Europäischen Kommission,

nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,

nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ([1]),

nach Anhörung des Ausschusses der Regionen,

gemäß dem ordentlichen Gesetzgebungsverfahren ([2]),

in Erwägung nachstehender Gründe:

(1) Die Kommission hat in ihrer Mitteilung „Solidere und intelligentere Informationssysteme für das Grenzmanagement und mehr Sicherheit“ vom 6. April 2016 darauf hingewiesen, dass die Datenverwaltungsarchitektur der Union im Bereich der Grenzkontrolle und der Sicherheit verbessert werden muss. Durch die Mitteilung wurde ein Prozess eingeleitet, durch den die Interoperabilität zwischen den EU-Informationssystemen für die Bereiche Sicherheit, Grenzmanagement und Migrationssteuerung hergestellt werden soll, um die strukturellen, die Arbeit der nationalen Behörden behindernden Mängel dieser Systeme zu beheben und sicherzustellen, dass Grenzschutzbeamten, Zollbehörden, Polizeibediensteten und Justizbehörden die erforderlichen Informationen zur Verfügung stehen.

(2) Der Rat hat in seinem Fahrplan zur Verbesserung des Informationsaustauschs und des Informationsmanagements einschließlich von Interoperabilitätslösungen im Bereich Justiz und Inneres vom 6. Juni 2016 verschiedene rechtliche, technische und praktische Probleme auf dem Weg zur Interoperabilität der EU-Informationssysteme aufgezeigt und Lösungen dafür gefordert.

(3) Das Europäische Parlament hat in seiner Entschließung vom 6. Juli 2016 zu den strategischen Prioritäten für das Arbeitsprogramm der Kommission für 2017 ([3]) dazu aufgefordert, Vorschläge für die Verbesserung und Weiterentwicklung von bestehenden EU-Informationssystemen, die Schließung von Informationslücken und Wege hin zur Interoperabilität sowie Vorschläge für einen zwingend vorgeschriebenen Informationsaustausch auf EU-Ebene mit den erforderlichen Datenschutzvorkehrungen vorzulegen.

(4) In seinen Schlussfolgerungen vom 15. Dezember 2016 forderte der Europäische Rat, dass die Arbeiten zur Gewährleistung der Interoperabilität von EU-Informationssystemen und -Datenbanken fortgesetzt werden.

(5) Die hochrangige Expertengruppe für Informationssysteme und Interoperabilität kam in ihrem Abschlussbericht vom 11. Mai 2017 zu dem Schluss, dass es notwendig und technisch möglich ist, auf Lösungen für die Interoperabilität hinzuarbeiten, und dass diese Interoperabilität grundsätzlich sowohl operative Verbesserungen bewirken als auch gemäß den Datenschutzvorschriften umgesetzt werden könnte.

(6) Gemäß ihrer Mitteilung vom 6. April 2016 und mit den Erkenntnissen und Empfehlungen der Expertengruppe für Informationssysteme und Interoperabilität hat die Kommission in ihrer Mitteilung „Auf dem Weg zu einer wirksamen und echten Sicherheitsunion — Siebter Fortschrittsbericht“ vom 16. Mai 2017 ein neues Konzept für die Verwaltung grenz-, sicherheits- und migrationsrelevanter Daten vorgestellt, durch das unter uneingeschränkter Achtung der Grundrechte die Interoperabilität aller EU-Informationssysteme für die Bereiche Sicherheit, Grenzmanagement und Migrationssteuerung gewährleistet wäre.

([1]) ABl. C 283 vom 10.8.2018, S. 48.
([2]) Standpunkt des Europäischen Parlaments vom 16. April 2019 (noch nicht im Amtsblatt veröffentlicht) und Beschluss des Rates vom 14. Mai 2019.
([3]) ABl. C 101 vom 16.3.2018, S. 116.

(7) Der Rat hat die Kommission in seinen Schlussfolgerungen vom 9. Juni 2017 zum weiteren Vorgehen zur Verbesserung des Informationsaustauschs und zur Sicherstellung der Interoperabilität der EU-Informationssysteme aufgefordert, die von der hochrangigen Expertengruppe vorgeschlagenen Lösungen zur Verbesserung der Interoperabilität umzusetzen.

(8) In seinen Schlussfolgerungen vom 23. Juni 2017 hat der Europäische Rat hat die Notwendigkeit einer besseren Interoperabilität zwischen den Datenbanken betont und die Kommission aufgefordert, so rasch wie möglich Gesetzgebungsvorschläge auf der Grundlage der Vorschläge der hochrangigen Expertengruppe für Informationssysteme und Interoperabilität vorzubereiten.

(9) Um die Effektivität und Effizienz von Kontrollen an den Außengrenzen zu verbessern und um zur Verhinderung und Bekämpfung illegaler Einwanderung und zur Gewährleistung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Union einschließlich der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der inneren Sicherheit im Hoheitsgebiet der Mitgliedstaaten beizutragen, um die Umsetzung der gemeinsamen Visumpolitik zu verbessern, um die Prüfung von Anträgen auf internationalen Schutz zu unterstützen, um zur Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten beizutragen, um die Identifizierung von unbekannten Personen, die sich nicht ausweisen können, oder von nicht identifizierten sterblichen Überresten bei Naturkatastrophen, Unfällen oder terroristischen Anschlägen zu erleichtern, und damit das Vertrauen der Öffentlichkeit in das Migrations- und Asylsystem der Union, die Sicherheitsmaßnahmen der Union und die Fähigkeit der Union zum Schutz der Außengrenzen erhalten bleibt, sollte Interoperabilität zwischen den EU-Informationssystemen — d. h. zwischen dem Einreise-/Ausreisesystem (im Folgenden „EES“), dem Visa-Informationssystem (im Folgenden „VIS“), dem Europäischen Reiseinformations- und -genehmigungssystem (im Folgenden „ETIAS“), Eurodac, dem Schengener Informationssystem (im Folgenden „SIS“) und dem Europäischen Strafregisterinformationssystem für Drittstaatsangehörige (im Folgenden „ECRIS-TCN“) — hergestellt werden, damit diese EU-Informationssysteme und ihre Daten einander ergänzen können, wobei die Grundrechte des Einzelnen, insbesondere das Recht auf Schutz personenbezogener Daten, zu achten sind. Als Interoperabilitätskomponenten sollten zu diesem Zweck ein Europäisches Suchportal (European search portal — ESP), ein gemeinsamer Dienst für den Abgleich biometrischer Daten (biometric matching service — im Folgenden „BMS“), ein gemeinsamer Speicher für Identitätsdaten (common identity repository — im Folgenden „CIR“) und ein Detektor für Mehrfachidentitäten (multiple-identity detector — im Folgenden „MID“) geschaffen werden.

(10) Die EU-Informationssysteme sollten so miteinander verbunden werden, dass sie einander ergänzen, damit die korrekte Identifizierung von Personen, einschließlich unbekannter Personen, die sich nicht ausweisen können, oder nicht identifizierter sterblicher Überreste, vereinfacht und ein Beitrag zur Bekämpfung von Identitätsbetrug geleistet wird, damit die Datenqualitätsanforderungen der verschiedenen EU-Informationssysteme verbessert und harmonisiert werden, damit den Mitgliedstaaten die technische und die operative Umsetzung der EU-Informationssysteme erleichtert wird, damit die für die einzelnen EU-Informationssysteme geltenden Sicherheitsvorkehrungen für die Sicherheit und den Schutz der Daten verschärft werden und damit der Zugang zum EES, zum VIS, zum ETIAS und zu Eurodac zum Zwecke der Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten einheitlich geregelt wird und die Zwecke des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN gefördert werden.

(11) Die Interoperabilitätskomponenten sollten sich auf das EES, das VIS, das ETIAS, Eurodac, das SIS und das ECRIS-TCN erstrecken. Zudem sollten sie sich auf Europol-Daten erstrecken, jedoch nur, soweit es erforderlich ist, um Europol-Daten gleichzeitig zu diesen EU-Informationssystemen abfragen zu können.

(12) Die Interoperabilitätskomponenten sollten die personenbezogenen Daten von Personen verarbeiten, deren personenbezogene Daten in den zugrundeliegenden EU-Informationssystemen und von Europol verarbeitet werden.

(13) Das ESP sollte mit dem Ziel geschaffen werden, den mitgliedstaatlichen Behörden und den Stellen der Union mit technischen Mitteln einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu den EU-Informationssystemen, den Europol-Daten und den Datenbanken der Internationalen kriminalpolizeilichen Organisation (Interpol) nach Maßgabe ihrer Zugangsrechte zu erleichtern, soweit das notwendig ist, um ihren Aufgaben nachzukommen. Das ESP sollte auch geschaffen werden, um die Ziele des EES, des VIS, des ETIAS, von Eurodac, des SIS, des ECRIS-TCN und der Europol-Daten zu unterstützen. Das ESP sollte die gleichzeitige, parallel erfolgende Abfrage aller einschlägigen EU-Informationssysteme sowie der Europol-Daten und der Interpol-Datenbanken ermöglichen und auf diese Weise als einzige Schnittstelle (im Folgenden „Fenster“) für eine nahtlose, unter vollständiger Wahrung der Zugangskontroll- und Datenschutzanforderungen der zugrundeliegenden Systeme erfolgende Abfrage der erforderlichen Informationen in den verschiedenen Zentralsystemen dienen.

(14) Das ESP sollte so konzipiert werden, dass bei der Abfrage der Interpol-Datenbanken sichergestellt ist, dass die von einem Nutzer des ESP für eine Abfrage eingegebenen Daten nicht mit den Eigentümern der Interpol-Daten geteilt werden. Durch die Konzipierung des ESP sollte auch sichergestellt werden, dass die Interpol-Datenbanken nur gemäß dem anwendbaren Unionsrecht und nationalen Recht abgefragt werden.

(15) Nutzer des ESP, die gemäß der Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates ([4]) Zugang zu Europol-Daten haben, sollten die Europol-Daten gleichzeitig zu den EU-Informationssystem, zu denen sie Zugang haben, abfragen dürfen. Jedwede sich an eine solche Anfrage anschließende Datenverarbeitung sollte in Übereinstimmung mit der Verordnung (EU) 2016/794 stehen und insbesondere etwaigen vom Datenlieferanten festgelegten Zugangs- oder Nutzungsbeschränkungen Rechnung tragen.

(16) Das ESP sollte so konzipiert und konfiguriert werden, dass nur solche Datenabfragen zugelassen werden, die Daten verwenden, die sich auf Personen oder Reisedokumente beziehen, die in einem EU-Informationssystem, in den Europol-Daten oder in den Interpol-Datenbanken vorhanden sind.

(17) Um den systematischen Rückgriff auf die einschlägigen *EU*-Informationssysteme zu ermöglichen, sollte das ESP für die Abfrage des CIR, des EES, des VIS, des ETIAS, von Eurodac und des ECRIS-TCN verwendet werden. Gleichwohl sollte eine nationale Verbindung zu den verschiedenen EU-Informationssystemen aufrechterhalten werden, um eine technische Ausweichmöglichkeit zu haben. Das ESP sollte zudem von den Stellen der Union dazu genutzt werden, das zentrale SIS in Übereinstimmung mit ihren jeweiligen Zugangsrechten abzufragen und ihren Aufgaben nachzukommen. Das ESP sollte als zusätzliches, die bestehenden spezifischen Schnittstellen ergänzendes Werkzeug für die Abfrage des zentralen SIS, von Europol-Daten und der Interpol-Datenbanken dienen.

(18) Biometrische Daten wie Fingerabdrücke und Gesichtsbilder sind einmalig und daher für die Personenidentifizierung weit zuverlässiger als alphanumerische Daten. Der gemeinsame BMS sollte als technisches Hilfsmittel für die Verstärkung und Vereinfachung der Funktion der einschlägigen EU-Informationssysteme und der anderen Interoperabilitätskomponenten dienen. Der Hauptzweck des gemeinsamen BMS sollte darin bestehen, die Identifizierung einer in mehreren Datenbanken erfassten Person unter Rückgriff auf eine einzige technologische Komponente (anstatt auf mehrere Komponenten) anhand eines systemübergreifenden Abgleichs ihrer biometrischen Daten zu ermöglichen. Der gemeinsame BMS sollte zur Sicherheit beitragen und finanzielle, wartungstechnische und operative Vorteile bieten. Alle automatischen Systeme zur Identifizierung von Fingerabdrücken einschließlich der derzeit für Eurodac, das VIS und das SIS eingesetzten Systeme arbeiten mit biometrischen Merkmalsdaten (im Folgenden „Templates“), die aus einem Merkmalsauszug konkreter biometrischer Proben generiert werden. Sämtliche biometrischen Templates dieser Art sollten im gemeinsamen BMS an einem einzigen Ort logisch voneinander getrennt nach den Informationssystemen, aus denen sie stammen, zusammengefasst und gespeichert werden, um dadurch den systemübergreifenden Vergleich anhand biometrischer Templates zu vereinfachen und Größenvorteile bei der Entwicklung und Wartung der EU-Zentralsysteme zu ermöglichen.

(19) Die im gemeinsamen BMS gespeicherten biometrischen Templates sollten aus Daten bestehen, die aus einem Merkmalsauszug konkreter biometrischer Proben stammen und die in einer Weise generiert werden, dass eine Umkehr des Auszugsprozesses nicht möglich ist. Biometrische Templates sollten zwar aus biometrischen Daten generiert werden, aber es sollte nicht möglich sein, dieselben biometrischen Daten aus den biometrischen Templates zu erhalten. Da Daten in Form von Handballenabdrücken und DNA-Profile nur im SIS gespeichert werden und gemäß den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit nicht zum Abgleich mit Daten in anderen Informationssystemen genutzt werden können, sollten im gemeinsamen BMS keine DNA-Profile oder biometrische Templates gespeichert werden, die aus Daten in Form von Handballenabdrücken generiert wurden.

(20) Bei biometrischen Daten handelt es sich um sensible personenbezogene Daten. Mit dieser Verordnung sollten die Grundlagen und die Garantien für die Verarbeitung derartiger Daten für die Zwecke einer eindeutigen Identifizierung betroffener Personen festgelegt werden.

(21) Das EES, das VIS, das ETIAS, Eurodac und das ECRIS-TAN erfordern eine genaue Identifizierung der Personen, deren personenbezogene Daten in diesen Systemen erfasst werden. Der CIR sollte daher die korrekte Identifizierung der in diesen Systemen erfassten Personen erleichtern.

(22) Die in diesen EU-Informationssystemen gespeicherten personenbezogenen Daten können sich auf unterschiedliche oder unvollständige Identitäten ein und derselben Person beziehen. Die Mitgliedstaaten verfügen über effiziente Möglichkeiten zur Identifizierung ihrer Staatsangehörigen oder von als dauerhaft in ihrem Hoheitsgebiet wohnhaft gemeldeten Personen. Die Interoperabilität zwischen den EU-Informationssystemen sollte zur korrekten Identifizierung der in diesen Systemen erfassten Personen beitragen. Im CIR sollten jene personenbezogenen Daten von in den Systemen erfassten Personen gespeichert werden, die für eine genauere Identifizierung der Personen erforderlich sind, einschließlich deren Identitäts-, Reisedokumenten- und biometrische Daten — und das unabhängig davon, in welchem System die betreffenden Daten ursprünglich erfasst wurden. Im CIR sollten ausschließlich solche personenbezogenen Daten gespeichert werden, die für eine genaue Identitätsprüfung unbedingt erforderlich sind. Die im CIR erfassten personenbezogenen Daten sollten nicht länger als für die Zwecke der zugrunde liegenden Systeme unbedingt erforderlich gespeichert und entsprechend den Bestimmungen über die logische Trennung dieser Daten automatisch gelöscht werden, wenn die betreffenden Daten in den zugrunde liegenden Systemen gelöscht werden.

([4]) Verordnung (EU) 2016/794 des Europäischen Parlaments und des Rates vom 11. Mai 2016 über die Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) und zur Ersetzung und Aufhebung der Beschlüsse 2009/371/JI, 2009/934/JI, 2009/935/JI, 2009/936/JI und 2009/968/JI des Rates (ABl. L 135 vom 24.5.2016, S. 53).

(23) Ein neuer Datenverarbeitungsvorgang, der darin besteht, dass derartige Daten anstatt in den einzelnen separaten Systemen im CIR gespeichert werden, ist erforderlich, um eine genauere Identifizierung durch den automatischen Ver- und Abgleich solcher Daten zu ermöglichen. Die Tatsache, dass die Identitäts-, die Reisedokumenten- und die biometrischen Daten im CIR gespeichert werden, sollte die Datenverarbeitung für die Zwecke des EES, des VIS, des ETIAS, von Eurodac oder des ECRIS-TCN in keiner Weise behindern, da der CIR eine neue gemeinsame Komponente dieser zugrunde liegenden Systeme darstellen sollte.

(24) Daher ist es notwendig, im CIR für jede im EES, im VIS, im ETIAS, in Eurodac oder im ECRIS-TCN erfasste Person eine individuelle Datei anzulegen, um die bezweckte korrekte Personenidentifizierung im Schengen-Raum zu ermöglichen und den MID zu unterstützen, durch den zugleich die Identitätsprüfung von Bona-fide-Reisenden vereinfacht und Identitätsbetrug bekämpft werden soll. In der individuellen Datei sollten alle mit einer Person verknüpften Identitätsangaben an einem Ort gespeichert und den ordnungsgemäß ermächtigten Endnutzern zugänglich gemacht werden.

(25) Der CIR sollte auf diese Weise den Zugang von Behörden, die für die Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten zuständig sind, zu jenen EU-Informationssystemen, die nicht ausschließlich für die Zwecke der Verhinderung, Aufdeckung oder Untersuchung schwerer Straftaten errichtet wurden, erleichtern und vereinheitlichen.

(26) Der CIR sollte eine gemeinsame Speichereinheit für Identitäts-, Reisedokumenten- und biometrische Daten von im EES, im VIS, im ETIAS in Eurodac und im ECRIS-TCN erfassten Personen einschließen. Sie sollte Teil der technischen Architektur dieser Systeme sein und als gemeinsame Komponente von ihnen für die Speicherung und Abfrage der von ihnen verarbeiteten Identitäts-, Reisedokumenten- und biometrischen Daten dienen.

(27) Sämtliche Datensätze im CIR sollten logisch voneinander getrennt werden, indem jeder Datensatz durch eine entsprechende Kennzeichnung automatisch mit dem Namen des zugrunde liegenden Systems, zu dem er gehört, verknüpft wird. Die Zugangskontrollen des CIR sollten nach Maßgabe dieser Kennzeichnungen darüber entscheiden, ob Zugang zu den betreffenden Datensätzen gewährt wird.

(28) Wenn die Polizeibehörde eines Mitgliedstaats eine Person wegen des Fehlens eines Reisedokuments oder eines anderen glaubwürdigen Dokuments zum Nachweis der Identität dieser Person nicht identifizieren kann oder wenn Zweifel an den von dieser Person vorgelegten Identitätsdaten, der Echtheit des Reisedokuments oder der Identität des Inhabers bestehen oder wenn die Person zu einer Zusammenarbeit nicht in der Lage ist oder sie verweigert, sollte diese Polizeibehörde eine Abfrage im CIR vornehmen können, um die Person zu identifizieren. Für diese Zwecke sollten die Polizeibehörden Fingerabdrücke unter Einsatz von Livescanner-Techniken für Fingerabdrücke abnehmen, vorausgesetzt, dass das Verfahren im Beisein dieser Person eingeleitet wurde. Solche Abfragen im CIR sollten nicht für die Zwecke der Identifizierung Minderjähriger unter zwölf Jahren zulässig sein, es sei denn, das erfolgt zum Wohl des Kindes.

(29) Falls die biometrischen Daten einer Person nicht verwendet werden können oder eine Abfrage anhand dieser Daten nicht erfolgreich ist, sollte die Abfrage mittels Identitätsdaten der Person in Verbindung mit Reisedokumentendaten vorgenommen werden. Falls die Abfrage ergibt, dass im CIR Daten über diese Person gespeichert sind, sollten die mitgliedstaatlichen Behörden Zugriff auf den CIR erhalten, um in die Identitäts- und Reisedokumentendaten dieser Person Einsicht nehmen zu können, ohne dass das CIR ihnen in irgendeiner Form anzeigt, aus welchem EU-Informationssystem die Daten stammen.

(30) Die Mitgliedstaaten sollten nationale gesetzgeberische Maßnahmen zur Benennung der zu Identitätsprüfungen unter Rückgriff auf den CIR befugten Behörden und zur Festlegung der Verfahren, Bedingungen und Kriterien für derartige Prüfungen erlassen, die in Übereinstimmung mit dem Grundsatz der Verhältnismäßigkeit erfolgen sollten. Insbesondere sollte durch nationales Recht die Befugnis eingeführt werden, biometrische Daten einer Person in Gegenwart eines Bediensteten dieser Behörden während einer Identitätsprüfung zu erheben.

(31) Durch diese Verordnung sollte zudem eine neue Möglichkeit zur Vereinheitlichung des Zugangs der von den Mitgliedstaaten benannten Behörden, die für die Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten zuständig sind, und von Europol zu im EES, im VIS, im ETIAS oder in Eurodac gespeicherten Daten, die über Identitäts- oder Reisedokumentendaten hinausgehen, eingeführt werden. Derartige Daten können nämlich im Einzelfall für die Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten benötigt werden, wenn vernünftige Gründe für die Annahme vorliegen, dass deren Abfrage zur Verhinderung, Aufdeckung oder Untersuchung der terroristischen Straftaten oder sonstigen schweren Straftaten beitragen würde, insbesondere, wenn ein Verdacht besteht, dass der Verdächtige, der Täter oder das Opfer einer terroristischen Straftat oder einer sonstigen schweren Straftat eine Person ist, deren Daten im EES, im VIS, im ETIAS oder in Eurodac gespeichert sind.

(32) Die Frage eines vollständigen Zugangs zu in den EU-Informationssystemen gespeicherten Daten, die für die Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erforderlich sind und über die im CIR gespeicherten Identitätsdaten und Reisedokumentendaten hinausgehen, sollte weiterhin durch die einschlägigen Rechtsinstrumente geregelt werden. Die benannten Behörden, die für die Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten und sonstiger schwerer Straftaten zuständig sind, und Europol wissen nicht im Voraus, in welchen EU-Informationssystemen Daten zu den Personen, die Gegenstand ihrer Ermittlungen sind, gespeichert sind. Das führt zu Verzögerungen und Ineffizienz. Den von der benannten Behörde ermächtigten Endnutzern sollte daher angezeigt werden, in welchem dieser EU-Informationssysteme die dem Ergebnis einer Abfrage entsprechenden Daten gespeichert sind. Zu diesem Zweck sollte im Anschluss an die automatische Prüfung auf Vorliegen einer Übereinstimmung das betreffende Informationssystem automatisch gekennzeichnet werden (im Folgenden „Übereinstimmungskennzeichnungsfunktion").

(33) In diesem Zusammenhang sollte ein Treffer des CIR nicht als Grund oder Anlass interpretiert oder verwendet werden, Schlussfolgerungen über eine Person zu ziehen oder Maßnahmen gegen diese zu ergreifen, sondern sollte nur zum Zwecke einer Beantragung des Zugangs zu den zugrunde liegenden EU-Informationssystemen genutzt werden, vorbehaltlich der Bedingungen und Verfahren, die in den entsprechenden Rechtsinstrumenten zur Regelung dieses Zugangs festgelegt wurden. Jeder derartige Zugangsantrag sollte Kapitel VII dieser Verordnung und gegebenenfalls der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates ([5]), der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates ([6]) oder der Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates ([7]) unterliegen.

(34) Als allgemeine Regel sollten die benannten Behörden oder Europol in dem Fall, dass eine Übereinstimmungskennzeichnung anzeigt, dass Daten in Eurodac gespeichert sind, uneingeschränkten Zugang zu mindestens einem der betreffenden EU-Informationssysteme beantragen. Wenn ein solcher uneingeschränkter Zugang ausnahmsweise nicht beantragt wird, beispielsweise weil die benannten Behörden oder Europol die Daten bereits über andere Mittel erhalten haben oder der Erhalt der Daten nach nationalem Recht nicht mehr zulässig ist, sollte die Begründung dafür, dass kein Zugang beantragt wird, aufgezeichnet werden.

(35) In den Protokollen der Datenabfragen im CIR sollte der Zweck der jeweiligen Abfragen aufgeführt werden. Bei Datenabfragen, die nach dem zweistufigen Datenabfrageverfahren erfolgen, sollte in den Protokollen das Aktenzeichen des betreffenden nationalen Untersuchungsdossiers bzw. Falls angegeben werden, um dadurch anzuzeigen, dass die Abfrage zu den Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erfolgte.

(36) Von den benannten Behörden und von Europol vorgenommene Datenabfragen im CIR, die zu dem Zweck erfolgen, eine Antwort in Form einer Übereinstimmungskennzeichnung zu erhalten, in der angezeigt wird, dass die betreffenden Daten im EES, im VIS, im ETIAS oder in Eurodac gespeichert sind, erfordern eine automatische Verarbeitung personenbezogener Daten. Bei einer Übereinstimmungskennzeichnung sollten außer dem Hinweis, dass Daten der betroffenen Person in einem der EU-Informationssysteme gespeichert sind, keine personenbezogenen Daten der betroffenen Person angezeigt werden. Ermächtigte Endnutzer sollten keine die betroffene Person beschwerenden Entscheidungen treffen, die sich allein auf das Vorliegen einer Übereinstimmungskennzeichnung gründen. Der Zugriff des Endnutzers auf eine Übereinstimmungskennzeichnung würde somit einen nur sehr begrenzten Eingriff in das Recht der betroffenen Person auf Schutz ihrer personenbezogenen Daten bedeuten; gleichzeitig würde es den benannten Behörden und Europol aber erlauben, effizientere Anträge auf Zugang zu personenbezogenen Daten zu stellen.

(37) Der MID sollte mit dem Ziel geschaffen werden, das Funktionieren des CIR und die Ziele des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN zu unterstützen. Damit die jeweiligen Ziele dieser EU-Informationssysteme wirksam umgesetzt werden können, ist es erforderlich, dass die Personen, deren personenbezogene Daten in diesen Systemen gespeichert werden, genau identifiziert werden.

(38) Um die Ziele von EU-Informationssystemen besser zu erreichen, sollte es den auf diese Systeme zurückgreifenden Behörden möglich sein, die Identität von Personen, deren Daten in den einzelnen Systemen gespeichert sind, mit hinreichender Zuverlässigkeit zu verifizieren. Bei den in einem gegebenen System gespeicherten Identitätsdaten oder Reisedokumentendaten kann es sich um unbewusst gemachte Falschangaben, unvollständige Angaben oder

([5]) Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016, S. 1).

([6]) Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89).

([7]) Verordnung (EU) 2018/1725 des Europäischen Parlaments und des Rates vom 23. Oktober 2018 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe, Einrichtungen und sonstigen Stellen der Union, zum freien Datenverkehr und zur Aufhebung der Verordnung (EG) Nr. 45/2001 und des Beschlusses Nr. 1247/2002/EG (ABl. L 295 vom 21.11.2018, S. 39).

bewusst gemachte Falschangaben handeln, und mit den bisher bestehenden Möglichkeiten können unbewusst falsche, unvollständige oder bewusst falsche Identitätsdaten und Reisedokumentendaten nicht mittels Vergleich mit in anderen Systemen gespeicherten Daten als solche erkannt werden. Um hier Abhilfe zu schaffen, ist es erforderlich, auf Unionsebene ein technisches Instrument einzuführen, das die genaue Identifizierung von Personen zu diesen Zwecken ermöglicht.

(39) Der MID sollte Verknüpfungen zwischen den in den einzelnen EU-Informationssystemen erfassten Daten herstellen und speichern, damit Mehrfachidentitäten aufgedeckt werden können, um zugleich die Identitätsprüfung von Bona-fide-Reisenden zu vereinfachen und Identitätsbetrug zu bekämpfen. Der MID sollte ausschließlich Verknüpfungen zwischen Daten über Personen enthalten, die in mehr als einem EU-Informationssystem erfasst sind. Die verknüpften Daten sollten strikt auf die Daten begrenzt werden, die erforderlich sind, um zu verifizieren, ob eine Person in gerechtfertigter Weise oder in ungerechtfertigter Weise mit mehreren Identitäten in unterschiedlichen Systemen erfasst ist, oder um zu überprüfen, ob es sich bei zwei Personen mit ähnlichen Identitätsdaten um ein und dieselbe Person handelt. Die durch das ESP und den gemeinsamen BMS erfolgende Datenverarbeitung zum Zwecke der systemübergreifenden Verknüpfung von individuellen Dateien sollte ein absolutes Mindestmaß nicht überschreiten und zu diesem Zweck auf eine Prüfung auf Mehrfachidentitäten begrenzt werden, welche dann erfolgen sollte, wenn neue Daten in eines der Systeme, die Daten im CIR hinterlegt haben, oder in das SIS aufgenommen werden. Der MID sollte Absicherungen gegen eine mögliche Diskriminierung von Personen mit legalen Mehrfachidentitäten und gegen derartige Personen beschwerende Entscheidungen einschließen.

(40) Diese Verordnung sieht die Einführung neuer Datenverarbeitungsverfahren vor, die die korrekte Identifizierung der betroffenen Personen ermöglichen sollen. Diese Verfahren bedeuten einen Eingriff in die nach den Artikeln 7 und 8 der Charta der Grundrechte der Europäischen Union geschützten Grundrechte dieser Personen. Da die EU-Informationssysteme nur im Falle einer korrekten Identifizierung der betroffenen Personen wirksam genutzt werden können, ist ein solcher Eingriff aufgrund der Ziele, zu deren Erreichung die einzelnen EU-Informationssysteme errichtet wurden (wirksames Management der Unionsgrenzen, Wahrung der inneren Sicherheit der Union und wirksame Umsetzung der Asyl- und der Visapolitik der Union), gerechtfertigt.

(41) Das ESP und der gemeinsame BMS sollten immer dann, wenn von einer nationalen Behörde oder von einer Stelle der Union neue Datensätze angelegt oder hochgeladen werden, einen Datenabgleich über die im CIR und im SIS erfassten Personen vornehmen. Der Datenabgleich sollte automatisch erfolgen. Um etwaige Verknüpfungen anhand biometrischer Daten aufzudecken, sollten der CIR und das SIS auf den gemeinsamen BMS zurückgreifen. Um etwaige Verknüpfungen anhand alphanumerischer Daten aufzudecken, sollten der CIR und das SIS auf das ESP zurückgreifen. Der CIR und das SIS sollten dazu geeignet sein, die gleichen oder ähnlichen Daten über eine in verschiedenen Systemen erfasste Person zu ermitteln. Werden solche Daten ermittelt, sollte eine Verknüpfung angelegt werden, die anzeigt, dass es sich jeweils um ein und dieselbe Person handelt. Der CIR und das SIS sollten so konfiguriert werden, dass etwaige kleinere Transliterations- oder Buchstabierfehler in einer Weise erkannt werden, dass sie keine nicht gerechtfertigten beschwerenden Maßnahmen für die betreffende Person zur Folge haben.

(42) Die nationale Behörde oder die Stelle der Union, die die Daten in das betreffende EU-Informationssystem eingegeben hat, sollte diese Verknüpfungen bestätigen bzw. entsprechend ändern. Die nationale Behörde oder die Stelle der Union sollte auf die im CIR oder im SIS und im MID gespeicherten Daten für die Zwecke einer manuellen Verifizierung verschiedener Identitäten zugreifen dürfen.

(43) Eine manuelle Verifizierung verschiedener Identitäten sollte von der Behörde vorgenommen werden, die die Daten eingegeben bzw. aktualisiert hat, welche zu der Übereinstimmung geführt haben, aufgrund deren eine Verknüpfung zu in einem anderen EU-Informationssystem gespeicherten Daten angelegt wurde. Die für die manuelle Verifizierung von verschiedenen Identitäten zuständige Behörde sollte jeweils prüfen, ob Mehrfachidentitäten vorliegen, die sich in gerechtfertigter Weise oder in ungerechtfertigter Weise auf dieselbe Person beziehen. Eine derartige Prüfung sollte nach Möglichkeit im Beisein der betreffenden Person erfolgen und bei Bedarf unter Anforderung zusätzlicher Präzisierungen oder Auskünfte. Die Prüfung sollte unverzüglich und in Übereinstimmung mit den im Unionsrecht und im nationalen Recht festgelegten Anforderungen an die Genauigkeit von Informationen vorgenommen werden.

(44) Für über das SIS erhaltene/generierte Verknüpfungen, die sich auf Ausschreibungen von Personen zum Zwecke der Übergabe- oder Auslieferungshaft, von Vermissten oder Schutzbedürftigen oder von im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesuchten Personen oder auf Personenausschreibungen zum Zwecke der verdeckten Kontrolle, Ermittlungsanfragen oder gezielten Kontrollen beziehen, sollte das SIRENE-Büro des Mitgliedstaats, der die Ausschreibung vorgenommen hat, für die manuelle Verifizierung verschiedener Identitäten zuständig sein. Diese Kategorien von SIS-Ausschreibungen haben einen sensiblen Charakter und sollten daher

nicht notwendigerweise gegenüber den Behörden, die die damit verknüpften Daten in einem anderen EU-Informationssystem eingegeben oder aktualisiert haben, offengelegt werden. Durch die Erstellung einer Verknüpfung zu SIS-Daten sollte den nach Maßgabe der Verordnungen des Europäischen Parlaments und des Rates (EU) 2018/1860 ([8]), (EU) 2018/1861 ([9]) und (EU) 2018/1862 ([10]) zu ergreifenden Maßnahmen nicht vorgegriffen werden.

(45) Die Erstellung solcher Verknüpfungen erfordert Transparenz gegenüber den betroffenen Einzelpersonen. Um die Umsetzung der notwendigen Schutzmaßnahmen gemäß dem anwendbaren Datenschutzrecht der Union zu erleichtern, sollten Einzelpersonen, die Gegenstand einer roten Verknüpfung oder einer weißen Verknüpfung nach einer manuellen Verifizierung verschiedener Identitäten sind, unbeschadet der Einschränkungen zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass nationale Ermittlungen nicht beeinträchtigt werden, schriftlich unterrichtet werden. Diese Einzelpersonen sollten eine einmalige Kennnummer erhalten, anhand derer sie die Behörde finden können, an die sie sich zwecks Ausübung ihrer Rechte wenden sollten.

(46) Wird eine gelbe Verknüpfung erstellt, so sollte die Behörde, die für die manuelle Verifizierung verschiedener Identitäten zuständig ist, Zugang zum MID erhalten. Wenn eine rote Verknüpfung besteht, so sollten mitgliedstaatliche Behörden oder Stellen der Union, die Zugang zu mindestens einem im CIR enthaltenen EU-Informationssystem oder zum SIS haben, Zugang zum MID erhalten. Eine rote Verknüpfung sollte anzeigen, dass eine Person in ungerechtfertigter Weise verschiedene Identitäten benutzt oder dass eine Person die Identität eines anderen benutzt.

(47) Besteht eine weiße oder eine grüne Verknüpfung zwischen Daten aus zwei EU-Informationssystemen, so sollten mitgliedstaatlichen Behörden und Stellen der Union Zugang zum MID erhalten, wenn die jeweilige Behörde oder Stelle Zugang zu beiden Informationssystemen hat. Ein solcher Zugang sollte zu dem alleinigen Zweck gewährt werden, dieser Behörde oder Stelle zu ermöglichen, potenzielle Fälle zu ermitteln, in denen die Daten im MID, CIR und SIS falsch verknüpft oder unter Verstoß gegen diese Verordnung verarbeitet wurden, und Maßnahmen zu ergreifen, um die Situation zu bereinigen und die Verknüpfung zu aktualisieren oder zu löschen.

(48) Die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) sollte automatische Datenqualitätskontrollmechanismen und gemeinsame Datenqualitätsindikatoren konzipieren. Ferner sollte eu-LISA dafür verantwortlich sein, Kapazitäten für die zentrale Überwachung der Datenqualität zu entwickeln und regelmäßige Datenanalyseberichte zu erstellen, um eine bessere Kontrolle der Umsetzung der EU-Informationssysteme in den Mitgliedstaaten zu ermöglichen. Die gemeinsamen Datenqualitätsindikatoren sollten Mindestqualitätsstandards für die Datenspeicherung in den EU-Informationssystemen oder in den Interoperabilitätskomponenten einschließen. Ziel dieser Datenqualitätsstandards sollte sein, dass die EU-Informationssysteme und die Interoperabilitätskomponenten die automatische Ermittlung anscheinend falscher oder unstimmiger Dateneinträge ermöglichen und so dem Mitgliedstaat, der die Daten eingegeben hat, die Möglichkeit gegeben wird, die betreffenden Daten zu überprüfen und etwaige erforderliche Abhilfemaßnahmen zu ergreifen.

(49) Die Kommission sollte die von eu-LISA erstellten Qualitätsberichte auswerten und gegebenenfalls entsprechende Empfehlungen an die Mitgliedstaaten richten. Die Mitgliedstaaten sollten dafür verantwortlich sein, einen Aktionsplan aufzustellen, in dem Maßnahmen zur Behebung etwaiger Mängel bei der Datenqualität beschrieben werden, und regelmäßig über dabei erzielte Fortschritte Bericht erstatten.

(50) Das universelle Nachrichtenformat (Universal Message Format — im Folgenden „UMF“) sollte als Standard für den strukturierten grenzübergreifenden Informationsaustausch zwischen Informationssystemen, Behörden und/oder Organisationen im Bereich Justiz und Inneres dienen. Durch das UMF sollten ein gemeinsames Vokabular und logische Strukturen für üblicherweise ausgetauschte Informationen vorgegeben werden, damit ausgetauschte Inhalte einheitlich und semantisch gleichwertig erstellt und gelesen werden können und somit die Interoperabilität verbessert wird.

(51) Im VIS, im SIS sowie in allen anderen bestehenden oder neuen Modellen für den grenzübergreifenden Informationsaustausch und Informationssystemen im Bereich Justiz und Inneres, die von Mitgliedstaaten entwickelt wurden oder werden, kann die Umsetzung des UMF-Standards in Betracht gezogen werden.

([8]) Verordnung (EU) 2018/1860 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Nutzung des Schengener Informationssystems für die Rückkehr illegal aufhältiger Drittstaatsangehöriger (ABl. L 312 vom 7.12.2018, S. 1).

([9]) Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006 (ABl. L 312 vom 7.12.2018, S. 14).

([10]) Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56).

(52) Es sollte ein zentraler Speicher für Berichte und Statistiken (central repository for reporting and statistics — im Folgenden „CRRS“) eingerichtet werden, der die systemübergreifende Erhebung statistischer Daten und die Erstellung von Analyseberichten zu politischen und operativen Zwecken gemäß den anwendbaren Rechtsinstrumenten sowie für die Zwecke der Datenqualität ermöglicht. Der CRRS sollte von eu-LISA konzipiert, umgesetzt und an ihren technischen Standorten eingerichtet werden. Er sollte anonymisierte statistische Daten aus den EU-Informationssystemen, dem CIR, dem MID und dem gemeinsamen BMS enthalten. Die im CRRS enthaltenen Daten sollten keine Identifizierung von Einzelpersonen ermöglichen. Die Daten sollten von eu-LISA automatisch anonymisiert und als solche im CRRS gespeichert werden. Die Anonymisierung sollte automatisch erfolgen, und den Bediensteten von eu-LISA sollte kein direkter Zugang zu den in den EU-Informationssystemen oder in den Interoperabilitätskomponenten gespeicherten personenbezogenen Daten gewährt werden.

(53) Die Verordnung (EU) 2016/679 findet auf die Verarbeitung personenbezogener Daten zum Zwecke der Interoperabilität durch nationale Behörden im Rahmen dieser Verordnung Anwendung, sofern diese Verarbeitung nicht durch benannte Behörden oder zentrale Anlaufstellen der Mitgliedstaaten zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten erfolgt.

(54) Wird die Verarbeitung personenbezogener Daten durch die Mitgliedstaaten zum Zwecke der Interoperabilität gemäß der vorliegenden Verordnung von den zuständigen Behörden zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten durchgeführt, so findet die Richtlinie (EU) 2016/680 Anwendung.

(55) Die Verordnung (EU) 2016/679, die Verordnung (EU) 2018/1725 oder, sofern relevant, die Richtlinie (EU) 2016/680 gelten für jedwede Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, die gemäß der vorliegenden Verordnung erfolgen. Unbeschadet der Gründe für eine Übermittlung nach Kapitel V der Verordnung (EU) 2016/679 oder, sofern relevant, der Richtlinie (EU) 2016/680 sollte das Urteil eines Gerichts oder die Entscheidung einer Verwaltungsbehörde eines Drittlandes, durch die ein für die Verarbeitung Verantwortlicher oder Datenauftragsverarbeiter verpflichtet wird, personenbezogene Daten zu übermitteln oder offenzulegen, nur anerkannt werden oder in irgendeiner Weise durchsetzbar sein, wenn Grundlage eine internationale Übereinkunft ist, die zwischen dem anfordernden Drittland und der Union oder einem Mitgliedstaat in Kraft ist.

(56) Die einschlägigen Datenschutzbestimmungen der Verordnung (EU) 2018/1862 und der Verordnung (EU) 2019/816 ([11]) des Europäischen Parlaments und des Rates gelten für die Verarbeitung personenbezogener Daten in den von jenen Verordnungen geregelten Systemen.

(57) Die Verordnung (EU) 2018/1725 gilt für die Verarbeitung personenbezogener Daten durch eu-LISA und andere Organen und Einrichtungen der Union bei der Wahrnehmung ihrer Aufgaben gemäß der vorliegenden Verordnung und lässt die Verordnung (EU) 2016/794 unberührt, welche ihrerseits für die Verarbeitung personenbezogener Daten durch Europol maßgeblich ist.

(58) Die Aufsichtsbehörden gemäß der Verordnung (EU) 2016/679 oder der Richtlinie (EU) 2016/680 sollten die Rechtmäßigkeit der Verarbeitung personenbezogener Daten durch die Mitgliedstaaten überwachen. Der Europäische Datenschutzbeauftragte sollte die Tätigkeiten der Organe und Einrichtungen der Union bei der Verarbeitung personenbezogener Daten überwachen. Der Europäische Datenschutzbeauftragte und die Aufsichtsbehörden sollten bei der Überwachung der Verarbeitung personenbezogener Daten durch Interoperabilitätskomponenten zusammenarbeiten. Damit der Europäische Datenschutzbeauftragte die ihm gemäß dieser Verordnung übertragenen Aufgaben wahrnehmen kann, sind ausreichende Ressourcen, einschließlich personeller und finanzieller Ressourcen, erforderlich.

(59) Der Europäische Datenschutzbeauftragte wurde gemäß Artikel 28 Absatz 2 der Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates ([12]) angehört und hat am 16. April 2018 ([13]) eine Stellungnahme abgegeben.

(60) Die Artikel-29-Datenschutzgruppe hat am 11. April 2018 eine Stellungnahme abgegeben.

(61) Die Mitgliedstaaten und eu-LISA sollten über Sicherheitspläne verfügen, die die Erfüllung der Sicherheitsanforderungen erleichtern und sie sollten Sicherheitsfragen gemeinsam angehen. Zudem sollte eu-LISA sicherstellen, dass zur Gewährleistung der Datenintegrität im Zusammenhang mit Konzeption, Entwicklung und Betrieb der Interoperabilitätskomponenten fortwährend auf die neuesten technologischen Entwicklungen zurückgegriffen wird. Zu den Pflichten von eu-Lisa in dieser Hinsicht sollte es gehören, die Maßnahmen zu ergreifen, die notwendig sind, um den Zugang von Unbefugten, wie etwa Personal externer Dienstleistungserbringer, zu

([11]) Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, sowie zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) Nr. 2018/1726 (siehe Seite 1 dieses Amtsblatts).

([12]) Verordnung (EG) Nr. 45/2001 des Europäischen Parlaments und des Rates vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr (ABl. L 8 vom 12.1.2001, S. 1).

([13]) ABl. C 233 vom 4.7.2018, S.12.

personenbezogenen Daten zu verhindern, die über die Interoperabilitätskomponenten verarbeitet werden. Bei der Vergabe von Aufträgen für die Erbringung von Dienstleistungen sollten die Mitgliedstaaten und eu-Lisa alle Maßnahmen prüfen, die notwendig sind, um die Einhaltung der Rechts- und Verwaltungsvorschriften im Zusammenhang mit dem Schutz personenbezogener Daten und der Privatsphäre des Einzelnen bzw. dem Schutz wesentlicher Sicherheitsinteressen gemäß der Verordnung (EU) 2018/1046 des Europäischen Parlaments und des Rates ([14]) und anwendbaren internationalen Übereinkommen sicherzustellen. eu-LISA sollte bei der Entwicklung der Interoperabilitätskomponenten die Grundsätze des eingebauten Datenschutzes und der datenschutzfreundlichen Grundeinstellungen anwenden.

(62) Zu statistischen Zwecken und für die Berichterstattung ist es erforderlich, ermächtigten Bediensteten der in der vorliegenden Verordnung genannten zuständigen Behörden, Organe und Stellen der Union Zugang zu bestimmten Daten aus bestimmten Interoperabilitätskomponenten ohne die Möglichkeit einer Identifizierung von Einzelpersonen zu erteilen.

(63) Damit sich die mitgliedstaatlichen Behörden und Stellen der Union an die neuen Anforderungen an die Nutzung des ESP anpassen können, ist es erforderlich, einen Übergangszeitraum vorzusehen. Ebenso sollten, um ein kohärentes und optimales Funktionieren des MID zu ermöglichen, Übergangsmaßnahmen für dessen Inbetriebnahme vorgesehen werden.

(64) Da das Ziel dieser Verordnung, nämlich die Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen, von den Mitgliedstaaten nicht ausreichend verwirklicht werden kann, sondern vielmehr wegen des Umfangs und der Wirkungen dieses Vorhabens auf Unionsebene besser zu verwirklichen ist, kann die Union im Einklang mit dem in Artikel 5 des Vertrags über die Europäische Union (EUV) verankerten Subsidiaritätsprinzip tätig werden. Entsprechend dem in demselben Artikel genannten Grundsatz der Verhältnismäßigkeit geht diese Verordnung nicht über das für die Verwirklichung dieses Ziels erforderliche Maß hinaus.

(65) Die verbleibenden Mittel, die nach der Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates ([15]) für intelligente Grenzen vorgesehen sind, sollten gemäß Artikel 5 Absatz 5 Buchstabe b der Verordnung (EU) Nr. 515/2014 neu zugewiesen und auf diese Verordnung übertragen werden, um die Kosten der Entwicklung der Interoperabilitätskomponenten zu decken.

(66) Um bestimmte technische Einzelaspekte dieser Verordnung zu ergänzen, sollte der Kommission die Befugnis übertragen werden, gemäß Artikel 290 des Vertrags über die Arbeitsweise der Europäischen Union Rechtsakte über folgendes zu erlassen:

— die Verlängerung des Übergangszeitraums für den Einsatz des ESP;

— die Verlängerung des Übergangszeitraums für die Prüfung auf Mehrfachidentitäten durch die ETIAS-Zentralstelle;

— die Verfahren zur Bestimmung der Fälle, in denen die Identitätsdaten als gleich oder ähnlich angesehen werden können;

— die Bestimmungen für den Betrieb des CRRS, einschließlich spezifischer Sicherheitsvorkehrungen für die Verarbeitung personenbezogener Daten und Sicherheitsvorschriften für den Speicher; und

— detaillierte Bestimmungen über den Betrieb des Web-Portals.

Es ist von besonderer Bedeutung,, dass die Kommission im Zuge ihrer Vorbereitungsarbeit angemessene Konsultationen, auch auf der Ebene von Sachverständigen, durchführt, die mit den Grundsätzen im Einklang stehen, die in der Interinstitutionellen Vereinbarung vom 13. April 2016 über bessere Rechtsetzung ([16]) niedergelegt wurden. Um für eine gleichberechtigte Beteiligung an der Vorbereitung delegierter Rechtsakte zu sorgen, erhalten das Europäische Parlament und der Rat alle Dokumente zur gleichen Zeit wie die Sachverständigen der Mitgliedstaaten, und ihre Sachverständigen haben systematisch Zugang zu den Sitzungen der Sachverständigengruppen der Kommission, die mit der Vorbereitung der delegierten Rechtsakte befasst sind.

(67) Um einheitliche Bedingungen für die Durchführung dieser Verordnung zu gewährleisten, sollten der Kommission Durchführungsbefugnisse übertragen werden, um die Zeitpunkte festzulegen, ab denen das ESP, das gemeinsame BMS, das CIR, das MID und das CRRS ihren Betrieb aufnehmen.

([14]) Verordnung (EU, Euratom) 2018/1046 des Europäischen Parlaments und des Rates vom 18. Juli 2018 über die Haushaltsordnung für den Gesamthaushaltsplan der Union, zur Änderung der Verordnungen (EU) Nr. 1296/2013, (EU) Nr. 1301/2013, (EU) Nr. 1303/2013, (EU) Nr. 1304/2013, (EU) Nr. 1309/2013, (EU) Nr. 1316/2013, (EU) Nr. 223/2014, (EU) Nr. 283/2014 und des Beschlusses Nr. 541/2014/EU sowie zur Aufhebung der Verordnung (EU, Euratom) Nr. 966/2012 (ABl. L 193 vom 30.7.2018, S. 1).

([15]) Verordnung (EU) Nr. 515/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 zur Schaffung eines Instruments für die finanzielle Unterstützung für Außengrenzen und Visa im Rahmen des Fonds für die innere Sicherheit und zur Aufhebung der Entscheidung Nr. 574/2007/EG (ABl. L 150 vom 20.5.2014, S. 143).

([16]) ABl. L 123 vom 12.5.2016, S. 1

(68) Zudem sollten der Kommission Durchführungsbefugnisse zum Erlass detaillierter Bestimmungen über folgende Aspekte übertragen werden: die technischen Einzelheiten der Profile von Nutzern des ESP; die Spezifikationen der technischen Lösung, die die Abfrage von EU-Informationssystemen der EU, Europol-Daten und Interpol-Datenbanken durch das ESP erlaubt, und das Format der Antworten des ESP; die technischen Vorschriften für die Erstellung von Verknüpfungen im MID zwischen Daten aus verschiedenen EU-Informationssystemen; Inhalt und Darstellung des für die Unterrichtung der betroffenen Person zu benutzenden Formulars, wenn eine rote Verknüpfung erstellt wird; die Leistungsanforderungen und Leistungsüberwachung des gemeinsamen BMS; Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie gemeinsame Datenqualitätsindikatoren; die Entwicklung des UMF-Standards; das Verfahren zur Zusammenarbeit im Fall eines Sicherheitsvorfalls; und die Spezifikationen der technischen Lösung für die Mitgliedstaaten, um die Anträge von Nutzern auf Zugang zu verwalten. Diese Befugnisse sollten gemäß der Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates ([17]) ausgeübt werden.

(69) Da die Interoperabilitätskomponenten die Verarbeitung einer erheblichen Menge sensibler personenbezogener Daten umfassen werden, ist es wichtig, dass Personen, deren Daten durch diese Komponenten verarbeitet werden, als Betroffene ihre Rechte gemäß der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2018/1725 wirksam ausüben können. Den betroffenen Personen sollte ein Web-Portal zur Verfügung gestellt werden, das es ihnen erleichtert, ihre Rechte auf Zugang zu ihren personenbezogenen Daten sowie auf deren Berichtigung, Löschung und Einschränkung von deren Verarbeitung auszuüben. eu-LISA sollte dieses Web-Portal einrichten und verwalten.

(70) Einer der wesentlichen Grundsätze des Datenschutzes ist die Datenminimierung: gemäß Artikel 5 Absatz 1 Buchstabe c der Verordnung (EU) 2016/679 muss die Verarbeitung personenbezogener Daten dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Aus diesem Grund sollte bei den Interoperabilitätskomponenten nicht vorgesehen sein, dass neue personenbezogene Daten gespeichert werden, mit Ausnahme der Verknüpfungen, die im MID gespeichert werden und die das notwendige Minimum für die Zwecke dieser Verordnung darstellen.

(71) Diese Verordnung sollte klare Bestimmungen über die Haftung und das Recht auf Schadenersatz für die rechtswidrige Verarbeitung personenbezogener Daten und andere gegen diese Verordnung verstoßende Handlungen beinhalten. Diese Bestimmungen sollten das Recht auf Schadenersatz durch den für die Verarbeitung Verantwortlichen oder den Datenauftragsverarbeiter sowie deren Haftung gemäß der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2018/1725 unberührt lassen. eu-LISA sollte für jeden von ihr in ihrer Eigenschaft als Datenauftragsverarbeiter verursachten Schaden haften, wenn sie den ihr spezifisch in dieser Verordnung auferlegten Pflichten nicht nachgekommen ist oder wenn sie die rechtmäßig erteilten Anweisungen des Mitgliedstaats, der der für die Datenverarbeitung Verantwortliche ist, nicht beachtet oder gegen diese Anweisungen gehandelt hat.

(72) Diese Verordnung gilt unbeschadet der Anwendung der Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates ([18]).

(73) Nach den Artikeln 1 und 2 des dem EUV und dem AEUV beigefügten Protokolls Nr. 22 über die Position Dänemarks beteiligt sich Dänemark nicht an der Annahme dieser Verordnung und ist weder durch diese Verordnung gebunden noch zu seiner Anwendung verpflichtet. Da diese Verordnung, soweit sich ihre Bestimmungen auf das SIS nach Maßgabe der Verordnung (EU) 2018/1862 beziehen, den Schengen-Besitzstand ergänzt, beschließt Dänemark gemäß Artikel 4 des genannten Protokolls innerhalb von sechs Monaten, nachdem der Rat diese Verordnung angenommen hat, ob es sie in nationales Recht umsetzt.

(74) Soweit sich ihre Bestimmungen auf das SIS nach Maßgabe der Verordnung (EU) 2018/1862 beziehen, beteiligt sich das Vereinigte Königreich an dieser Verordnung gemäß Artikel 5 Absatz 1 des dem EUV und dem AEUV beigefügten Protokolls Nr. 19 über den in den Rahmen der Europäischen Union einbezogenen Schengen-Besitzstand (im Folgenden „Protokoll über den Schengen-Besitzstand“) sowie gemäß Artikel 8 Absatz 2 des Beschlusses 2000/365/EG des Rates ([19]). Soweit sich ihre Bestimmungen auf Eurodac und das ECRIS-TCN beziehen, hat das Vereinigte Königreich mit Schreiben vom 18. Mai 2018 ferner mitgeteilt, dass es sich nach Artikel 3 des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts an der Annahme und Anwendung dieser Verordnung beteiligen möchte.

([17]) Verordnung (EU) Nr. 182/2011 des Europäischen Parlaments und des Rates vom 16. Februar 2011 zur Festlegung der allgemeinen Regeln und Grundsätze, nach denen die Mitgliedstaaten die Wahrnehmung der Durchführungsbefugnisse durch die Kommission kontrollieren (ABl. L 55 vom 28.2.2011, S. 13).

([18]) Richtlinie 2004/38/EG des Europäischen Parlaments und des Rates vom 29. April 2004 über das Recht der Unionsbürger und ihrer Familienangehörigen, sich im Hoheitsgebiet der Mitgliedstaaten frei zu bewegen und aufzuhalten, zur Änderung der Verordnung (EWG) Nr. 1612/68 und zur Aufhebung der Richtlinien 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG und 93/96/EWG (ABl. L 158 vom 30.4.2004, S. 77).

([19]) Beschluss 2000/365/EG des Rates vom 29. Mai 2000 zum Antrag des Vereinigten Königreichs Großbritannien und Nordirland, einzelne Bestimmungen des Schengen-Besitzstands auf sie anzuwenden (ABl. L 131 vom 1.6.2000, S. 43).

(75) Soweit sich ihre Bestimmungen auf das SIS nach Maßgabe der Verordnung (EU) 2018/1862 beziehen, könnte Irland sich grundsätzlich an dieser Verordnung gemäß Artikel 5 Absatz 1 des dem EUV und dem AEUV beigefügten Protokolls Nr. 19 über den in den Rahmen der Europäischen Union einbezogenen Schengen-Besitzstand sowie gemäß Artikel 6 Absatz 2 des Beschlusses 2002/192/EG des Rates ([20]) beteiligen. Soweit sich ihre Bestimmungen der vorliegenden Verordnung auf Eurodac und das ECRIS-TAN beziehen, beteiligt sich Irland darüber hinaus nach den Artikeln 1 und 2 des dem EUV und dem AEUV beigefügten Protokolls Nr. 21 über die Position des Vereinigten Königreichs und Irlands hinsichtlich des Raums der Freiheit, der Sicherheit und des Rechts und unbeschadet des Artikels 4 dieses Protokolls nicht an der Annahme dieser Verordnung und ist weder durch diese Verordnung gebunden noch zu ihrer Anwendung verpflichtet. Da es unter diesen Umständen nicht möglich ist sicherzustellen, dass die vorliegende Verordnung in allen ihren Teilen in Irland gilt, wie Artikel 288 AEUV verlangt, beteiligt Irland sich nicht an der Annahme der vorliegenden Verordnung und ist weder durch die vorliegende Verordnung gebunden noch zu Ihrer Anwendung verpflichtet, unbeschadet seiner Rechte und Pflichten nach den Protokollen Nr. 19 und Nr. 21.

(76) Für Island und Norwegen stellt diese Verordnung, soweit sich ihre Bestimmungen auf das SIS nach Maßgabe der Verordnung (EU) 2018/1862 beziehen, eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Übereinkommens zwischen dem Rat der Europäischen Union sowie der Republik Island und dem Königreich Norwegen über die Assoziierung der beiden letztgenannten Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands ([21]) dar, die zu dem in Artikel 1 Buchstabe g des Beschlusses 1999/437/EG des Rates ([22]) genannten Bereich gehören.

(77) Für die Schweiz stellt diese Verordnung, soweit sich ihre Bestimmungen auf das SIS nach Maßgabe der Verordnung (EU) 2018/1862 beziehen, eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands ([23]) dar, die zu dem in Artikel 1 Buchstabe g des Beschlusses 1999/437/EG in Verbindung mit Artikel 3 des Beschlusses 2008/146/EG des Rates ([24]) genannten Bereich gehören.

(78) Für Liechtenstein stellt diese Verordnung, soweit sich ihre Bestimmungen auf das SIS nach Maßgabe der Verordnung (EU) 2018/1862 beziehen, eine Weiterentwicklung der Bestimmungen des Schengen-Besitzstands im Sinne des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zu dem Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands ([25]) dar, die zu dem in Artikel 1 Buchstabe G des Beschlusses 1999/437/EG in Verbindung mit Artikel 3 des Beschlusses 2011/350/EU des Rates ([26]) genannten Bereich gehören.

(79) Diese Verordnung steht im Einklang mit den Grundrechten und Grundsätzen, die insbesondere mit der Charta der Grundrechte der Europäischen Union anerkannt wurden, und sollte unter Wahrung dieser Rechte und Grundsätze angewandt werden.

(80) Damit sich diese Verordnung in den bestehenden Rechtsrahmen einfügt, sollten die Verordnung (EU) 2018/1726 des Europäischen Parlaments und des Rates ([27]) und die Verordnungen (EU) 2018/1862 und (EU) 2019/816 entsprechend geändert werden, —

([20]) Beschluss 2002/192/EG des Rates vom 28. Februar 2002 zum Antrag Irlands auf Anwendung einzelner Bestimmungen des Schengen-Besitzstands auf Irland (ABl. L 64 vom 7.3.2002, S. 20).

([21]) ABl. L 176 vom 10.7.1999, S. 36.

([22]) Beschluss 1999/437/EG des Rates vom 17. Mai 1999 zum Erlass bestimmter Durchführungsvorschriften zu dem Übereinkommen zwischen dem Rat der Europäischen Union und der Republik Island und dem Königreich Norwegen über die Assoziierung dieser beiden Staaten bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (ABl. L 176 vom 10.7.1999, S. 31).

([23]) ABl. L 53 vom 27.2.2008, S. 52.

([24]) Beschluss 2008/149/JI des Rates vom 28. Jänner 2008 über den Abschluss — im Namen der Europäischen Gemeinschaft — des Abkommens zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands (ABl. L 53 vom 27.2.2008, S. 50).

([25]) ABl. L 160 vom 18.6.2011, S. 21.

([26]) Beschluss 2011/350/EU des Rates vom 7. März 2011 über den Abschluss — im Namen der Europäischen Union — des Protokolls zwischen der Europäischen Union, der Europäischen Gemeinschaft, der Schweizerischen Eidgenossenschaft und dem Fürstentum Liechtenstein über den Beitritt des Fürstentums Liechtenstein zum Abkommen zwischen der Europäischen Union, der Europäischen Gemeinschaft und der Schweizerischen Eidgenossenschaft über die Assoziierung der Schweizerischen Eidgenossenschaft bei der Umsetzung, Anwendung und Entwicklung des Schengen-Besitzstands in Bezug auf die Abschaffung der Kontrollen an den Binnengrenzen und den freien Personenverkehr (ABl. L 160 vom 18.6.2011, S. 19).

([27]) Verordnung (EU) 2018/1726 des Europäischen Parlaments und des Rates vom 14. November 2018 über die Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA), zur Änderung der Verordnung (EG) Nr. 1987/2006 und des Beschlusses 2007/533/JI des Rates sowie zur Aufhebung der Verordnung (EU) Nr. 1077/2011 (ABl. L 295 vom 21.11.2018, S. 99).

HABEN FOLGENDE VERORDNUNG ERLASSEN:

KAPITEL I

Allgemeine Bestimmungen

Artikel 1

Gegenstand

(1) Durch diese Verordnung und die Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates ([28]) wird ein Rahmen für die Sicherstellung der Interoperabilität zwischen dem Einreise-/Ausreisesystem (im Folgenden „EES"), dem Visa-Informationssystem (im Folgenden „VIS"), dem Europäischen Reiseinformations- und -genehmigungssystem (im Folgenden „ETIAS"), Eurodac, dem Schengener Informationssystem (im Folgenden „SIS") und dem Europäischen Strafregisterinformationssystem für Drittstaatsangehörige (im Folgenden „ECRIS-TCN") geschaffen.

(2) Dieser Rahmen umfasst folgende Interoperabilitätskomponenten:

a) Europäisches Suchportal (European search portal — im Folgenden „ESP"),

b) gemeinsamer Dienst für den Abgleich biometrischer Daten (biometric matching service — im Folgenden „gemeinsamer BMS"),

c) gemeinsamer Speicher für Identitätsdaten (common identity repository — im Folgenden „CIR"),

d) Detektor für Mehrfachidentitäten (multiple-identity detector — im Folgenden „MID").

(3) Zudem werden in dieser Verordnung Bestimmungen über die Datenqualitätsanforderungen, ein universelles Nachrichtenformat (Universal Message Format — im Folgenden „UMF"), einen zentralen Speicher für Berichte und Statistiken (central repository for reporting and statistics — im Folgenden „CRRS") sowie die Verantwortlichkeiten der Mitgliedstaaten und der Agentur der Europäischen Union für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (eu-LISA) bei der Konzipierung, der Entwicklung und dem Betrieb der Interoperabilitätskomponenten festgelegt.

(4) Diese Verordnung regelt ferner die Verfahren und Bedingungen für den Zugang der benannten Behörden und der Agentur der Europäischen Union für die Zusammenarbeit auf dem Gebiet der Strafverfolgung (Europol) zum EES, zum VIS, zum ETIAS und zu Eurodac zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer oder sonstiger schwerer Straftaten.

(5) Durch diese Verordnung wird auch ein Rahmen für die Überprüfung der Identitäten von Personen und für die Identifizierung von Personen festgelegt.

Artikel 2

Ziele

(1) Durch die mittels dieser Verordnung sichergestellte Interoperabilität sollen folgende Ziele erreicht werden:

a) Verbesserung der Wirksamkeit und Effizienz der Grenzübertrittskontrollen an den Außengrenzen,

b) Beitrag zur Verhinderung und Bekämpfung illegaler Einwanderung,

c) Gewährleistung eines hohen Maßes an Sicherheit im Raum der Freiheit, der Sicherheit und des Rechts der Union einschließlich der Aufrechterhaltung der öffentlichen Sicherheit und Ordnung sowie des Schutzes der inneren Sicherheit im Hoheitsgebiet der Mitgliedstaaten,

d) verbesserte Umsetzung der gemeinsamen Visumpolitik,

e) Unterstützung bei der Prüfung von Anträgen auf internationalen Schutz,

f) Beitrag zur Verhinderung, Aufdeckung und Untersuchung terroristischer und sonstiger schwerer Straftaten,

g) Erleichterung der Identifizierung von unbekannten Personen, die sich nicht ausweisen können, oder von nicht-identifizierten sterblichen Überresten bei Naturkatastrophen, Unfällen oder terroristischen Anschlägen.

(2) Die Ziele nach Absatz 1 sollen durch folgende Maßnahmen erreicht werden:

a) Sicherstellung der korrekten Identifizierung von Personen,

b) Beitrag zur Bekämpfung von Identitätsbetrug,

([28]) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates, der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (siehe Seite 27 dieses Amtsblatts).

c) Verbesserung der Datenqualität und Harmonisierung der Qualitätsanforderungen an die in den EU-Informationssystemen gespeicherten Daten unter Beachtung der Datenverarbeitungsanforderungen gemäß den rechtlichen Regelungen der einzelnen Systeme sowie den Datenschutzstandards und -grundsätzen,

d) Erleichterung und Unterstützung der technischen und der operativen Umsetzung der EU-Informationssysteme durch die Mitgliedstaaten,

e) Verschärfung, Vereinfachung und Vereinheitlichung der für die einzelnen EU-Informationssysteme geltenden Bedingungen für die Sicherheit und den Schutz der Daten, ohne Auswirkungen auf den besonderen Schutz und die Garantien, die für bestimmte Kategorien von Daten vorgesehen sind,

f) Vereinheitlichung der Bedingungen für den Zugang benannter Behörden zum EES, zum VIS, zum ETIAS und zu Eurodac unter Sicherstellung der erforderlichen und verhältnismäßigen Bedingungen für diesen Zugang sowie

g) Unterstützung der Zwecke des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN.

Artikel 3

Anwendungsbereich

(1) Diese Verordnung gilt für Eurodac, das SIS und das ECRIS-TCN.

(2) Diese Verordnung gilt zudem in dem Maße für Europol-Daten, wie es erforderlich ist, damit diese gleichzeitig zu den in Absatz 1 genannten EU-Informationssystemen abgefragt werden können.

(3) Diese Verordnung gilt für Personen, deren personenbezogene Daten in den in Absatz 1 genannten EU-Informationssystemen und in den in Absatz 2 genannten Europol-Daten verarbeitet werden können.

Artikel 4

Begriffsbestimmungen

Für die Zwecke dieser Verordnung bezeichnet der Ausdruck

1. „Außengrenzen“ die Außengrenzen im Sinne des Artikels 2 Nummer 2 der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates ([29]);

2. „Grenzübertrittskontrollen“ die Grenzübertrittskontrollen im Sinne des Artikels 2 Nummer 11 der Verordnung (EU) 2016/399;

3. „Grenzschutzbehörde“ die Grenzschutzbeamten, die nach nationalem Recht angewiesen sind, Grenzübertrittskontrollen durchzuführen;

4. „Aufsichtsbehörden“ die Aufsichtsbehörde gemäß Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 und die Aufsichtsbehörde gemäß Artikel 41 Absatz 1 der Richtlinie (EU) 2016/680;

5. „Verifizierung“ den Abgleich von Datensätzen zur Überprüfung einer Identitätsangabe (1:1-Abgleich);

6. „Identifizierung“ die Feststellung der Identität einer Person durch den Abgleich mit vielen Datensätzen in einer Datenbank (1:n-Abgleich);

7. „alphanumerische Daten“ Daten in Form von Buchstaben, Ziffern, Sonderzeichen, Leerzeichen und Satzzeichen;

8. „Identitätsdaten“ die in Artikel 27 Absatz 3 Buchstaben a bis e genannten Daten;

9. „Fingerabdruckdaten“ Fingerabdrücke und Fingerabdruckspuren, die aufgrund ihrer Einzigartigkeit und der darin enthaltenen Bezugspunkte präzise und schlüssige Abgleiche zur Identität einer Person ermöglichen;

([29]) Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates vom 9. März 2016 über einen Gemeinschaftskodex für das Überschreiten der Grenzen durch Personen (Schengener Grenzkodex) (ABl. L 77 vom 23.3.2016, S. 1).

10. „Gesichtsbild“ eine digitale Aufnahme des Gesichts einer Person;

11. „biometrische Daten“ Fingerabdruckdaten oder Gesichtsbilder oder beides;

12. „biometrisches Template“ eine mathematische Repräsentation, die mittels Merkmalsauszug aus biometrischen Daten generiert wird, welche auf die für Identifizierungs- und Verifizierungszwecke erforderlichen Merkmale begrenzt sind;

13. „Reisedokument“ einen Reisepass oder ein anderes gleichwertiges Dokument, das seinen Inhaber zum Überschreiten der Außengrenzen berechtigt und in dem ein Visum angebracht werden kann;

14. „Reisedokumentendaten“ die Art, die Nummer und das Ausstellungsland des Reisedokuments, das Datum des Ablaufs der Gültigkeitsdauer des Reisedokuments und den aus drei Buchstaben bestehenden Code des Landes, das das Reisedokument ausgestellt hat;

15. „EU-Informationssysteme“ die Systeme EES, VIS, ETIAS, Eurodac, SIS und ECRIS-TCN;

16. „Europol-Daten“ die personenbezogenen Daten, die zu den in Artikel 18 Absatz 2 Buchstaben a, b und c der Verordnung (EU) 2016/794 genannten Zwecken von Europol verarbeitet werden;

17. „Interpol-Datenbanken“ die Interpol-Datenbank für gestohlene und verlorene Reisedokumente (Stolen and Lost Travel Document database, „SLTD-Datenbank“) und die Interpol-Datenbank zur Erfassung von Ausschreibungen zugeordneten Reisedokumenten (Travel Documents Associated with Notices database, „TDAWN-Datenbank“);

18. „Übereinstimmung“ eine Übereinstimmung als Ergebnis eines automatischen Abgleichs zwischen zuvor oder zeitgleich in einem Informationssystem oder in einer Datenbank erfassten personenbezogenen Daten;

19. „Polizeibehörde“ die zuständige Behörde im Sinne des Artikels 3 Nummer 7 der Richtlinie (EU) 2016/680;

20. „benannte Behörden“ die benannten mitgliedstaatlichen Behörden im Sinne von Artikel 3 Absatz 1 Nummer 26 der Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates ([30]), Artikel 2 Absatz 1 Buchstabe e des Beschlusses 2008/633/JI des Rates ([31]) und Artikel 3 Absatz 1 Nummer 21 der Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates ([32]);

21. „„terroristische Straftat“ eine Straftat nach nationalem Recht, die einer der in der Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates ([33]) aufgeführten Straftaten entspricht oder dieser gleichwertig ist;

22. „schwere Straftat“ eine Straftat, die einer der in Artikel 2 Absatz 2 des Rahmenbeschlusses 2002/584/JI des Rates ([34]) aufgeführten Straftaten entspricht oder dieser gleichwertig ist, wenn die Straftat nach dem nationalen Recht mit einer Freiheitsstrafe oder freiheitsentziehenden Maßnahme im Höchstmaß von mindestens drei Jahren bedroht ist;

23. „Einreise-/Ausreisesystem“ oder „EES“ das durch die Verordnung (EU) 2017/2226 eingerichtete Einreise-/Ausreisesystem;

24. „Visa-Informationssystem“ oder „VIS“ das durch die Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates ([35]) eingerichtete Visa-Informationssystem;

25. „Europäisches Reiseinformations- und -genehmigungssystem“ oder „ETIAS“ das durch die Verordnung (EU) 2018/1240 eingerichtete Europäische Reiseinformations- und -genehmigungssystem;

([30]) Verordnung (EU) 2017/2226 des Europäischen Parlaments und des Rates vom 30. November 2017 über ein Einreise-/Ausreisesystem (EES) zur Erfassung der Ein- und Ausreisedaten sowie der Einreiseverweigerungsdaten von Drittstaatsangehörigen an den Außengrenzen der Mitgliedstaaten und zur Festlegung der Bedingungen für den Zugang zum EES zu Gefahrenabwehr- und Strafverfolgungszwecken und zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen sowie der Verordnungen (EG) Nr. 767/2008 und (EU) Nr. 1077/2011 (ABl. L 327 vom 9.12.2017, S. 20).

([31]) Beschluss 2008/633/JI des Rates vom 23. Juni 2008 über den Zugang der benannten Behörden der Mitgliedstaaten und von Europol zum Visa-Informationssystem (VIS) für Datenabfragen zum Zwecke der Verhütung, Aufdeckung und Ermittlung terroristischer und sonstiger schwerwiegender Straftaten (ABl. L 218 vom 13.8.2008, S. 129).

([32]) Verordnung (EU) 2018/1240 des Europäischen Parlaments und des Rates vom 12. September 2018 über die Einrichtung eines Europäischen Reiseinformations- und -genehmigungssystems (ETIAS) und zur Änderung der Verordnungen (EU) Nr. 1077/2011, (EU) Nr. 515/2014, (EU) 2016/399, (EU) 2016/1624 und (EU) 2017/2226 (ABl. L 236 vom 19.9.2018, S. 1).

([33]) Richtlinie (EU) 2017/541 des Europäischen Parlaments und des Rates vom 15. März 2017 zur Terrorismusbekämpfung und zur Ersetzung des Rahmenbeschlusses 2002/475/JI des Rates und zur Änderung des Beschlusses 2005/671/JI des Rates (ABl. L 88 vom 31.3.2017, S. 6).

([34]) Rahmenbeschluss 2002/584/JI des Rates vom 13. Juni 2002 über den Europäischen Haftbefehl und die Übergabeverfahren zwischen den Mitgliedstaaten (ABl. L 190 vom 18.7.2002, S. 1).

([35]) Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung) (ABl. L 218 vom 13.8.2008, S. 60).

26. „Eurodac“ das durch die Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates ([36]) eingerichtete Eurodac-System;

27. „Schengener Informationssystem“ oder „SIS“ das durch die Verordnungen (EU) 2018/1860, (EU) 2018/1861 und (EU) 2018/1862 eingerichtete Schengener Informationssystem;

28. „ECRIS-TCN“ das durch die Verordnung (EU) 2019/816 eingerichtete zentralisierte System für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen vorliegen;

Artikel 5

Nichtdiskriminierung und Grundrechte

Bei der Verarbeitung personenbezogener Daten für die Zwecke dieser Verordnung dürfen keine Personen aufgrund des Geschlechts, der Rasse, der Hautfarbe, der ethnischen oder sozialen Herkunft, der genetischen Merkmale, der Sprache, der Religion oder der Weltanschauung, einer politischen oder sonstigen Anschauung, der Zugehörigkeit zu einer nationalen Minderheit, des Vermögens, der Geburt, einer Behinderung, des Alters oder der sexuellen Ausrichtung diskriminiert werden. Die Menschenwürde und die Integrität sowie die Grundrechte der Betroffenen, darunter auch das Recht auf Achtung der Privatsphäre und auf Schutz der personenbezogenen Daten, müssen uneingeschränkt gewahrt werden. Besonderer Aufmerksamkeit bedürfen Kinder, ältere Menschen, Menschen mit Behinderungen und Menschen, die internationalen Schutz benötigen. Dem Kindeswohl ist vorrangig Rechnung zu tragen.

KAPITEL II

Europäisches Suchportal

Artikel 6

Europäisches Suchportal

(1) Es wird ein Europäisches Suchportal (European search portal, im Folgenden „ESP“) geschaffen, das den mitgliedstaatlichen Behörden und den Stellen der Union einen raschen, unterbrechungsfreien, effizienten, systematischen und kontrollierten Zugang zu den EU-Informationssystemen, den Europol-Daten und den Interpol-Datenbanken zur Wahrnehmung ihrer Aufgaben und nach Maßgabe ihrer Zugangsrechte und im Einklang mit den Zielen und Zwecken des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN erleichtern soll.

(2) Das ESP umfasst

a) eine zentrale Infrastruktur einschließlich eines Suchportals, das die gleichzeitige Abfrage des EES, des VIS, des ETIAS, von Eurodac, des SIS, des ECRIS-TCN, der Europol-Daten und der Interpol-Datenbanken ermöglicht;

b) einen sicheren Kommunikationskanal zwischen dem ESP und denjenigen Mitgliedstaaten und Stellen der Union, die berechtigt sind, das ESP zu nutzen;

c) eine sichere Kommunikationsinfrastruktur zwischen dem ESP und dem EES, dem VIS, dem ETIAS, Eurodac, dem zentralen SIS, dem ECRIS-TCN, den Europol-Daten und den Interpol-Datenbanken sowie zwischen dem ESP und den zentralen Infrastrukturen des CIR und des MID.

(3) eu-LISA entwickelt das ESP und sorgt für seine technische Verwaltung.

Artikel 7

Nutzung des Europäischen Suchportals

(1) Die Nutzung des ESP ist den mitgliedstaatlichen Behörden und den Stellen der Union vorbehalten, die auf mindestens eines der EU-Informationssysteme nach Maßgabe der für diese EU-Informationssysteme geltenden Rechtsinstrumente, den CIR und den MID nach Maßgabe der vorliegenden Verordnung, Europol-Daten nach Maßgabe der Verordnung (EU) 2016/794 oder die Interpol-Datenbanken nach Maßgabe der einschlägigen Bestimmungen des Unionsrechts oder des nationalen Rechts zugreifen können.

Diese mitgliedstaatlichen Behörden und Stellen der Union dürfen nur für die Ziele und Zwecke, die in den für diese EU-Informationssysteme geltenden Rechtsinstrumenten, der Verordnung (EU) 2016/794 und in der vorliegenden Verordnung festgelegt sind, auf das ESP und die von ihm bereitgestellten Daten zurückgreifen.

([36]) Verordnung (EU) Nr. 603/2013 des Europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (ABl. L 180 vom 29.6.2013, S. 1).

(2) Die in Absatz 1 genannten mitgliedstaatlichen Behörden und Stellen der Union nutzen das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten in den Zentralsystemen von Eurodac und des ECRIS-TCN nach Maßgabe ihrer jeweiligen Zugangsrechte gemäß den für diese EU-Informationssysteme geltenden Rechtsinstrumenten und dem nationalen Recht. Sie nutzen das ESP zudem nach Maßgabe ihrer in dieser Verordnung festgelegten Zugangsrechte für die Abfrage des CIR für die in den Artikeln 20, 21 und 22 genannten Zwecke.

(3) Die in Absatz 1 genannten mitgliedstaatlichen Behörden können das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten im in den Verordnungen (EU) 2018/1860 und (EU) 2018/1861 genannten zentralen SIS nutzen.

(4) Wenn es nach dem Unionsrecht vorgesehen ist, können die in Absatz 1 genannten Stellen der Union das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten im zentralen SIS nutzen.

(5) Die in Absatz 1 genannten mitgliedstaatlichen Behörden und Stellen der Union können das ESP für die Abfrage von Daten zu Personen oder deren Reisedokumenten in den Europol-Daten nach Maßgabe ihrer jeweiligen Zugangsrechte nach dem Unionsrecht beziehungsweise nach nationalem Recht nutzen.

Artikel 8

Erstellung von ESP-Nutzerprofilen

(1) Um die Nutzung des ESP zu ermöglichen, erstellt eu-LISA in Zusammenarbeit mit den Mitgliedstaaten auf der Grundlage jeder Kategorie von ESP-Nutzern und der Abfragezwecke ein Profil, das den in Absatz 2 genannten technischen Einzelheiten und Zugangsrechten Rechnung trägt. Jedes Profil enthält dabei nach Maßgabe des Unionsrechts und des nationalen Rechts folgende Informationen:

a) die für die Datenabfrage zu verwendenden Suchfelder,

b) die EU-Informationssysteme, die Europol-Daten und die Interpol-Datenbanken, die abzufragen sind, diejenigen, die abgefragt werden können und diejenigen, zu denen dem Nutzer ein Abfrageergebnis ausgegeben werden muss,

c) die spezifischen Daten in den EU-Informationssystemen, den Europol-Daten und den Interpol-Datenbanken, die abgefragt werden dürfen,

d) die Kategorien der Daten, die als Abfrageergebnis ausgegeben werden dürfen.

(2) Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der technischen Einzelheiten der in Absatz 1 genannten Profile gemäß der jeweiligen Zugangsrechte der ESP-Nutzer nach den geltenden Rechtsinstrumenten zur Regelung der EU-Informationssysteme und nach nationalem Recht. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 70 Absatz 2 genannten Prüfverfahren erlassen.

(3) Die in Absatz 1 genannten Profile werden regelmäßig und mindestens einmal pro Jahr von eu-LISA in Zusammenarbeit mit den Mitgliedstaaten überprüft sowie erforderlichenfalls aktualisiert.

Artikel 9

Abfragen

(1) Die ESP-Nutzer geben, um Abfragen vorzunehmen, alphanumerische und/oder biometrische Daten in das ESP ein. Bei einer Abfrage fragt das ESP anhand der vom Nutzer des ESP eingegebenen Daten und nach Maßgabe des jeweiligen Nutzerprofils gleichzeitig das EES, das ETIAS, das VIS, das SIS, Eurodac, das ECRIS-TCN, den CIR, die Europol-Daten und die Interpol-Datenbanken ab.

(2) Die Kategorien von Daten für die Abfrage über das ESP entsprechen den Kategorien von Daten für Personen oder Reisedokumente, die für die Abfrage der verschiedenen EU-Informationssysteme, der Europol-Daten und der Interpol-Datenbanken nach Maßgabe der für sie geltenden Rechtsinstrumente verwendet werden können.

(3) eu-LISA erstellt in Zusammenarbeit mit den Mitgliedstaaten für das ESP eine Dokumentation zur Schnittstellenansteuerung in dem in Artikel 38 genannten UMF.

(4) Bei einer Abfrage durch einen ESP-Nutzer werden aus dem EES, dem ETIAS, dem VIS, dem SIS, Eurodac, dem ECRIS-TCN, dem CIR, dem MID, den Europol-Daten und aus den Interpol-Datenbanken von ihnen gehaltene Daten als Antwort auf die Abfrage bereitgestellt.

Unbeschadet des Artikels 20 wird in der vom ESP erteilten Antwort angegeben, aus welchem EU-Informationssystem beziehungsweise aus welcher Datenbank die betreffenden Daten stammen.

Das ESP liefert keine Angaben zu Daten in EU-Informationssystemen, zu Europol-Daten und zu den Interpol-Datenbanken, auf die der Nutzer nach dem anwendbaren Unionsrecht und nationalen Recht nicht zugreifen darf.

(5) Über das ESP durchgeführte Abfragen der Interpol-Datenbanken erfolgen so, dass dem für die Interpol-Ausschreibung Verantwortlichen keine Informationen preisgegeben werden.

(6) Sobald Daten aus einem der EU-Informationssysteme, den Europol-Daten oder den Interpol-Datenbanken verfügbar sind, werden dem Nutzer über das ESP Antworten erteilt. Diese Antworten enthalten lediglich die Daten, auf die der Nutzer nach dem Unionsrecht und dem nationalen Recht zugreifen darf.

(7) Die Kommission erlässt einen Durchführungsrechtsakt, um das technische Verfahren für Abfragen der EU-Informationssysteme, Europol-Daten und Interpol-Datenbanken durch das ESP und das Format der vom ESP erteilten Antworten festzulegen. Dieser Durchführungsrechtsakt wird nach dem Prüfverfahren gemäß Artikel 70 Absatz 2 erlassen.

Artikel 10

Führen von Protokollen

(1) Unbeschadet der Artikel 12 und 18 der Verordnung (EU) 2018/1862, des Artikels 29 der Verordnung (EG) 2019/816 und des Artikels 40 der Verordnung (EU) 2016/794 führt eu-LISA Protokolle sämtlicher im ESP erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat oder Stelle der Union, der bzw. die die Abfrage vornimmt, und verwendetes ESP-Nutzerprofil,

b) Datum und Uhrzeit der Abfrage,

c) abgefragte Informationssysteme der EU und Europol-Daten.

(2) Jeder Mitgliedstaat führt Protokolle über die Abfragen, die seine zur Nutzung des ESP ordnungsgemäß ermächtigten Behörden und deren Bedienstete durchführen. Jede Stelle der Union führt Protokolle über die Abfragen, die ihre ordnungsgemäß ermächtigten Bediensteten durchführen.

(3) Die in den Absätzen 1 und 2 genannten Protokolle werden nur zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald diese Protokolle nicht mehr für das Kontrollverfahren benötigt werden.

Artikel 11

Ausweichverfahren für den Fall, dass eine Nutzung des Europäischen Suchportals technisch nicht möglich ist

(1) Wenn es wegen eines Ausfalls des ESP technisch nicht möglich ist, das ESP für die Abfrage eines oder mehrerer der EU-Informationssysteme oder des CIR zu nutzen, werden die ESP-Nutzer von eu-LISA automatisch entsprechend benachrichtigt.

(2) Wenn es wegen eines Ausfalls der nationalen Infrastruktur eines Mitgliedstaats technisch nicht möglich ist, das ESP für die Abfrage eines oder mehrerer EU-Informationssysteme oder des CIR zu nutzen, benachrichtigt der betroffene Mitgliedstaat eu-LISA und die Kommission automatisch.

(3) In den Fällen der Absätze 1 oder 2 des vorliegenden Artikels gilt die in Artikel 7 Absätze 2 und 4 festgelegte Pflicht nicht, bis das technische Versagen behoben ist, und die Mitgliedstaaten fragen die EU-Informationssysteme oder das CIR unmittelbar ab, wenn sie nach dem Unionsrecht oder dem nationalen Recht hierzu verpflichtet sind.

(4) Wenn es wegen eines Ausfalls der Infrastruktur einer Stelle der Union technisch nicht möglich ist, das ESP für die Abfrage eines oder mehrerer EU-Informationssysteme oder des CIR zu nutzen, benachrichtigt die betroffene Stelle eu-LISA und die Kommission automatisch.

KAPITEL III

Gemeinsamer Dienst für den Abgleich biometrischer Daten

Artikel 12

Gemeinsamer Dienst für den Abgleich biometrischer Daten

(1) Es wird ein gemeinsamer Dienst für den Abgleich biometrischer Daten (shared biometric matching service — im Folgenden „gemeinsamer BMS“) eingerichtet, der die Aufgabe hat, biometrische Templates, die aus den im CIR und im SIS gespeicherten biometrischen Daten nach Artikel 13 generiert wurden, zu speichern und die systemübergreifende Abfrage mehrerer EU-Informationssysteme anhand biometrischer Daten zu ermöglichen, um den CIR und den MID sowie die Ziele des EES, des VIS, von Eurodac, des SIS und des ECRIS-TCN zu unterstützen.

(2) Der gemeinsame BMS umfasst

a) eine zentrale Infrastruktur, die die einzelnen Zentralsysteme des EES, des VIS, des SIS, von Eurodac bzw. des ECRIS-TCN insoweit ersetzt, als in ihr biometrische Templates gespeichert werden und sie Suchen mit biometrischen Daten ermöglicht,

b) eine sichere Kommunikationsinfrastruktur zwischen dem gemeinsamen BMS, dem zentralen SIS und dem CIR.

(3) eu-LISA entwickelt den gemeinsamen BMS und sorgt für seine technische Verwaltung.

Artikel 13

Speicherung biometrischer Templates im gemeinsamen Dienst für den Abgleich biometrischer Daten

(1) Der gemeinsame BMS speichert die biometrischen Templates, die er aus folgenden biometrischen Daten generiert:

a) Daten nach Artikel 20 Absatz 3 Buchstaben w und y, außer Daten von Handflächenabdrücken, der Verordnung (EU) 2018/1862;

b) Daten nach Artikel 5 Absatz 1 Buchstabe b und Artikel 5 Absatz 2 der Verordnung (EU) 2019/816.

Die biometrischen Templates werden im gemeinsamen BMS logisch voneinander getrennt nach den Informationssystemen, aus denen die Daten stammen, gespeichert.

(2) Für jeden Satz der in Absatz 1 genannten Daten fügt der gemeinsame BMS jedem biometrischen Template einen Verweis auf die EU-Informationssysteme, in denen die betreffenden biometrischen Daten gespeichert sind, und einen Verweis auf die tatsächlichen Datensätze in diesen EU-Informationssystemen hinzu.

(3) Die biometrischen Templates dürfen erst in den gemeinsamen BMS eingegeben werden, nachdem der gemeinsame BMS die einem der EU-Informationssysteme hinzugefügten biometrischen Daten einer automatischen Qualitätskontrolle unterzogen hat, um sicherzustellen, dass ein Mindestdatenqualitätsstandard eingehalten wird.

(4) Bei der Speicherung der in Absatz 1 genannten Daten sind die in Artikel 37 Absatz 2 genannten Qualitätsstandards einzuhalten.

(5) Die Kommission legt im Wege eines Durchführungsrechtsakts die Leistungsanforderungen und praktischen Vorkehrungen für die Überwachung der Leistung des gemeinsamen BMS fest, um sicherzustellen, dass die Wirksamkeit biometrischer Suchvorgänge auch bei Verfahren gewährleistet ist, bei denen die Zeit eine Rolle spielt, wie etwa Grenzkontrollen und Identifizierungen. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 70 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 14

Abfrage biometrischer Daten mithilfe des gemeinsamen Dienstes für den Abgleich biometrischer Daten

Um die im CIR und im SIS gespeicherten biometrischen Daten abzufragen, nutzen der CIR und das SIS die im gemeinsamen BMS gespeicherten biometrischen Templates. Die Abfragen anhand biometrischer Daten werden zu den Zwecken vorgenommen, die in dieser Verordnung sowie in den Verordnungen (EG) Nr. 767/2008, (EU) 2017/2226, (EU) 2018/1860, (EU) 2018/1861, (EU) 2018/1862 und (EU) 2019/816 vorgesehen sind.

Artikel 15

Datenspeicherung im gemeinsamen Dienst für den Abgleich biometrischer Daten

Die in Artikel 13 Absätze 1 und 2 genannten Daten werden im gemeinsamen BMS nur so lange gespeichert, wie die entsprechenden biometrischen Daten im CIR beziehungsweise im SIS gespeichert werden. Die Daten werden automatisch aus dem gemeinsamen BMS gelöscht.

Artikel 16

Führen von Protokollen

(1) Unbeschadet der Artikel 12 und 18 der Verordnung (EG) Nr. 2018/1862 und des Artikels 29 der Verordnung (EU) 2019/816 führt eu-LISA Protokolle sämtlicher im gemeinsamen BMS erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat oder Stelle der Union, der bzw. die die Abfrage vornimmt,

b) Chronik der Erstellung und der Speicherung biometrischer Templates,

c) die EU-Informationssysteme, die mit den im gemeinsamen BMS gespeicherten biometrischen Templates abgefragt wurden,

d) Datum und Uhrzeit der Abfrage,

e) Art der für die Abfrage verwendeten biometrischen Daten,

f) Abfrageergebnisse sowie Datum und Uhrzeit der Ergebnisanzeige.

(2) Jeder Mitgliedstaat führt Protokolle über die Abfragen, die seine zur Nutzung des gemeinsamen BMS ordnungsgemäß ermächtigten Behörden und deren Bedienstete durchführen. Jede Stelle der Union führt Protokolle über die Abfragen, die ihre ordnungsgemäß ermächtigten Bediensteten durchführen.

(3) Die in den Absätzen 1 und 2 genannten Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald die Protokolle nicht mehr für das Kontrollverfahren benötigt werden.

KAPITEL IV

Gemeinsamer Speicher für Identitätsdaten

Artikel 17

Gemeinsamer Speicher für Identitätsdaten

(1) Es wird ein gemeinsamer Speicher für Identitätsdaten (CIR) geschaffen, in dem für jede im EES, im VIS, im ETIAS, in Eurodac oder im ECRIS-TCN erfasste Person eine individuelle Datei mit den in Artikel 18 genannten Daten angelegt wird und der dazu dient, die korrekte Identifizierung von im EES, im VIS, im ETIAS, in Eurodac und im ECRIS-TCN gemäß Artikel 20 erfassten Personen zu erleichtern und zu unterstützen, das Funktionieren des MID gemäß Artikel 21 zu unterstützen und den etwaig erforderlichen Zugang von benannten Behörden und Europol zu dem EES, dem VIS, dem ETIAS und Eurodac zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer und anderer schwerer Straftaten gemäß Artikel 22 zu erleichtern und einheitlich zu regeln.

(2) Der CIR umfasst

a) eine zentrale Infrastruktur, die die einzelnen Zentralsysteme des EES, des VIS, des ETIAS, von Eurodac und des ECRIS-TCN insoweit ersetzt, als in ihr die in Artikel 18 genannten Daten gespeichert werden,

b) einen sicheren Kommunikationskanal zwischen dem CIR und den Mitgliedstaaten und Stellen der Union, die nach dem Unionsrecht und nationalen Recht berechtigt sind, den CIR zu nutzen,

c) eine sichere Kommunikationsinfrastruktur zwischen dem CIR und dem EES, dem VIS, dem ETIAS, Eurodac und dem ECRIS-TCN sowie den zentralen Infrastrukturen des ESP, des gemeinsamen BMS und des MID.

(3) eu-LISA entwickelt den CIR und sorgt für seine technische Verwaltung.

(4) Ist es aufgrund eines Ausfalls des CIR technisch nicht möglich, den CIR zur Identifizierung einer Person gemäß Artikel 20, zur Aufdeckung von Mehrfachidentitäten gemäß Artikel 21 oder zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer und anderer schwerer Straftaten gemäß Artikel 22 zu nutzen, werden die CIR-Nutzer automatisch von eu-LISA benachrichtigt.

(5) eu-LISA erstellt in Zusammenarbeit mit den Mitgliedstaaten für den CIR eine Dokumentation zur Schnittstellenansteuerung in dem in Artikel 38 genannten UMF.

Artikel 18

Im gemeinsamen Speicher für Identitätsdaten gespeicherte Daten

(1) Im CIR werden folgende Daten logisch voneinander getrennt nach den Informationssystemen, aus denen sie stammen, gespeichert: Daten nach Artikel 5 Absatz 1 Buchstabe b und Artikel 5 Absatz 2 sowie folgende Daten nach Artikel 5 Absatz 1 Buchstabe a der Verordnung (EU) 2019/816: Nachname (Familienname), Vorname(n), Geburtsdatum, Geburtsort (Gemeinde und Staat), Staatsangehörigkeit(en), Geschlecht, gegebenenfalls frühere Namen, soweit vorhanden Pseudonyme und/oder Aliasnamen sowie, soweit vorhanden, Informationen zu Reisedokumenten.

(2) Für jeden Satz der in Absatz 1 genannten Daten fügt der CIR einen Verweis auf die EU-Informationssysteme hinzu, aus denen die betreffenden Daten stammen.

(3) Die Behörden, die auf das CIR zugreifen, tun das gemäß ihren jeweiligen Zugangsrechten nach den für diese EU-Informationssysteme geltenden Rechtsinstrumenten und nach dem nationalen Recht sowie nach Maßgabe ihrer in dieser Verordnung festgelegten Zugangsrechte für die Zwecke nach den Artikeln 20, 21 und 22.

(4) Für jeden Satz der in Absatz 1 genannten Daten fügt der CIR einen Verweis auf den tatsächlichen Datensatz in den EU-Informationssystemen, aus dem die Daten stammen, hinzu.

(5) Bei der Speicherung der in Absatz 1 genannten Daten sind die in Artikel 37 Absatz 2 genannten Qualitätsstandards einzuhalten.

Artikel 19

Hinzufügung, Änderung und Löschung von Daten im gemeinsamen Speicher für Identitätsdaten

(1) Bei jeder Hinzufügung, Änderung oder Löschung von Daten in Eurodac oder im ECRIS-TCN werden die in den individuellen Dateien im CIR gespeicherten Daten nach Artikel 18 automatisch entsprechend hinzugefügt, geändert oder gelöscht.

(2) Wird im MID nach Maßgabe der Artikel 32 oder 33 eine weiße oder eine rote Verknüpfung zwischen Daten von zwei oder mehr EU-Informationssystemen, die Bestandteil des CIR sind, erstellt, werden vom CIR keine neuen individuellen Dateien angelegt, sondern die neuen Daten der individuellen Datei der verknüpften Daten hinzugefügt.

Artikel 20

Zugang zum gemeinsamen Speicher für Identitätsdaten zwecks Identifizierung

(1) Abfragen im CIR werden von einer Polizeibehörde gemäß den Absätzen 2 und 5 nur in den folgenden Situationen vorgenommen:

a) wenn eine Polizeibehörde eine Person wegen des Fehlens eines Reisedokuments oder eines anderen glaubwürdigen Dokuments zum Nachweis der Identität dieser Person nicht identifizieren kann;

b) wenn Zweifel an den von einer Person vorgelegten Identitätsdaten bestehen;

c) wenn Zweifel an der Echtheit des Reisedokuments oder eines anderen glaubwürdigen, von einer Person vorgelegten Dokuments bestehen;

d) wenn Zweifel an der Identität des Inhabers eines Reisedokuments oder eines anderen glaubwürdigen Dokuments bestehen; oder

e) wenn eine Person zu einer Zusammenarbeit nicht in der Lage ist oder sie verweigert.

Eine solche Abfrage zu Minderjährigen unter zwölf Jahren ist unzulässig, es sei denn, sie erfolgt zum Wohl des Kindes.

(2) Ist eine der in Absatz -1 aufgeführten Situationen gegeben, und wurden einer Polizeibehörde mittels nationaler Gesetzgebungsmaßnahmen die in Absatz 5 genannten Befugnisse übertragen, darf sie ausschließlich zum Zwecke der Identifizierung einer Person anhand der bei einer Identitätskontrolle direkt vor Ort erhobenen biometrischen Daten dieser Person Abfragen im CIR vornehmen, sofern das Verfahren im Beisein dieser Person eingeleitet wurde.

(3) Falls eine solche Abfrage ergibt, dass im CIR Daten zu der betreffenden Person gespeichert sind, darf die betreffende Polizeibehörde die in Artikel 18 Absatz 1 genannten Daten einsehen.

Falls die biomettrischen Daten der betreffenden Person nicht verwendet werden können oder die Abfrage anhand dieser Daten nicht erfolgreich ist, ist die Abfrage anhand von Identitätsdaten dieser Person in Verbindung mit Reisedokumentendaten oder anhand der von der betreffenden Person bereitgestellten Identitätsdaten vorzunehmen.

(4) Sind einer Polizeibehörde mittels nationaler Legislativmaßnahmen die in Absatz 6 genannten Befugnisse übertragen worden, darf sie im Falle einer Naturkatastrophe, eines Unfalls oder eines Terroranschlags und ausschließlich zum Zwecke der Identifizierung unbekannter Personen, die sich nicht ausweisen können, oder nicht identifizierter menschlicher Überreste mit den biometrischen Daten dieser Personen Abfragen im CIR vornehmen.

(5) Mitgliedstaaten, die die in Absatz 2 vorgesehene Möglichkeit nutzen möchten, erlassen entsprechende nationale Gesetzgebungsmaßnahmen. Dabei berücksichtigen die Mitgliedstaaten, dass jede Diskriminierung von Drittstaatsangehörigen vermieden werden muss. Durch derartige Gesetzgebungsmaßnahmen sind die genauen Zwecke der zu den in Artikel 2 Absatz 1 Buchstaben b und c genannten Zwecken erfolgenden Identifizierung festzulegen. Durch derartige Gesetzgebungsmaßnahmen sind zudem die zuständigen Polizeibehörden zu benennen sowie die Verfahren, Bedingungen und Kriterien derartiger Kontrollen festzulegen.

(6) Mitgliedstaaten, die die in Absatz 4 vorgesehene Möglichkeit nutzen möchten, erlassen entsprechende nationale Legislativmaßnahmen, in denen die hierfür geltenden Verfahren, Bedingungen und Kriterien festgelegt sind.

Artikel 21

Zugang zum gemeinsamen Speicher für Identitätsdaten zwecks Aufdeckung etwaiger Mehrfachidentitäten

(1) Falls bei der Abfrage des CIR eine gelbe Verknüpfung gemäß Artikel 28 Absatz 4 angezeigt wird, darf die Behörde, die für die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29 zuständig ist, ausschließlich zu Verifizierungszwecken auf die im CIR gespeicherten, durch die gelbe Verknüpfung bezeichneten Daten nach Artikel 18 Absätze 1 und 2 zugreifen.

(2) Falls bei der Abfrage des CIR eine rote Verknüpfung gemäß Artikel 32 angezeigt wird, dürfen die in Artikel 26 Absatz 2 genannten Behörden ausschließlich zur Bekämpfung von Identitätsbetrug auf die im CIR gespeicherten, durch die rote Verknüpfung bezeichneten Daten nach Artikel 18 Absätze 1 und 2 zugreifen.

Artikel 22

Abfrage des gemeinsamen Speichers für Identitätsdaten zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten

(1) Gibt es in einem konkreten Einzelfall vernünftige Gründe dafür, dass die Abfrage der EU-Informationssysteme zur Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten beitragen kann, insbesondere, wenn der Verdacht besteht, dass der Verdächtige, Täter oder das Opfer einer terroristischen Straftat oder sonstiger schwerer Straftaten eine Person ist, die in Eurodac gespeichert ist, können die benannten Behörden und Europol den CIR abfragen, um in Erfahrung zu bringen, ob in Eurodac Daten zu einer spezifischen Person gespeichert sind.

(2) Falls die Abfrage im CIR ergibt, dass in Eurodac Daten zu der betreffenden Person gespeichert sind, zeigt der CIR den benannten Behörden und Europol durch einen Verweis nach Artikel 18 Absatz 2 an, dass in Eurodac übereinstimmende Daten gespeichert sind. Alle vom CIR ausgegebenen Antworten müssen so beschaffen sein, dass die Sicherheit der Daten nicht gefährdet wird.

Die Antwort, aus der hervorgeht, dass Daten zu dieser Person in Eurodac gespeichert sind, darf ausschließlich für die Zwecke der Übermittlung eines Antrags auf uneingeschränkten Zugang vorbehaltlich der Bedingungen und Verfahren, die in dem einschlägigen Rechtsinstrument festgelegt sind, verwendet werden.

Bei einer Übereinstimmung oder mehreren Übereinstimmungen stellt die benannte Behörde oder Europol einen Antrag auf uneingeschränkten Zugang zu mindestens einem der Informationssysteme, aus dem eine Übereinstimmung generiert wurde.

Wenn ein solcher uneingeschränkter Zugang ausnahmsweise nicht beantragt wird, verzeichnet die benannte Behörde die Begründung für die Nichtbeantragung, die in der nationalen Datei rückverfolgbar sein muss. Europol verzeichnet die Begründung in der entsprechenden Datei.

(3) Der vollständige Zugang zu den im Eurodac gespeicherten Daten, welche für die Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten erforderlich sind, unterliegt weiterhin den Bedingungen und Verfahren, die im entsprechenden Rechtsinstrument festgelegt sind.

Artikel 23

Datenspeicherung im gemeinsamen Speicher für Identitätsdaten

(1) Die in Artikel 18 Absätze 1, 2 und 4 genannten Daten werden im CIR automatisch nach Maßgabe der Datenspeicherungsbestimmungen der Verordnung (EU) 2019/816 gelöscht.

(2) Die individuellen Dateien werden im CIR nur so lange gespeichert, wie die entsprechenden Daten in mindestens einem der EU-Informationssysteme gespeichert werden, von dem Daten im CIR enthalten sind. Durch die Erstellung einer Verknüpfung wird die Speicherfrist der einzelnen durch die Verknüpfung bezeichneten Daten nicht berührt.

Artikel 24

Führen von Protokollen

(1) Unbeschadet des Artikels 29 der Verordnung (EU) 2019/816 führt eu-LISA Protokolle sämtlicher im CIR erfolgenden Datenverarbeitungsvorgänge gemäß den Absätzen 2, 3 und 4 des vorliegenden Artikels.

(2) eu-LISA führt Protokolle sämtlicher im CIR gemäß Artikel 20 erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat oder Stelle der Union, der bzw. die die Abfrage vornimmt,

b) Zweck des Zugriffs vonseiten des Nutzers, der die Abfrage über den CIR vornimmt,

c) Datum und Uhrzeit der Abfrage,

d) Art der für die Abfrage verwendeten Daten,

e) Ergebnisse der Abfrage.

(3) eu-LISA führt Protokolle sämtlicher im CIR gemäß Artikel 21 erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat oder Stelle der Union, der bzw. die die Abfrage vornimmt,

b) Zweck des Zugriffs vonseiten des Nutzers, der die Abfrage über den CIR vornimmt,

c) Datum und Uhrzeit der Abfrage,

d) falls eine Verknüpfung erstellt wird, die für die Abfrage verwendeten Daten und die Ergebnisse der Abfrage mit Angabe des EU-Informationssystems, aus dem die Daten stammen,

(4) eu-LISA führt Protokolle sämtlicher im CIR gemäß Artikel 22 erfolgenden Datenverarbeitungsvorgänge. Die Protokolle enthalten folgende Angaben:

a) Datum und Uhrzeit der Abfrage,

b) die für die Abfrage verwendeten Daten,

c) Ergebnisse der Abfrage,

d) Mitgliedstaat oder Stelle der Union, der bzw. die den CIR abfragen.

Die zuständige Aufsichtsbehörde nach Artikel 41 der Richtlinie (EU) 2016/680 oder der Europäische Datenschutzbeauftragte nach Artikel 43 der Verordnung (EU) 2016/794 überprüft regelmäßig, spätestens jedoch alle sechs Monate, die betreffenden Zugangsprotokolle darauf, ob die Verfahren und Bedingungen nach Artikel 22 Absätze 1 und 2 der vorliegenden Verordnung eingehalten wurden.

(5) Jeder Mitgliedstaat führt Protokolle über die Abfragen, die seine zur Nutzung des CIR ordnungsgemäß ermächtigten Behörden und die Bediensteten dieser Behörden gemäß den Artikeln 20, 21 und 22 durchführen. Jede Stelle der Union führt Protokolle über die Abfragen, die ihre ordnungsgemäß ermächtigten Bediensteten gemäß den Artikeln 21 und 22 durchführen.

Zusätzlich führt jeder Mitgliedstaat für jeden Zugang zum CIR nach Artikel 22 folgende Protokolle:

a) nationales Aktenzeichen,

b) Zugangszweck,

c) nach Maßgabe der nationalen Vorschriften die eindeutige Nutzerkennung des Beamten, der die Abfrage vorgenommen hat, und des Beamten, der die Abfrage angeordnet hat.

(6) Gemäß der Verordnung (EU) 2016/794 führt Europol für jeden Zugang zum CIR nach Artikel 22 der vorliegenden Verordnung Protokolle der eindeutigen Nutzerkennung des Beamten, der die Abfrage vorgenommen hat, und des Beamten, der die Abfrage angeordnet hat.

(7) Die in den Absätzen 2 bis 6genannten Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald die Protokolle nicht mehr für das Kontrollverfahren benötigt werden.

(8) eu-LISA speichert die Protokolle über die Chronik der Daten in individuellen Dateien. eu-LISA löscht solche Protokolle automatisch, sobald die Daten gelöscht werden.

KAPITEL V

Detektor für Mehrfachidentitäten

Artikel 25

Detektor für Mehrfachidentitäten

(1) Zur Unterstützung des Funktionierens des CIR und der Ziele des EES, des VIS, des ETIAS, von Eurodac, des SIS und des ECRIS-TCN wird ein Detektor für Mehrfachidentitäten (MID) eingerichtet, der Identitätsbestätigungsdateien nach Artikel 34 erstellt und speichert, die Verknüpfungen zwischen in den EU-Informationssystemen einschließlich des CIR und des SIS enthaltenen Daten enthält und die Aufdeckung von Mehrfachidentitäten ermöglicht, mit dem doppelten Ziel, Identitätsprüfungen zu vereinfachen und Identitätsbetrug zu bekämpfen.

(2) Der MID umfasst

a) eine zentrale Infrastruktur, die Verknüpfungen und Angaben zu EU-Informationssystemen speichert;

b) eine sichere Kommunikationsinfrastruktur, über die der MID mit dem SIS und den zentralen Infrastrukturen des ESP und des CIR verbunden ist.

(3) eu-LISA entwickelt den MID und sorgt für seine technische Verwaltung.

Artikel 26

Zugriff auf den Detektor für Mehrfachidentitäten

(1) Für die Zwecke der manuellen Verifizierung verschiedener Identitäten nach Artikel 29 erhalten folgende Stellen Zugriff auf die im MID gespeicherten Daten nach Artikel 34:

a) das SIRENE-Büro des Mitgliedstaats, der eine SIS-Ausschreibung gemäß der Verordnung (EU) 2018/1862 eingibt oder aktualisiert;

b) die Zentralbehörden des Urteilsmitgliedstaats bei der Eingabe oder Änderung von Daten im ECRIS-TCN nach Artikel 5 oder nach Artikel 9 der Verordnung (EU) 2019/816

(2) Die mitgliedstaatlichen Behörden und die Stellen der Union, die Zugang zu mindestens einem in den CIR integrierten EU-Informationssystem oder zum SIS haben, erhalten über rote Verknüpfungen nach Artikel 32 Zugang zu den in Artikel 34 Buchstaben a und b genannten Daten.

(3) Die mitgliedstaatlichen Behörden und die Stellen der Union haben Zugang zu weißen Verknüpfungen nach Artikel 33, wenn sie Zugang zu den beiden EU-Informationssystemen haben, die die Daten enthalten, zwischen denen die weiße Verknüpfung erstellt wurde.

(4) Die mitgliedstaatlichen Behörden und die Stellen der Union haben Zugang zu grünen Verknüpfungen nach Artikel 31, wenn sie Zugang zu den beiden EU-Informationssystemen haben, die die Daten enthalten, zwischen denen die grüne Verknüpfung erstellt wurde, und eine Abfrage dieser Informationssysteme eine Übereinstimmung bei den beiden verknüpften Datensätzen ergeben hat.

Artikel 27

Prüfung auf Mehrfachidentitäten

(1) Im CIR und im SIS wird eine Prüfung auf Mehrfachidentitäten eingeleitet, wenn

a) im SIS nach den Kapiteln VI bis IX der Verordnung (EU) 2018/1862 eine Ausschreibung zu einer Person erstellt oder aktualisiert wird;

b) im ECRIS-TCN nach Artikel 5 oder nach Artikel 9 der Verordnung (EU) 2019/816 ein Datensatz angelegt oder geändert wird.

(2) Wenn die in einem EU-Informationssystem enthaltenen Daten nach Absatz 1 biometrische Daten umfassen, nutzen der CIR und das zentrale SIS den gemeinsamen BMS für die Prüfung auf Mehrfachidentitäten. Der gemeinsame BMS vergleicht die aus neuen biometrischen Daten generierten biometrischen Templates mit den bereits im gemeinsamen BMS vorhandenen biometrischen Templates, um zu überprüfen, ob die zu derselben Person gehörenden Daten bereits im CIR oder im zentralen SIS gespeichert sind.

(3) Zusätzlich zu dem in Absatz 2 genannten Vorgang nutzen der CIR und das zentrale SIS das ESP, um anhand der folgenden Daten die im zentralen SIS bzw. im CIR gespeicherten Daten zu durchsuchen:

a) Nachnamen, Vornamen, Geburtsnamen, frühere Namen und Aliasnamen, Geburtsort, Geburtsdatum, Geschlecht und sämtliche Staatsangehörigkeiten gemäß Artikel 20 Absatz 3 der Verordnung (EU) 2018/1862;

b) Nachname (Familienname), Vorname(n), Geburtsdatum, Geburtsort (Gemeinde und Staat), Staatsangehörigkeit(en) und Geschlecht gemäß Artikel 5 Absatz 1 Buchstabe a der Verordnung (EU) 2019/816;

(4) Zusätzlich zu dem in den Absätzen 2 und 3 genannten Vorgang nutzen der CIR und das zentrale SIS das ESP, um anhand der Reisedokumentendaten die im zentralen SIS bzw. im CIR gespeicherten Daten zu durchsuchen.

(5) Die Prüfung auf Mehrfachidentitäten wird nur durchgeführt, um Daten, die in einem EU-Informationssystem vorhanden sind, mit Daten, die in anderen EU-Informationssystemen vorhanden sind, zu vergleichen.

Artikel 28

Ergebnisse der Prüfung auf Mehrfachidentitäten

(1) Wenn die Abfragen nach Artikel 27 Absätze 2, 3 und 4 keine Übereinstimmung ergeben, werden die in Artikel 27 Absatz 1 genannten Verfahren gemäß den einschlägigen Rechtsinstrumenten fortgesetzt.

(2) Wenn die Abfrage nach Artikel 27 Absätze 2, 3 und 4 eine oder mehrere Übereinstimmungen ergibt, erstellen der CIR und gegebenenfalls das SIS eine Verknüpfung zwischen den für die Abfrage verwendeten Daten und den Daten, die zu der Übereinstimmung geführt haben.

Wenn mehrere Übereinstimmungen gemeldet werden, wird eine Verknüpfung zwischen allen Daten, die zu der Übereinstimmung geführt haben, erstellt. Wenn die Daten bereits verknüpft waren, wird die bestehende Verknüpfung auf die zur Abfrage verwendeten Daten ausgeweitet.

(3) Wenn die Abfrage nach Artikel 27 Absätze 2, 3 und 4 eine oder mehrere Übereinstimmungen ergibt und die Identitätsdaten der verknüpften Dateien gleich oder ähnlich sind, wird eine weiße Verknüpfung nach Artikel 33 erstellt.

(4) Wenn die Abfrage nach Artikel 27 Absätze 2, 3 und 4 eine oder mehrere Übereinstimmungen ergibt und die Identitätsdaten der verknüpften Dateien nicht als ähnlich angesehen werden können, wird eine gelbe Verknüpfung nach Artikel 30 erstellt, und das Verfahren nach Artikel 29 gelangt zur Anwendung.

(5) Die Kommission erlässt gemäß Artikel 69 delegierte Rechtsakte zur Festlegung der Verfahren für die Bestimmung der Fälle, in denen Identitätsdaten als identisch oder ähnlich angesehen werden können.

(6) Die Verknüpfungen werden in der Identitätsbestätigungsdatei gemäß Artikel 34 gespeichert.

(7) Die Kommission legt in Zusammenarbeit mit eu-LISA die technischen Vorschriften für die Erstellung von Verknüpfungen zwischen Daten aus unterschiedlichen EU-Informationssystemen im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 70 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 29

Manuelle Verifizierung verschiedener Identitäten und zuständige Behörden

(1) Unbeschadet von Absatz 2 sind für die manuelle Verifizierung verschiedener Identitäten folgende Behörden zuständig:

a) das SIRENE-Büro des Mitgliedstaats bei Übereinstimmungen, die bei der Erfassung oder Aktualisierung einer SIS-Ausschreibung gemäß der Verordnung (EU) 2018/1862 erzielt wurden;

b) bei Übereinstimmungen, die bei der Erfassung oder Änderung von Daten im ECRIS-TCN nach Artikel 5 oder Artikel 9 der Verordnung (EU 2019/816 erzielt wurden, die Zentralbehörden des Urteilsmitgliedstaats.

Der MID gibt die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde in der Identitätsbestätigungsdatei an.

(2) Die für die manuelle Verifizierung verschiedener Identitäten in der Identitätsbestätigungsdatei zuständige Behörde ist das SIRENE-Büro des Mitgliedstaats, der die Ausschreibung eingegeben hat, wenn eine Verknüpfung zu Daten erstellt wird, die in einer Ausschreibung

a) von Personen zum Zwecke der Übergabe- oder Auslieferungshaft nach Artikel 26 der Verordnung (EU) 2018/1862 enthalten sind;

b) von Vermissten oder schutzbedürftigen Personen nach Artikel 32 der Verordnung (EU) 2018/1862 enthalten sind;

c) von Personen, die im Hinblick auf ihre Teilnahme an einem Gerichtsverfahren gesucht werden, nach Artikel 34 der Verordnung (EU) 2018/1862 enthalten sind;

d) von Personen für verdeckte Kontrollen, Ermittlungsanfragen oder gezielte Kontrollen nach Artikel 36 der Verordnung (EU) 2018/1862 enthalten sind.

(3) Die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde erhält Zugriff auf die in der betreffenden Identitätsbestätigungsdatei enthaltenen verknüpften Daten und auf die im CIR und gegebenenfalls im SIS verknüpften Identitätsdaten. Sie prüft die verschiedenen Identitäten unverzüglich. Sobald die Prüfung abgeschlossen ist, aktualisiert sie die Verknüpfung gemäß den Artikeln 31, 32 und 33 und fügt diese unverzüglich zur Identitätsbestätigungsdatei hinzu.

(4) Wenn mehr als eine Verknüpfung erstellt wird, prüft die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde jede Verknüpfung gesondert.

(5) Wenn Daten, die zu einer Übereinstimmung geführt haben, bereits verknüpft sind, berücksichtigt die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde die bestehenden Verknüpfungen bei der Prüfung, ob neue Verknüpfungen erstellt werden müssen.

Artikel 30

Gelbe Verknüpfung

(1) Wurde noch keine manuelle Verifizierung verschiedener Identitäten vorgenommen, wird eine Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen in folgenden Fällen als gelb klassifiziert:

a) Die verknüpften Daten enthalten dieselben biometrischen Daten, aber ähnliche oder unterschiedliche Identitätsdaten;

b) die verknüpften Daten enthalten unterschiedliche Identitätsdaten, aber dieselben Reisedokumentendaten, und in mindestens eines der EU-Informationssysteme enthält keine biometrischen Daten zu der betroffenen Person;

c) die verknüpften Daten enthalten dieselben Identitätsdaten, aber unterschiedliche biometrische Daten;

d) die verknüpften Daten enthalten ähnliche oder unterschiedliche Identitätsdaten, dieselben Reisedokumentendaten, aber unterschiedliche biometrische Daten.

(2) Wenn eine Verknüpfung gemäß Absatz 1 als gelb klassifiziert wird, gelangt das Verfahren nach Artikel 29 zur Anwendung.

Artikel 31

Grüne Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen wird als grün klassifiziert, wenn

a) die verknüpften Daten unterschiedliche biometrischen Daten, aber dieselben Identitätsdaten enthalten und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde festgestellt hat, dass sich die verknüpften Daten auf zwei unterschiedliche Personen beziehen;

b) die verknüpften Daten unterschiedliche biometrischen Daten, ähnliche oder unterschiedliche Identitätsdaten und dieselben Reisedokumentendaten enthalten und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde festgestellt hat, dass sich die verknüpften Daten auf zwei unterschiedliche Personen beziehen;

c) die verknüpften Daten unterschiedliche Identitätsdaten, aber dieselben Reisedokumentendaten enthalten, mindestens eines der EU-Informationssysteme keine biometrischen Daten zu der betroffenen Person enthält und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde festgestellt hat, dass sich die verknüpften Daten auf zwei unterschiedliche Personen beziehen.

(2) Wenn eine Abfrage im CIR oder im SIS durchgeführt wird und eine grüne Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen besteht, zeigt der MID an, dass die Identitätsdaten der verknüpften Daten nicht ein und dieselbe Person bezeichnen.

(3) Wenn eine mitgliedstaatliche Behörde Belege hat, aus denen hervorgeht, dass eine grüne Verknüpfung im MID unrichtig erfasst wurde, dass eine grüne Verknüpfung nicht dem neuesten Stand entspricht oder dass mit der Verarbeitung der Daten im MID oder den EU-Informationssystemen gegen diese Verordnung verstoßen wurde, muss sie die betreffenden im CIR und im SIS gespeicherten Daten überprüfen und die Verknüpfung gegebenenfalls unverzüglich berichtigen oder aus dem MID löschen. Diese mitgliedstaatliche Behörde setzt unverzüglich den für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaat in Kenntnis.

Artikel 32

Rote Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen wird in folgenden Fällen als rot klassifiziert:

a) Die verknüpften Daten enthalten dieselben biometrischen Daten, aber ähnliche oder unterschiedliche Identitätsdaten, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten in ungerechtfertigter Weise auf ein und dieselbe Person beziehen;

b) die verknüpften Daten enthalten dieselben, ähnliche oder unterschiedliche Identitätsdaten und die gleichen Reisedokumentendaten, aber unterschiedliche biometrische Daten, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten auf zwei unterschiedliche Personen beziehen, von denen mindestens eine dasselbe Reisedokument in ungerechtfertigter Weise benutzt;

c) die verknüpften Daten enthalten dieselben Identitätsdaten, aber unterschiedliche biometrische Daten und unterschiedliche oder keine Reisedokumentendaten, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten in ungerechtfertigter Weise auf zwei unterschiedliche Personen bezeichnen;

d) die verknüpften Daten enthalten unterschiedliche Identitätsdaten aber dieselben Reisedokumentendaten, mindestens eines der EU-Informationssysteme enthält keine biometrischen Daten zu der betreffenden Person, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten in ungerechtfertigter Weise auf ein und dieselbe Person beziehen.

(2) Wenn eine Abfrage im CIR oder im SIS durchgeführt wird und eine rote Verknüpfung zwischen Daten in zwei oder mehr EU-Informationssystemen besteht, zeigt der MID die in Artikel 34 genannten Daten an. Bei etwaigen Folgemaßnahmen zu einer roten Verknüpfung sind die einschlägigen Bestimmungen des Unionsrechts und des nationalen Rechts einzuhalten, wobei sich etwaige rechtliche Folgen für die betreffende Person nur auf die einschlägigen Daten zu dieser Person gründen dürfen. Aufgrund der bloßen Existenz einer roten Verknüpfung entstehen für die betroffene Person keine rechtlichen Folgen.

(3) Wenn eine rote Verknüpfung zwischen Daten im EES, im VIS, im ETIAS, in Eurodac oder im ECRIS-TCN erstellt wird, wird die im CIR gespeicherte individuelle Datei gemäß Artikel 19 Absatz 2 aktualisiert.

(4) Unbeschadet der Bestimmungen für die Handhabung von Ausschreibungen im SIS in den Verordnungen (EU) 2018/1860, (EU) 2018/1861 und (EU) 2018/1862 und unbeschadet der erforderlichen Einschränkungen zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass bei der Erstellung einer roten Verknüpfung keine nationalen Ermittlungen beeinträchtigt werden, teilt die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde der betroffenen Person mit, dass illegale Mehrfachidentitätsdaten vorliegen, und teilt der Person die einmalige Kennnummer gemäß Artikel 34 Buchstabe c der vorliegenden Verordnung, die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde gemäß Artikel 34 Buchstabe d der vorliegenden Verordnung und die Adresse des nach Artikel 49 der vorliegenden Verordnung eingerichteten Web-Portals mit.

(5) Die in Absatz 4 genannten Informationen werden von der für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde schriftlich anhand eines Standardformulars zur Verfügung gestellt. Die Kommission legt den Inhalt und die Darstellung dieses Formulars im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 70 Absatz 2 genannten Prüfverfahren erlassen.

(6) Wenn eine rote Verknüpfung erstellt wird, unterrichtet der MID automatisch die Behörden, die für die verknüpften Daten zuständig sind.

(7) Wenn eine Behörde eines Mitgliedstaates oder eine Stelle der Union mit Zugriff auf den CIR oder das SIS Belege dafür hat, dass eine rote Verknüpfung im MID unrichtig erfasst wurde oder dass mit der Verarbeitung der Daten im MID, im CIR oder im SIS gegen diese Verordnung verstoßen wurde, muss die Behörde oder Stelle die betreffenden im CIR oder SIS gespeicherten Daten überprüfen und,

a) wenn sich die Verknüpfung auf eine der SIS-Ausschreibungen gemäß Artikel 29 Absatz 2 bezieht, umgehend das zuständige SIRENE-Büro des Mitgliedstaats informieren, das die SIS-Ausschreibung erstellt hat;

b) in allen anderen Fällen die Verknüpfung umgehend entweder berichtigen oder aus dem MID löschen.

Wird ein SIRENE-Büro gemäß Unterabsatz 1 Buchstabe a kontaktiert, verifiziert es die von der mitgliedstaatlichen Behörde oder Stelle der Union vorgelegten Belege unverzüglich und berichtigt gegebenenfalls umgehend die Verknüpfung oder löscht diese aus dem MID.

Die mitgliedstaatliche Behörde, die die Belege erhält, informiert unverzüglich die Behörde des Mitgliedstaats, die für die manuelle Verifizierung verschiedener Identitäten zuständig ist, über jegliche Berichtigung oder Löschung einer roten Verknüpfung.

Artikel 33

Weiße Verknüpfung

(1) Eine Verknüpfung zwischen Daten aus zwei oder mehr EU-Informationssystemen wird in folgenden Fällen als weiß klassifiziert:

a) Die verknüpften Daten enthalten dieselben biometrischen Daten und dieselben oder ähnliche Identitätsdaten;

b) die verknüpften Daten enthalten dieselben oder ähnliche Identitätsdaten, dieselben Reisedokumentendaten und in mindestens einem der EU-Informationssysteme liegen keine biometrischen Daten zu der betroffenen Person vor;

c) die verknüpften Daten enthalten dieselben biometrischen Daten, dieselben Reisedokumentendaten und ähnliche Identitätsdaten;

d) die verknüpften Daten enthalten dieselben biometrischen Daten, aber ähnliche oder unterschiedliche Identitätsdaten, und die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde hat festgestellt, dass sich die verknüpften Daten in gerechtfertigter Weise auf ein und dieselbe Person beziehen.

(2) Wenn eine Abfrage im CIR oder im SIS durchgeführt wird und eine weiße Verknüpfung zwischen Daten in zwei oder mehr EU-Informationssystemen besteht, zeigt der MID an, dass die Identitätsdaten der verknüpften Daten ein und dieselbe Person bezeichnen. In der Antwort der abgefragten EU-Informationssysteme werden gegebenenfalls alle verknüpften Daten zu der Person angezeigt, wodurch eine Übereinstimmung auf Basis der Daten, die durch die weiße Verknüpfung verknüpft sind, erfolgt, soweit die Behörde, welche die Abfrage durchführt, nach dem Unionsrecht oder nationalen Recht Zugriff auf die verknüpften Daten hat.

(3) Wenn eine weiße Verknüpfung zwischen Daten im EES, im VIS, im ETIAS, in Eurodac oder im ECRIS-TCN erstellt wird, wird die im CIR gespeicherte individuelle Datei gemäß Artikel 19 Absatz 2 aktualisiert.

(4) Wenn nach einer manuellen Verifizierung von verschiedenen Identitäten eine weiße Verknüpfung erstellt wird, teilt die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde der betreffenden Person unbeschadet der Bestimmungen für die Handhabung von Ausschreibungen im SIS in den Verordnungen (EU) 2018/1860, (EU) 2018/1861 und (EU) 2018/1862 und unbeschadet der erforderlichen Einschränkungen zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass keine nationalen Ermittlungen beeinträchtigt werden, mit, dass ähnliche oder verschiedene Identitätsdaten vorliegen, und teilt der Person die einmalige Kennnummer gemäß Artikel 34 Buchstabe c der vorliegenden Verordnung, die für die manuelle Verifizierung verschiedener Identitäten zuständige Behörde gemäß Artikel 34 Buchstabe d der vorliegenden Verordnung und die Adresse des nach Artikel 49 der vorliegenden Verordnung eingerichteten Web-Portals mit.

(5) Wenn eine mitgliedstaatliche Behörde Belege hat, aus denen hervorgeht, dass eine weiße Verknüpfung im MID unrichtig erfasst wurde, dass eine weiße Verknüpfung nicht dem neuesten Stand entspricht oder dass mit der Verarbeitung der Daten im MID oder in den EU-Informationssystemen gegen diese Verordnung verstoßen wurde, muss sie die betreffenden im CIR und im SIS gespeicherten Daten überprüfen und die Verknüpfung gegebenenfalls unverzüglich berichtigen oder aus dem MID löschen. Diese mitgliedstaatliche Behörde setzt unverzüglich den für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaat in Kenntnis.

(6) Die in Absatz 4 genannten Informationen werden von der für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde schriftlich anhand eines Standardformulars zur Verfügung gestellt. Die Kommission legt den Inhalt und die Darstellung dieses Formulars im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 70 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 34

Identitätsbestätigungsdatei

Die Identitätsbestätigungsdatei enthält folgende Daten:

a) die in den Artikeln 30 bis 33 genannten Verknüpfungen;

b) eine Angabe der EU-Informationssysteme, in denen die verknüpften Daten gespeichert sind;

c) eine einmalige Kennnummer, die das Abrufen der verknüpften Daten aus den entsprechenden EU-Informationssystemen ermöglicht;

d) eine Angabe der für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde;

e) das Datum der Erstellung oder jeder Aktualisierung der Verknüpfung.

Artikel 35

Datenspeicherung im Detektor für Mehrfachidentitäten

Die Identitätsbestätigungsdateien und die in ihnen enthaltenen Daten einschließlich der Verknüpfungen werden im MID nur so lange gespeichert, wie die verknüpften Daten in zwei oder mehr EU-Informationssystemen gespeichert werden. Sie werden automatisch aus dem MID gelöscht.

Artikel 36

Führen von Protokollen

(1) eu-LISA führt Protokolle über alle Datenverarbeitungsvorgänge im MID. Die Protokolle enthalten folgende Angaben:

a) Mitgliedstaat, der die Abfrage vornimmt;

b) Zweck des Zugriffs des Nutzers;

c) Datum und Uhrzeit der Abfrage,

d) Art der für die Abfrage verwendeten Daten;

e) Verweis auf die verknüpften Daten;

f) Chronik der Identitätsbestätigungsdatei.

(2) Jeder Mitgliedstaat führt Protokolle über die Abfragen, die seine zur Nutzung des MID ordnungsgemäß ermächtigten Behörden und deren Bedienstete durchführen. Jede Stelle der Union führt Protokolle über die Abfragen, die ihre ordnungsgemäß ermächtigten Bediensteten durchführen.

(3) Die in den Absätzen 1 und 2 genannten Protokolle dürfen nur zur datenschutzrechtlichen Kontrolle, einschließlich der Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung sowie zur Sicherstellung der Datensicherheit und -integrität verwendet werden. Die Protokolle werden in geeigneter Weise vor unbefugtem Zugriff geschützt und ein Jahr nach ihrer Erstellung gelöscht. Werden sie jedoch für ein bereits eingeleitetes Kontrollverfahren benötigt, werden sie gelöscht, sobald die Protokolle nicht mehr für das Kontrollverfahren benötigt werden.

KAPITEL VI

Maßnahmen zur Unterstützung der Interoperabilität

Artikel 37

Datenqualität

(1) Unbeschadet der Verantwortlichkeiten der Mitgliedstaaten für die Qualität der in die Systeme eingegebenen Daten führt eu-LISA für die im SIS, in Eurodac, im ECRIS-TCN, im gemeinsamen BMS und im CIR gespeicherten Daten Mechanismen und Verfahren für die automatische Datenqualitätskontrolle ein.

(2) eu-LISA setzt Mechanismen für die Bewertung der Richtigkeit des gemeinsamen BMS, gemeinsame Datenqualitätsindikatoren und die Mindestqualitätsstandards für die Speicherung von Daten im SIS, in Eurodac, im ECRIS-TCN, im gemeinsamen BMS und im CIR um.

Nur Daten, die den Mindestqualitätsstandards genügen, dürfen in das SIS, Eurodac, das ECRIS-TCN, den gemeinsamen BMS, den CIR und den MID eingegeben werden.

(3) eu-LISA legt den Mitgliedstaaten regelmäßig Berichte über die Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie die gemeinsamen Datenqualitätsindikatoren vor. Ferner legt eu-LISA der Kommission regelmäßig Berichte über die festgestellten Probleme und die betroffenen Mitgliedstaaten vor. eu-LISA legt diese Berichte auf Anfrage auch dem Europäischen Parlament und dem Rat vor. Keiner der in diesem Absatz genannten Berichte darf personenbezogene Daten enthalten.

(4) Die Einzelheiten der Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie der gemeinsamen Datenqualitätsindikatoren und der Mindestqualitätsstandards für die Speicherung von Daten im SIS, in Eurodac, im ECRIS-TCN, im gemeinsamen BMS und im CIR, insbesondere bei biometrischen Daten, werden in Durchführungsrechtsakten festgelegt. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 70 Absatz 2 genannten Prüfverfahren erlassen.

(5) Ein Jahr nach der Einführung der Mechanismen und Verfahren für die automatische Datenqualitätskontrolle, der gemeinsamen Datenqualitätsindikatoren und der Mindestdatenqualitätsstandards und danach jedes Jahr evaluiert die Kommission die Umsetzung der Datenqualität durch die Mitgliedstaaten und gibt erforderlichenfalls Empfehlungen ab. Die Mitgliedstaaten legen der Kommission einen Aktionsplan zur Beseitigung etwaiger im Evaluierungsbericht festgestellter Mängel und insbesondere zur Lösung von Problemen bei der Datenqualität, die sich aus fehlerhaften Daten in EU-Informationssystemen ergeben, vor. Die Mitgliedstaaten erstatten der Kommission regelmäßig Bericht über die Fortschritte bei der Umsetzung dieses Aktionsplans, bis dieser vollständig umgesetzt ist.

Die Kommission übermittelt den Evaluierungsbericht dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten, dem Europäischen Datenschutzausschuss und der durch die Verordnung (EG) Nr. 168/2007 des Rates ([37]) eingerichteten Agentur der Europäischen Union für Grundrechte.

Artikel 38

Universelles Nachrichtenformat (Universal Message Format)

(1) Das universelle Nachrichtenformat (UMF) wird eingeführt. Mit dem UMF werden Standards für bestimmte inhaltliche Elemente des grenzüberschreitenden Informationsaustauschs zwischen Informationssystemen, Behörden und/oder Organisationen im Bereich Justiz und Inneres festgelegt.

([37]) Verordnung (EG) Nr. 168/2007 des Rates vom 15. Februar 2007 zur Errichtung einer Agentur der Europäischen Union für Grundrechte (ABl. L 53 vom 22.2.2007, S. 1).

(2) Der UMF-Standard ist bei der Entwicklung von Eurodac, des ECRIS-TCN, des ESP, des CIR und des MID sowie gegebenenfalls bei der Entwicklung neuer Modelle für den Informationsaustausch und neuer Informationssysteme im Bereich Justiz und Inneres durch eu-LISA oder eine andere Stelle der Union zu verwenden.

(3) Die Kommission erlässt einen Durchführungsrechtsakt zur Festlegung und Entwicklung des in Absatz 1 dieses Artikels genannten UMF-Standards. Dieser Durchführungsrechtsakt wird gemäß dem in Artikel 70 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 39

Zentraler Speicher für Berichte und Statistiken

(1) Es wird ein zentraler Speicher für Berichte und Statistiken (CRRS) eingerichtet, um die Ziele von Eurodac, des SIS sowie des ECRIS-TCN gemäß den geltenden Rechtsinstrumenten zu unterstützen und systemübergreifende statistische Daten und analytische Berichte für politische und operative Zwecke sowie für die Zwecke der Datenqualität bereitzustellen.

(2) eu-LISA sorgt an ihren technischen Standorten für die Einrichtung, die Implementierung und das Hosting des CRRS, das logisch nach den EU-Informationssystemen getrennt die Daten und Statistiken nach Artikel 74 der Verordnung (EU) 2018/1862 und Artikel 32 der Verordnung (EU) 2019/816 enthält. Der Zugang zum CRRS erfolgt in Form eines kontrollierten, gesicherten Zugangs und spezifischen Nutzerprofilen und wird den in Artikel 74 der Verordnung (EU) 2018/1862 und Artikel 32 der Verordnung (EU) 2019/816 genannten Behörden ausschließlich zu Berichterstattungs- und Statistikzwecken gewährt.

(3) eu-LISA anonymisiert die Daten und speichert diese anonymisierten Daten im CRRS. Die Anonymisierung der Daten erfolgt nach einem automatisierten Verfahren.

Die im CRRS enthaltenen Daten dürfen keine Identifizierung von Einzelpersonen ermöglichen.

(4) Der CRRS umfasst

a) die für die Anonymisierung von Daten notwendigen Instrumente;

b) eine zentrale Infrastruktur, die aus einem Datenregister anonymisierter Daten besteht;

c) eine sichere Kommunikationsinfrastruktur, über die der CRRS mit dem SIS, Eurodac und dem ECRIS-TCN sowie den zentralen Infrastrukturen des gemeinsamen BMS, des CIR und des MID verbunden ist.

(5) Die Kommission erlässt einen delegierten Rechtsakt gemäß Artikel 69, um detaillierte Bestimmungen über den Betrieb des CRRS, einschließlich spezifischer Garantien für die Verarbeitung personenbezogener Daten gemäß den Absätzen 2 und 3 des vorliegenden Artikels und der für den Speicher geltenden Sicherheitsvorschriften festzulegen.

KAPITEL VII

Datenschutz

Artikel 40

Für die Verarbeitung Verantwortlicher

(1) Für die Verarbeitung von Daten im gemeinsamen BMS sind die mitgliedstaatlichen Behörden, die jeweils für die Verarbeitung in Eurodac, im SIS und im ECRIS-TCN verantwortlich sind, Verantwortliche im Sinne des Artikels 4 Nummer 7 der Verordnung (EU) 2016/679 oder des Artikels 3 Nummer 8 der Richtlinie (EU) 2016/680 für die aus den in Artikel 13 der vorliegenden Verordnung genannten Daten generierten biometrischen Templates, die sie in die zugrunde liegenden Systeme eingeben, und tragen die Verantwortung für die Verarbeitung der biometrischen Templates im gemeinsamen BMS.

(2) Für die Verarbeitung von Daten im CIR sind die mitgliedstaatlichen Behörden, die jeweils für die Verarbeitung in Eurodac und im ECRIS-TCN verantwortlich sind, Verantwortliche im Sinne des Artikels 4 Nummer 7 der Verordnung (EU) 2016/679 oder Artikel 3 Nummer 8 der Richtlinie (EU) 2016/680 für die in Artikel 18 der vorliegenden Verordnung genannten Daten, die sie in die zugrunde liegenden Systeme eingeben, und tragen die Verantwortung für die Verarbeitung dieser personenbezogenen Daten im CIR.

(3) Für die Verarbeitung von Daten im MID

a) ist die Europäische Agentur für die Grenz- und Küstenwache ein für die Verarbeitung Verantwortlicher im Sinne des Artikels 3 Nummer 8 der Verordnung (EU) 2018/1725 für die Verarbeitung personenbezogener Daten durch die ETIAS-Zentralstelle;

b) sind die mitgliedstaatlichen Behörden, die Daten in der Identitätsbestätigungsdatei hinzufügen oder ändern, Verantwortliche im Sinne des Artikels 4 Nummer 7 der Verordnung (EU) 2016/679 oder des Artikels 3 Nummer 8 der Richtlinie (EU) 2016/680 und tragen die Verantwortung für die Verarbeitung personenbezogener Daten im MID.

(4) Zum Zwecke der datenschutzrechtlichen Kontrolle, einschließlich zur Prüfung der Zulässigkeit einer Abfrage und der Rechtmäßigkeit der Datenverarbeitung, haben die für die Verarbeitung Verantwortlichen Zugang zu den Protokollen nach den Artikeln 10, 16, 24 und 36 für die Eigenkontrolle nach Artikel 44.

Artikel 41

Datenauftragsverarbeiter

Für die Verarbeitung personenbezogener Daten im gemeinsamen BMS, im CIR und im MID ist eu-LISA Datenauftragsverarbeiter im Sinne des Artikels 3 Nummer 12 Buchstabe a der Verordnung (EU) 2018/1725.

Artikel 42

Sicherheit der Verarbeitung

(1) eu-LISA, die ETIAS-Zentralstelle, Europol und die mitgliedstaatlichen Behörden gewährleisten die Sicherheit der Verarbeitung personenbezogener Daten nach Maßgabe dieser Verordnung. Bei der Erfüllung sicherheitsbezogener Aufgaben arbeiten eu-LISA, die ETIAS-Zentralstelle, Europol und die mitgliedstaatlichen Behörden zusammen.

(2) Unbeschadet des Artikels 33 der Verordnung (EU) 2018/1725 ergreift eu-LISA die erforderlichen Maßnahmen, um die Sicherheit der Interoperabilitätskomponenten und der mit ihnen verbundenen Kommunikationsinfrastruktur sicherzustellen.

(3) Insbesondere trifft eu-LISA die erforderlichen Maßnahmen, einschließlich der Annahme eines Sicherheitsplans, eines Betriebskontinuitätsplans und eines Notfallwiederherstellungsplans, um

a) die Daten physisch zu schützen, unter anderem durch Aufstellung von Notfallplänen für den Schutz kritischer Infrastrukturen;

b) Unbefugten den Zugang zu Datenverarbeitungseinrichtungen und -anlagen zu verwehren;

c) zu verhindern, dass Datenträger unbefugt gelesen, kopiert, verändert oder entfernt werden;

d) die unbefugte Dateneingabe sowie die unbefugte Kenntnisnahme, Änderung oder Löschung gespeicherter personenbezogener Daten zu verhindern;

e) die unbefugte Datenverarbeitung sowie das unbefugte Kopieren, Ändern oder Löschen von Daten zu verhindern;

f) zu verhindern, dass automatisierte Datenverarbeitungssysteme mithilfe von Datenübertragungseinrichtungen von Unbefugten genutzt werden;

g) sicherzustellen, dass die zum Zugang zu den Interoperabilitätskomponenten berechtigten Personen nur mittels einer persönlichen Benutzerkennung und vertraulicher Zugriffsverfahren ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können;

h) sicherzustellen, dass überprüft und festgestellt werden kann, welchen Stellen personenbezogene Daten durch Datenübertragungseinrichtungen übermittelt werden können;

i) sicherzustellen, dass überprüft und festgestellt werden kann, welche Daten wann, von wem und zu welchem Zweck in den Interoperabilitätskomponenten verarbeitet wurden;

j) das unbefugte Lesen, Kopieren, Ändern oder Löschen von personenbezogenen Daten während der Übermittlung personenbezogener Daten an die oder aus den Interoperabilitätskomponenten oder während des Transports von Datenträgern zu verhindern, insbesondere durch geeignete Verschlüsselungstechniken;

k) sicherzustellen, dass eingesetzte Systeme im Störungsfall für den Normalbetrieb wiederhergestellt werden können;

l) die Zuverlässigkeit sicherzustellen, indem dafür Sorge getragen wird, dass alle Funktionsstörungen der Interoperabilitätskomponenten ordnungsgemäß gemeldet werden;

m) die Wirksamkeit der in diesem Absatz genannten Sicherheitsmaßnahmen zu überwachen, die erforderlichen organisatorischen Maßnahmen für die interne Überwachung zu treffen, um die Einhaltung dieser Verordnung sicherzustellen, und diese Sicherheitsmaßnahmen vor dem Hintergrund neuer technologischer Entwicklungen zu bewerten.

(4) Die Mitgliedstaaten, Europol und die ETIAS-Zentralstelle treffen für die Verarbeitung personenbezogener Daten durch die Behörden, die das Recht auf Zugang zu Interoperabilitätskomponenten haben, Sicherheitsmaßnahmen, die den in Absatz 3 genannten entsprechen.

Artikel 43

Sicherheitsvorfälle

(1) Jedes Ereignis, das sich auf die Sicherheit der Interoperabilitätskomponenten auswirkt oder auswirken kann und darin gespeicherte Daten beschädigen oder ihren Verlust herbeiführen kann, ist als Sicherheitsvorfall anzusehen; das gilt insbesondere, wenn möglicherweise ein unbefugter Datenzugriff erfolgt ist oder die Verfügbarkeit, die Integrität und die Vertraulichkeit von Daten tatsächlich oder möglicherweise nicht mehr gewährleistet war.

(2) Sicherheitsvorfällen ist durch eine rasche, wirksame und angemessene Reaktion zu begegnen.

(3) Unbeschadet der Meldung und Mitteilung einer Verletzung des Schutzes personenbezogener Daten gemäß Artikel 33 der Verordnung (EU) 2016/679, Artikel 30 der Richtlinie (EU) 2016/680 oder beiden Artikeln unterrichten die Mitgliedstaaten die Kommission, eu-LISA, die zuständigen Aufsichtsbehörden und den Europäischen Datenschutzbeauftragten unverzüglich über etwaige Sicherheitsvorfälle.

Unbeschadet der Artikel 34 und 35 der Verordnung (EU) 2018/1725 und Artikel 34 der Verordnung (EU) 2016/794 unterrichten die ETIAS-Zentralstelle und Europol die Kommission, eu-LISA und den Europäischen Datenschutzbeauftragten unverzüglich über etwaige Sicherheitsvorfälle.

Im Falle eines Sicherheitsvorfalls in Verbindung mit der zentralen Infrastruktur der Interoperabilitätskomponenten unterrichtet eu-LISA die Kommission und den Europäischen Datenschutzbeauftragten unverzüglich.

(4) Informationen über einen Sicherheitsvorfall, der sich auf den Betrieb der Interoperabilitätskomponenten oder die Verfügbarkeit, die Integrität und die Vertraulichkeit der Daten auswirkt oder auswirken kann, werden den Mitgliedstaaten, der ETIAS-Zentralstelle und Europol unverzüglich bereitgestellt und nach Maßgabe des von eu-LISA bereitzustellenden Plans für die Bewältigung von Sicherheitsvorfällen gemeldet.

(5) Die betroffenen Mitgliedstaaten, die ETIAS-Zentralstelle, Europol und eu-LISA arbeiten im Falle eines Sicherheitsvorfalls zusammen. Die Kommission legt die genauen Modalitäten dieser Zusammenarbeit im Wege von Durchführungsrechtsakten fest. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 70 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 44

Eigenkontrolle

Die Mitgliedstaaten und die zuständigen Stellen der Union stellen sicher, dass jede zum Zugriff auf die Interoperabilitätskomponenten berechtigte Behörde die erforderlichen Maßnahmen zur Überwachung der Einhaltung dieser Verordnung trifft und erforderlichenfalls mit der Aufsichtsbehörde zusammenarbeitet.

Die für die Verarbeitung Verantwortlichen im Sinne des Artikels 40 treffen die erforderlichen Maßnahmen, um die Ordnungsgemäßheit der Datenverarbeitung gemäß dieser Verordnung zu überwachen, unter anderem durch häufige Überprüfung der Protokolle gemäß den Artikeln 10, 16, 24 und 36, und arbeiten erforderlichenfalls mit den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten zusammen.

Artikel 45

Sanktionen

Die Mitgliedstaaten stellen sicher, dass jeder Missbrauch von Daten, jede Verarbeitung von Daten oder jeder Austausch von Daten, die dieser Verordnung zuwiderläuft, gemäß nationalem Recht geahndet werden können. Die vorgesehenen Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein.

Artikel 46

Haftung

(1) Unbeschadet des Anspruchs auf Schadenersatz durch den für die Verarbeitung Verantwortlichen oder den Datenauftragsverarbeiter und unbeschadet ihrer Haftung gemäß der Verordnung (EU) 2016/679, der Richtlinie (EU) 2016/680 und der Verordnung (EU) 2018/1725

a) hat jede Person oder jeder Mitgliedstaat, der/dem durch eine rechtswidrige Verarbeitung personenbezogener Daten oder durch andere gegen diese Verordnung verstoßende Handlungen seitens eines Mitgliedstaats ein materieller oder immaterieller Schaden entsteht, das Recht, von diesem Mitgliedstaat Schadenersatz zu verlangen;

b) hat jede Person oder jeder Mitgliedstaat, der/dem durch eine gegen diese Verordnung verstoßende Handlung seitens Europol, der Europäischen Agentur für die Grenz- und Küstenwache oder eu-LISA ein materieller oder immaterieller Schaden entsteht, das Recht, von der betreffenden Stelle Schadenersatz zu verlangen.

ter betreffende Mitgliedstaat, Europol, die Europäische Agentur für die Grenz- und Küstenwache oder eu-LISA werden vollständig oder teilweise von ihrer Haftung nach Unterabsatz 1 befreit, wenn sie nachweisen, dass sie für den Umstand, durch den der Schaden eingetreten ist, nicht verantwortlich sind.

(2) Verursacht eine Verletzung der in dieser Verordnung festgelegten Pflichten durch einen Mitgliedstaat einen Schaden an den Interoperabilitätskomponenten, haftet dieser Mitgliedstaat für den entstandenen Schaden, sofern und soweit es eu-LISA oder ein anderer durch diese Verordnung gebundener Mitgliedstaat nicht versäumt haben, angemessene Maßnahmen zur Verhinderung des Schadens oder zur Verringerung seiner Auswirkungen zu ergreifen.

(3) Die Geltendmachung von Schadenersatzansprüchen nach den Absätzen 1 und 2 gegen einen Mitgliedstaat unterliegt dem nationalen Recht des beklagten Mitgliedstaats. Die Geltendmachung von Schadenersatzansprüchen nach den Absätzen 1 und 2 gegen den für die Verarbeitung Verantwortlichen oder eu-LISA unterliegt den in den Verträgen vorgesehenen Voraussetzungen.

Artikel 47

Recht auf Information

(1) Die Behörde, die die personenbezogenen Daten erfasst, die im gemeinsamen BMS, im CIR oder im MID zu speichern sind, stellt den Personen, deren Daten erfasst werden, die Informationen zur Verfügung, die nach den Artikeln 13 und 14 der Verordnung (EU) 2016/679, den Artikeln 12 und 13 der Richtlinie (EU) 2016/680 und den Artikeln 15 und 16 der Verordnung (EU) 2018/1725 vorgeschrieben sind. Die Behörde stellt die Informationen zum Zeitpunkt der Datenerfassung zur Verfügung.

(2) Alle Informationen werden in einer in klarer und einfacher Sprache verfassten Sprachfassung, die die betreffende Person versteht oder von der vernünftigerweise angenommen werden darf, dass sie sie versteht, bereitgestellt. Die Informationen müssen für Minderjährige auch in einer dem Alter angemessenen Weise bereitgestellt werden.

(3) Die Vorschriften über das Recht auf Information, die in den anwendbaren Datenschutzvorschriften der Union enthalten sind, gelten für die im ECRIS-TCN gespeicherten und für die Zwecke dieser Verordnung verarbeiteten personenbezogenen Daten.

Artikel 48

Recht auf Auskunft, Berichtigung und Löschung von im MID gespeicherten personenbezogenen Daten sowie auf Einschränkung ihrer Verarbeitung

(1) Personen, die von ihren Rechten nach den Artikeln 15 bis 18 der Verordnung (EU) 2016/679, den Artikeln 17 bis 20 der Verordnung (EU) 2018/1725 und den Artikeln 14, 15 und 16 der Richtlinie (EU) 2016/680 Gebrauch machen möchten, können sich an die zuständige Behörde eines beliebigen Mitgliedstaats wenden, der den Antrag prüft und beantwortet.

(2) Der Mitgliedstaat, der einen solchen Antrag prüft, antwortet unverzüglich, in jedem Fall jedoch innerhalb von 45 Tagen nach Antragseingang. Diese Frist kann um weitere 15 Tage verlängert werden, wenn das unter Berücksichtigung der Komplexität und der Zahl der Anträge erforderlich ist. Der Mitgliedstaat, der den Antrag prüft, unterrichtet die betroffene Person innerhalb von 45 Tagen nach Antragseingang über eine Fristverlängerung, zusammen mit den Gründen für die Verzögerung. Die Mitgliedstaaten können entscheiden, dass die Antworten von Zentralstellen zu erteilen sind.

(3) Wird ein Antrag auf Berichtigung oder Löschung personenbezogener Daten bei einem anderen Mitgliedstaat als dem für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaat gestellt, so kontaktiert der Mitgliedstaat, an den der Antrag gerichtet wurde, innerhalb von sieben Tagen die Behörden des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats. Der für die manuelle Verifizierung verschiedener Identitäten zuständige Mitgliedstaat überprüft die Richtigkeit der Daten und die Rechtmäßigkeit der Datenverarbeitung unverzüglich, in jedem Fall jedoch innerhalb von 30 Tagen nach der Kontaktaufnahme. Diese Frist kann um weitere 15 Tage verlängert werden, wenn das unter Berücksichtigung der Komplexität und der Zahl der Anträge erforderlich ist. Der für die manuelle Verifizierung verschiedener Identitäten zuständige Mitgliedstaat unterrichtet den Mitgliedstaat, der ihn kontaktiert hat, von jeder solchen Fristverlängerung und nennt die Gründe für die Verzögerung. Der Mitgliedstaat, der die Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats kontaktiert hat, informiert die betroffene Person über das weitere Verfahren.

(4) Wird ein Antrag auf Berichtigung oder Löschung personenbezogener Daten bei einem Mitgliedstaat gestellt, in dem die ETIAS-Zentralstelle für die manuelle Verifizierung verschiedener Identitäten zuständig war, so kontaktiert der Mitgliedstaat, an den der Antrag gerichtet wurde, die ETIAS-Zentralstelle innerhalb von sieben Tagen, um sie darum zu ersuchen, eine Stellungnahme abzugeben. Die ETIAS-Zentralstelle gibt ihre Stellungnahme unverzüglich, in jedem Fall jedoch innerhalb von 30 Tagen nach der Kontaktaufnahme ab. Diese Frist kann um weitere 15 Tage verlängert werden, wenn das unter Berücksichtigung der Komplexität und der Zahl der Anträge erforderlich ist. Die betroffene Person wird von dem Mitgliedstaat, der die ETIAS-Zentralstelle kontaktiert hat, über das weitere Verfahren informiert.

(5) Falls bei einer Prüfung festgestellt wird, dass die im MID gespeicherten Daten unrichtig sind oder unrechtmäßig erfasst wurden, werden diese Daten vom für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaat oder, wenn kein Mitgliedstaat für die manuelle Verifizierung verschiedener Identitäten zuständig war oder wenn die ETIAS-Zentralstelle für die manuelle Verifizierung verschiedener Identitäten zuständig war, von dem Mitgliedstaat, an den der Antrag gerichtet wurde, unverzüglich berichtigt oder gelöscht. Die betroffene Person wird schriftlich darüber informiert, dass ihre Daten berichtigt oder gelöscht worden sind.

(6) Falls im MID gespeicherte Daten während ihrer Speicherfrist von einem Mitgliedstaat geändert werden, nimmt dieser Mitgliedstaat die Verarbeitung nach Artikel 27 und gegebenenfalls die Verarbeitung nach Artikel 29 vor, um zu ermitteln, ob die geänderten Daten verknüpft werden müssen. Ergibt sich bei der Verarbeitung keine Übereinstimmung, so löscht dieser Mitgliedstaat die Daten aus der Identitätsbestätigungsdatei. Falls bei der automatisierten Verarbeitung ein oder mehrere Übereinstimmungen gemeldet werden, erstellt oder aktualisiert dieser Mitgliedstaat die betreffende Verknüpfung gemäß den einschlägigen Bestimmungen dieser Verordnung.

(7) Ist der für die manuelle Verifizierung verschiedener Identitäten zuständige Mitgliedstaat oder gegebenenfalls der Mitgliedstaat, an den der Antrag gerichtet wurde, nicht der Ansicht, dass die im MID gespeicherten Daten unrichtig sind oder unrechtmäßig gespeichert wurden, so erlässt er eine Verwaltungsentscheidung, in der er der betroffenen Person unverzüglich schriftlich erläutert, warum er nicht zu einer Berichtigung oder Löschung der sie betreffenden Daten bereit ist.

(8) In der Entscheidung gemäß Absatz 7 wird die betroffene Person zudem darüber belehrt, dass sie die Entscheidung über ihren Antrag auf Auskunft über personenbezogene Daten bzw. Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten anfechten und wie sie gegebenenfalls bei den zuständigen Gerichten oder Behörden Klage erheben oder Beschwerde einlegen kann, einschließlich diesbezüglicher Hilfe, auch der Aufsichtsbehörden.

(9) Jeder Antrag auf Auskunft über personenbezogene Daten bzw. Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten enthält die zur Identifizierung der betroffenen Person notwendigen Informationen. Diese Informationen werden ausschließlich dazu verwendet, die Wahrnehmung der in diesem Artikel genannten Rechte zu ermöglichen, und anschließend unverzüglich gelöscht.

(10) Der für die manuelle Verifizierung verschiedener Identitäten zuständige Mitgliedstaat oder gegebenenfalls der Mitgliedstaat, an den der Antrag gerichtet wurde, führt eine schriftliche Aufzeichnung darüber, dass ein Antrag auf Auskunft über personenbezogene Daten bzw. Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten gestellt und wie dieser bearbeitet wurde, und stellt diese Aufzeichnung unverzüglich den Aufsichtsbehörden zur Verfügung.

(11) Dieser Artikel gilt unbeschadet etwaiger Beschränkungen und Einschränkungen der in diesem Artikel festgelegten Rechte gemäß der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680.

Artikel 49

Web-Portal

(1) Um die Ausübung der Rechte auf Auskunft über personenbezogene Daten bzw. Berichtigung, Löschung oder Einschränkung der Verarbeitung personenbezogener Daten zu erleichtern, wird ein Web-Portal eingerichtet.

(2) Das Web-Portal enthält Informationen über die Rechte und Verfahren nach den Artikeln 47 und 48 und eine Benutzerschnittstelle, die es Personen, deren Daten im MID verarbeitet werden und die davon unterrichtet wurden, dass eine rote Verknüpfung nach Artikel 32 Absatz 4 angezeigt wurde, ermöglicht, die Kontaktinformationen der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats zu erhalten.

(3) Um die Kontaktinformationen der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats zu erhalten, sollte die Person, deren Daten im MID verarbeitet werden, die Angaben zu der für die manuelle Verifizierung verschiedener Identitäten zuständigen Behörde nach Artikel 34 Buchstabe d eingeben. Das Web-Portal benutzt diese Angaben, um die Kontaktinformationen der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats abzurufen. Das Web-Portal umfasst auch eine E-Mail-Vorlage, um die Kommunikation zwischen dem Portalnutzer und der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats zu erleichtern. Diese E-Mail enthält ein Eingabefeld für die einmalige Kennnummer nach Artikel 34 Buchstabe c, um der zuständigen Behörde des für die manuelle Verifizierung verschiedener Identitäten zuständigen Mitgliedstaats zu ermöglichen, die betreffenden Daten zu identifizieren.

(4) Die Mitgliedstaaten stellen eu-LISA die Kontaktdaten aller Behörden zur Verfügung, die für die Prüfung und Beantwortung von Anträgen nach den Artikeln 47 und 48 zuständig sind, und überprüfen regelmäßig, ob diese Kontaktdaten aktuell sind.

(5) eu-LISA entwickelt das Web-Portal und sorgt für seine technische Verwaltung.

(6) Die Kommission erlässt einen delegierten Rechtsakt gemäß Artikel 69, um detaillierte Bestimmungen über den Betrieb des Web-Portals festzulegen, einschließlich der Benutzerschnittstelle, der Sprachen, in denen das Web-Portal zur Verfügung stehen soll, und der E-Mail-Vorlage.

Artikel 50

Übermittlung personenbezogener Daten an Drittstaaten, internationale Organisationen und private Stellen

Unbeschadet des Artikels 31 der Verordnung (EU) 2018/2008, der Artikel 25 und 26 der Verordnung (EU) 2016/794, des Artikels 41 der Verordnung (EU) 2017/2226, des Artikels 65 der Verordnung (EU) 2018/1240 und der Abfrage von Interpol-Datenbanken durch das ESP gemäß Artikel 9 Absatz 5 der vorliegenden Verordnung, die gemäß den Bestimmungen des Kapitels V der Verordnung (EU) 2018/1725 und des Kapitels V der Verordnung (EU) 2016/679 stehen, dürfen personenbezogene Daten, die in den Interoperabilitätskomponenten gespeichert sind, verarbeitet werden oder auf die über die Interoperabilitätskomponenten zugegriffen wird, nicht an Drittstaaten, internationale Organisationen oder private Stellen übermittelt oder diesen zur Verfügung gestellt werden.

Artikel 51

Kontrolle durch die Aufsichtsbehörden

(1) Jeder Mitgliedstaat stellt sicher, dass die Aufsichtsbehörden die Rechtmäßigkeit der Verarbeitung personenbezogener Daten gemäß der vorliegenden Verordnung durch den betreffenden Mitgliedstaat, einschließlich der Übermittlung an die und von den Interoperabilitätskomponenten, unabhängig überwachen.

(2) Jeder Mitgliedstaat trägt dafür Sorge, dass die gemäß der Richtlinie (EU) 2016/680 erlassenen nationalen Rechts- und Verwaltungsvorschriften gegebenenfalls auch für den Zugang von Polizeibehörden und benannten Behörden zu den Interoperabilitätskomponenten gelten, auch hinsichtlich der Rechte der Personen, auf deren Daten auf diese Weise zugegriffen wird.

(3) Die Aufsichtsbehörden stellen sicher, dass mindestens alle vier Jahre die durch die zuständigen nationalen Behörden erfolgenden Verarbeitungsvorgänge von personenbezogenen Daten für die Zwecke der vorliegenden Verordnung nach den einschlägigen internationalen Prüfungsstandards überprüft werden.

Die Aufsichtsbehörden veröffentlichen jährlich die Zahl der Anträge auf Berichtigung oder Löschung oder auf Einschränkung der Verarbeitung personenbezogener Daten, die getroffenen Folgemaßnahmen und die Zahl der Berichtigungen, Löschungen und Einschränkungen der Verarbeitung, die auf Antrag der betroffenen Personen vorgenommen wurden.

(4) Die Mitgliedstaaten stellen sicher, dass ihre Aufsichtsbehörden über ausreichende Ressourcen und Fachkenntnisse zur Wahrnehmung der Aufgaben verfügen, die ihnen gemäß dieser Verordnung übertragen werden.

(5) Die Mitgliedstaaten stellen alle Informationen, die von einer in Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörde angefordert werden, zur Verfügung, insbesondere Informationen zu den Tätigkeiten, die entsprechend ihren Verantwortlichkeiten gemäß der vorliegenden Verordnung durchgeführt werden. Die Mitgliedstaaten gewähren den in Artikel 51 Absatz 1 der Verordnung (EU) 2016/679 genannten Aufsichtsbehörden Zugang zu ihren Protokollen nach den Artikeln 10, 16, 24 und 36 der vorliegenden Verordnung sowie zu den Begründungen nach Artikel 22 Absatz 2 der vorliegenden Verordnung und gestatten ihnen jederzeit Zutritt zu allen ihren für Interoperabilitätszwecke genutzten Räumlichkeiten.

Artikel 52

Prüfungen durch den Europäischen Datenschutzbeauftragten

Der Europäische Datenschutzbeauftragte trägt dafür Sorge, dass die durch eu-LISA, die ETIAS-Zentralstelle und Europol für die Zwecke der vorliegenden Verordnung erfolgenden Verarbeitungsvorgänge von personenbezogenen Daten mindestens alle vier Jahre nach den einschlägigen internationalen Prüfungsstandards überprüft werden. Der Prüfbericht wird dem Europäischen Parlament, dem Rat, eu-LISA, der Kommission, den Mitgliedstaaten und der betreffenden Stelle der Union übermittelt. eu-LISA, die ETIAS-Zentralstelle und Europol erhalten vor der Annahme des Berichts Gelegenheit zur Stellungnahme.

eu-LISA, die ETIAS-Zentralstelle und Europol liefern die vom Europäischen Datenschutzbeauftragten angeforderten Informationen, gewähren dem Europäischen Datenschutzbeauftragten Zugang zu allen von ihm angeforderten Dokumenten und zu ihren Protokollen nach den Artikeln 10, 16, 24 und 36 und gestatten dem Europäischen Datenschutzbeauftragten jederzeit Zutritt zu allen ihren Räumlichkeiten.

Artikel 53

Zusammenarbeit zwischen den Aufsichtsbehörden und dem Europäischen Datenschutzbeauftragten

(1) Die Aufsichtsbehörden und der Europäische Datenschutzbeauftragte arbeiten — jeweils innerhalb ihres Kompetenzbereichs — im Rahmen ihrer jeweiligen Zuständigkeiten aktiv zusammen und sorgen für eine koordinierte Aufsicht der Nutzung der Interoperabilitätskomponenten und der Anwendung anderer Bestimmungen dieser Verordnung, insbesondere wenn der Europäische Datenschutzbeauftragte oder eine Aufsichtsbehörde größere Diskrepanzen zwischen den Verfahrensweisen der Mitgliedstaaten feststellt oder möglicherweise unrechtmäßige Übermittlungen über die Kommunikationskanäle der Interoperabilitätskomponenten bemerkt.

(2) In den in Absatz 1 dieses Artikels genannten Fällen wird eine koordinierte Aufsicht gemäß Artikel 62 der Verordnung (EU) 2018/1725 sichergestellt.

(3) Bis zum 12. Juni 2021 und danach alle zwei Jahre übermittelt der Europäische Datenschutzausschuss einen gemeinsamen Bericht über seine Tätigkeiten im Rahmen dieses Artikels an das Europäische Parlament, den Rat, die Kommission, Europol, die Europäische Agentur für die Grenz- und Küstenwache und eu-LISA. Dieser Bericht enthält für jeden Mitgliedstaat ein Kapitel, das von der Aufsichtsbehörde des betreffenden Mitgliedstaats erstellt wird.

KAPITEL VIII

Verantwortlichkeiten

Artikel 54

Verantwortlichkeiten von eu-LISA während der Konzept- und Entwicklungsphase

(1) eu-LISA stellt sicher, dass die zentralen Infrastrukturen der Interoperabilitätskomponenten gemäß dieser Verordnung betrieben werden.

(2) Die Interoperabilitätskomponenten werden an den technischen Standorten von eu-LISA betrieben und bieten die in dieser Verordnung vorgesehenen Funktionen gemäß den in Artikel 55 Absatz 1 festgelegten Bedingungen für die Sicherheit, Verfügbarkeit, Qualität und Leistung.

(3) eu-LISA ist verantwortlich für die Entwicklung der Interoperabilitätskomponenten sowie für jegliche Anpassungen, die erforderlich sind, um die Interoperabilität zwischen den Zentralsystemen des EES, des VIS, des ETIAS, des SIS, von Eurodac, dem ECRIS-TCN, dem ESP, dem gemeinsamen BMS, dem CIR, dem MID und dem CRRS herzustellen.

Unbeschadet des Artikels 62 hat eu-LISA keinen Zugang zu den personenbezogenen Daten, die über das ESP, den gemeinsamen BMS, den CIR oder den MID verarbeitet werden.

eu-LISA konzipiert die Architektur der Interoperabilitätskomponenten einschließlich ihrer Kommunikationsinfrastrukturen, legt ihre technischen Spezifikationen fest und bestimmt ihre Weiterentwicklung in Bezug auf die zentrale Infrastruktur und die sichere Kommunikationsinfrastruktur, die vom Verwaltungsrat vorbehaltlich einer befürwortenden Stellungnahme der Kommission angenommen werden. eu-LISA nimmt zudem etwaige erforderliche Anpassungen am SIS, an Eurodac oder am ECRIS-TCN vor, die für die Herstellung der Interoperabilität notwendig und in dieser Verordnung vorgesehen sind.

eu-LISA entwickelt und implementiert die Interoperabilitätskomponenten so bald wie möglich nach dem Inkrafttreten dieser Verordnung und nach Erlass der in Artikel 8 Absatz 2, Artikel 9 Absatz 7, Artikel 28 Absätze 5 und 7, Artikel 37 Absatz 4, Artikel 38 Absatz 3, Artikel 39 Absatz 5, Artikel 43 Absatz 5 und Artikel 74 Absatz 10 vorgesehenen Maßnahmen durch die Kommission.

Die Entwicklung umfasst die Ausarbeitung und Umsetzung der technischen Spezifikationen, die Erprobung und die gesamte Projektverwaltung und -koordination.

(4) Während der Konzept- und Entwicklungsphase wird ein Programmverwaltungsrat eingerichtet, der aus höchstens zehn Mitgliedern besteht. Dem Programmverwaltungsrat gehören sieben Mitglieder, die vom Verwaltungsrat von eu-LISA aus dem Kreis seiner Mitglieder oder stellvertretenen Mitglieder ernannt werden, der Vorsitzende der Beratergruppe für Interoperabilität gemäß Artikel 71, ein vom Exekutivdirektor ernannter Vertreter von eu-LISA sowie ein von der Kommission ernanntes Mitglied an. Die vom Verwaltungsrat von eu-LISA ernannten Mitglieder werden ausschließlich aus dem Kreis derjenigen Mitgliedstaaten gewählt, die nach dem Unionsrecht in vollem Umfang durch die Rechtsinstrumente gebunden sind, welche für die Entwicklung, die Errichtung, den Betrieb und die Nutzung aller EU-Informationssysteme gelten, und die sich an den Interoperabilitätskomponenten beteiligen werden.

(5) Der Programmverwaltungsrat tritt regelmäßig, mindestens jedoch dreimal pro Quartal zusammen. Er stellt die angemessene Verwaltung der Konzept- und Entwicklungsphase der Interoperabilitätskomponenten sicher.

Der Programmverwaltungsrat legt dem Verwaltungsrat von eu-LISA monatlich schriftliche Berichte über den Fortschritt des Projekts vor. Der Programmverwaltungsrat hat keine Entscheidungsbefugnis und kein Mandat zur Vertretung der Mitglieder des Verwaltungsrats von eu-LISA.

(6) Der Verwaltungsrat von eu-LISA legt die Geschäftsordnung des Programmverwaltungsrats fest, in der insbesondere Folgendes geregelt ist:

a) der Vorsitz,

b) die Sitzungsorte,

c) die Vorbereitung von Sitzungen,

d) die Zulassung von Sachverständigen zu den Sitzungen,

e) Kommunikationspläne, die gewährleisten, dass nicht teilnehmende Mitglieder des Verwaltungsrats lückenlos unterrichtet werden.

Den Vorsitz übernimmt ein Mitgliedstaat, der nach dem Unionsrecht in vollem Umfang durch die Rechtsinstrumente gebunden ist, die für die Entwicklung, die Errichtung, den Betrieb und die Nutzung aller EU-Informationssysteme gelten, und die sich an den Interoperabilitätskomponenten beteiligen werden.

Sämtliche Reise- und Aufenthaltskosten, die den Mitgliedern des Programmverwaltungsrats entstehen, werden von eu-LISA erstattet, wobei Artikel 10 der Geschäftsordnung von eu-LISA sinngemäß gilt. eu-LISA stellt das Sekretariat des Programmverwaltungsrats.

Die in Artikel 71 genannte Beratergruppe für Interoperabilität tritt bis zur Inbetriebnahme der Interoperabilitätskomponenten regelmäßig zusammen. Nach jeder Sitzung erstattet sie dem Programmverwaltungsrat Bericht. Sie stellt den technischen Sachverstand für die Unterstützung des Programmverwaltungsrats bei seinen Aufgaben bereit und überwacht den Stand der Vorbereitung in den Mitgliedstaaten.

Artikel 55

Verantwortlichkeiten von eu-LISA nach der Inbetriebnahme

(1) Nach der Inbetriebnahme der einzelnen Interoperabilitätskomponenten übernimmt eu-LISA die technische Verwaltung der zentralen Infrastruktur der Interoperabilitätskomponenten, einschließlich ihrer Wartung und von Technologieentwicklungen. In Zusammenarbeit mit den Mitgliedstaaten stellt eu-LISA sicher, dass vorbehaltlich einer Kosten-Nutzen-Analyse die beste verfügbare Technologie eingesetzt wird. eu-LISA ist zudem für die technische Verwaltung der in den Artikeln 6,12,17,25 und 39 genannten Kommunikationsinfrastruktur verantwortlich.

Die technische Verwaltung der Interoperabilitätskomponenten umfasst alle Aufgaben und technischen Lösungen, die erforderlich sind, um die Interoperabilitätskomponenten gemäß dieser Verordnung betriebsbereit zu halten und um den Mitgliedstaaten und den Stellen der Union 24 Stunden am Tag und 7 Tage in der Woche ununterbrochene Dienste zu erbringen. Dazu gehören die Wartungsarbeiten und technischen Anpassungen, die erforderlich sind, um sicherzustellen, dass die Komponenten gemäß den technischen Spezifikationen und insbesondere bei der Reaktionszeit bei Abfragen der zentralen Infrastrukturen mit zufriedenstellender technischer Qualität arbeiten.

Alle Interoperabilitätskomponenten werden so entwickelt und verwaltet, dass ein schneller, unterbrechungsfreier, effizienter und kontrollierter Zugang, die volle, ununterbrochene Verfügbarkeit der Komponenten und der im MID, im gemeinsamen BMS und im CIR gespeicherten Daten sowie eine Reaktionszeit entsprechend den operativen Erfordernissen der mitgliedstaatlichen Behörden und der Stellen der Union sichergestellt sind.

(2) Unbeschadet des Artikels 17 des Statuts der Beamten der Europäischen Union wendet eu-LISA angemessene Regeln zur Gewährleistung der beruflichen Schweigepflicht oder einer anderen vergleichbaren Geheimhaltungspflicht auf ihre Bediensteten an, die mit in den Interoperabilitätskomponenten gespeicherten Daten arbeiten. Diese Pflicht besteht auch nach dem Ausscheiden dieser Bediensteten aus dem Amt oder Dienstverhältnis oder der Beendigung ihrer Tätigkeit weiter.

Unbeschadet des Artikels 62 hat eu-LISA keinen Zugang zu den personenbezogenen Daten, die über das ESP, den gemeinsamen BMS, den CIR und den MID verarbeitet werden.

(3) eu-LISA entwickelt und pflegt einen Mechanismus und Verfahren für die Durchführung von Qualitätskontrollen der im gemeinsamen BMS und im CIR gespeicherten Daten gemäß Artikel 37.

(4) eu-LISA nimmt zudem Aufgaben im Zusammenhang mit Schulungen zur technischen Nutzung der Interoperabilitätskomponenten wahr.

Artikel 56

Zuständigkeiten der Mitgliedstaaten

(1) Jeder Mitgliedstaat ist zuständig für

a) die Anbindung an die Kommunikationsinfrastruktur des ESP und des CIR;

b) die Integration der bestehenden nationalen Systeme und Infrastrukturen in das ESP, den CIR und den MID;

c) die Organisation, die Verwaltung, den Betrieb und die Wartung seiner bestehenden nationalen Infrastruktur und deren Anbindung an die Interoperabilitätskomponenten;

d) die Verwaltung und die Regelung des Zugangs der dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen nationalen Behörden zum ESP, zum CIR und zum MID gemäß dieser Verordnung und für die Erstellung und regelmäßige Aktualisierung eines Verzeichnisses dieser Bediensteten und ihrer Profile;

e) den Erlass der in Artikel 20 Absätze 5 und 6 genannten Gesetzgebungsmaßnahmen zur Regelung des Zugriffs auf den CIR zu Identifizierungszwecken;

f) die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29;

g) die Einhaltung der durch das Unionsrecht aufgestellten Datenqualitätsanforderungen;

h) die Einhaltung der Regeln jedes EU-Informationssystems für die Sicherheit und die Integrität personenbezogener Daten;

i) die Beseitigung etwaiger Mängel, die im Evaluierungsbericht der Kommission über die Datenqualität nach Artikel 37 Absatz 5 festgestellt wurden.

(2) Jeder Mitgliedstaat bindet seine benannten Behörden mit dem CIR.

Artikel 57

Zuständigkeiten von Europol

(1) Europol sorgt dafür, dass über das ESP durchgeführte Abfragen von Europol-Daten verarbeitet werden. Europol passt seine Schnittstelle für die Abfrage von Europol-Systemen (Querying Europol Systems — QUEST) für die Verwendung von BPL-Daten (BPL — basic protection level — Basisschutzniveau) entsprechend an.

(2) Europol ist zuständig für die Verwaltung und die Regelung des Zugangs seiner dazu ordnungsgemäß ermächtigten Mitarbeiter zum ESP und zum CIR und der Nutzung dieser Komponenten durch diese Mitarbeiter gemäß dieser Verordnung sowie für die Erstellung und regelmäßige Aktualisierung eines Verzeichnisses dieser Bediensteten und ihrer Profile.

Artikel 58

Zuständigkeiten der ETIAS-Zentralstelle

Die ETIAS-Zentralstelle ist zuständig für

a) die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29;

b) die Prüfung der im EES, im VIS, in Eurodac und im SIS gespeicherten Daten auf Mehrfachidentitäten gemäß Artikel 65.

KAPITEL IX

Änderung anderer Rechtsakte der Union

Artikel 59

Änderung der Verordnung (EU) 2018/1726

Die Verordnung (EU) 2018/1726 wird wie folgt geändert:

1. Artikel 12 erhält folgende Fassung:

„*Artikel 12*

Datenqualität

(1) Unbeschadet der Verantwortung der Mitgliedstaaten für die in die Systeme unter der betrieblichen Verantwortung der Agentur eingegebenen Daten führt die Agentur unter enger Einbeziehung ihrer Beratergruppen für alle Systeme, die in die betriebliche Zuständigkeit der Agentur fallen, Mechanismen und Verfahren für die automatische Datenqualitätskontrolle, gemeinsame Datenqualitätsindikatoren und Mindestqualitätsstandards für die Speicherung von Daten gemäß den einschlägigen Rechtsinstrumenten der für diese Informationssysteme geltenden Rechtsinstrumente und des Artikels 37 der Verordnungen (EU) 2019/817 (*) und (EU) 2019/818 (**) des Europäischen Parlaments und des Rates ein.

(2) Die Agentur richtet gemäß Artikel 39 der Verordnungen (EU) 2019/817 und (EU) 2019/818 einen zentralen Speicher für Berichte und Statistiken, der nur anonymisierte Daten enthält und für den spezifische Bestimmungen in den Rechtsinstrumenten zur Regelung der Entwicklung, der Errichtung, des Betriebs und der Nutzung von von der Agentur verwalteten IT-Großsystemen gelten, ein."

(*) Verordnung (EU) 2019/817 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen in den Bereichen Grenzen und Visa und zur Änderung der Verordnungen (EG) Nr. 767/2008, (EU) 2016/399, (EU) 2017/2226, (EU) 2018/1240, (EU) 2018/1726 und (EU) 2018/1861 des Europäischen Parlaments und des Rates und der Entscheidung 2004/512/EG des Rates und des Beschlusses 2008/633/JI des Rates (ABl. L 135 vom 22.5.2019, S. 27).

(**) Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (ABl. L 135 vom 22.5.2019, S. 85)"

2. Artikel 19 Absatz 1 wird wie folgt geändert:

a) Folgender Buchstabe wird eingefügt:

„eea) die Berichte über den Stand der Entwicklung der Interoperabilitätskomponenten nach Artikel 78 Absatz 2 der Verordnung (EU) 2019/817 und Artikel 74 Absatz 2 der Verordnung (EU) 2019/818 anzunehmen."

b) Buchstabe ff erhält folgende Fassung:

„ff) die Berichte über die technische Funktionsweise des SIS nach Artikel 60 Absatz 7 der Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates (*) und Artikel 74 Absatz 8 der Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates (**), des VIS nach Artikel 50 Absatz 3 der Verordnung (EG) Nr. 767/2008 und Artikel 17 Absatz 3 des Beschlusses 2008/633/JI, des EES nach Artikel 72 Absatz 4 der Verordnung (EU) 2017/2226, des ETIAS nach Artikel 92 Absatz 4 der Verordnung (EU) 2018/1240, des ECRIS-TCN und der ECRIS-Referenzimplementierung nach Artikel 36 Absatz 8 der Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates (***) und der Interoperabilitätskomponenten nach Artikel 78 Absatz 3 der Verordnung (EU) 2019/817 und Artikel 74 Absatz 3 der Verordnung (EU) 2019/818 anzunehmen;"

(*) Verordnung (EU) 2018/1861 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der Grenzkontrollen, zur Änderung des Übereinkommens zur Durchführung des Übereinkommens von Schengen und zur Änderung und Aufhebung der Verordnung (EG) Nr. 1987/2006 (ABl. L 312 vom 7.12.2018, S. 14).

(**) Verordnung (EU) 2018/1862 des Europäischen Parlaments und des Rates vom 28. November 2018 über die Einrichtung, den Betrieb und die Nutzung des Schengener Informationssystems (SIS) im Bereich der polizeilichen Zusammenarbeit und der justiziellen Zusammenarbeit in Strafsachen, zur Änderung und Aufhebung des Beschlusses 2007/533/JI des Rates und zur Aufhebung der Verordnung (EG) Nr. 1986/2006 des Europäischen Parlaments und des Rates und des Beschlusses 2010/261/EU der Kommission (ABl. L 312 vom 7.12.2018, S. 56).

(***) Verordnung (EU) 2019/816 des Europäischen Parlaments und des Rates vom 17. April 2019 zur Einrichtung eines zentralisierten Systems für die Ermittlung der Mitgliedstaaten, in denen Informationen zu Verurteilungen von Drittstaatsangehörigen und Staatenlosen (ECRIS-TCN) vorliegen, sowie zur Ergänzung des Europäischen Strafregisterinformationssystems und zur Änderung der Verordnung (EU) Nr. 2018/1726 (ABl. L 135 vom 22.5.2019, S. 1)."

c) Buchstabe hh erhält folgende Fassung:

„hh) förmliche Stellungnahmen zu den Berichten des Europäischen Datenschutzbeauftragten über seine Überprüfungen nach Artikel 56 Absatz 2 der Verordnung (EU) 2018/1861, Artikel 42 Absatz 2 der Verordnung (EG) Nr. 767/2008 und Artikel 31 Absatz 2 der Verordnung (EU) Nr. 603/2013, Artikel 56 Absatz 2 der Verordnung (EU) 2017/2226, Artikel 67 der Verordnung (EU) 2018/1240, Artikel 29 Absatz 2 der Verordnung (EU) 2019/816 und Artikel 52 der Verordnungen (EU) 2019/817 und (EU) 2019/818 anzunehmen und für geeignete Folgemaßnahmen zu diesen Überprüfungen zu sorgen;"

d) Buchstabe mm erhält folgende Fassung:

„mm) die jährliche Veröffentlichung folgender Auflistungen sicherzustellen: der Liste der zuständigen Behörden, die nach Artikel 41 Absatz 8 der Verordnung (EU) 2018/1861 und Artikel 56 Absatz 7 der Verordnung (EU) 2018/1862 berechtigt sind, die im SIS gespeicherten Daten unmittelbar abzufragen, zusammen mit einer Liste der Stellen der nationalen Systeme des SIS (N.SIS -Stellen) und der SIRENE-Büros nach Artikel 7 Absatz 3 der Verordnung (EU) 2018/1861 bzw. Artikel 7 Absatz 3 der Verordnung (EU) 2018/1862 und der Liste der zuständigen Behörden nach Artikel 65 Absatz 2 der Verordnung (EU) 2017/2226, der Liste der zuständigen Behörden nach Artikel 87 Absatz 2 der Verordnung (EU) 2018/1240, der Liste der Zentralbehörden nach Artikel 34 Absatz 2 der Verordnung (EU) 2019/816 sowie der Liste der Behörden nach Artikel 71 Absatz 1 der Verordnung (EU) 2019/817 und Artikel 67 Absatz 1 der Verordnung (EU) 2019/818.“

3. Artikel 22 Absatz 4 erhält folgende Fassung:

„(4) Europol und Eurojust können an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine SIS II betreffende Angelegenheit im Zusammenhang mit der Anwendung des Beschlusses 2007/533/JI auf der Tagesordnung steht.

Die Europäische Agentur für die Grenz- und Küstenwache kann an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine das SIS betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) 2016/1624 auf der Tagesordnung steht.

Europol kann an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine das VIS betreffende Angelegenheit im Zusammenhang mit der Anwendung des Beschlusses 2008/633/JI oder eine Eurodac betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) Nr. 603/2013 auf der Tagesordnung steht.

Europol kann an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine das EES betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) 2017/2226 oder eine ETIAS betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) 2018/1240 auf der Tagesordnung steht.

Die Europäische Agentur für die Grenz- und Küstenwache kann an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine ETIAS betreffende Angelegenheit im Zusammenhang mit der Anwendung der Verordnung (EU) 2018/1240 auf der Tagesordnung steht.

Eurojust, Europol und die die Europäische Staatsanwaltschaft können an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine die Verordnung (EU) 2019/816 betreffende Angelegenheit auf der Tagesordnung steht.

Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache können an den Sitzungen des Verwaltungsrats als Beobachter teilnehmen, wenn eine die Verordnungen (EU) 2019/817 und (EU) 2019/818 betreffende Angelegenheit auf der Tagesordnung steht.

Der Verwaltungsrat kann weitere Personen, deren Stellungnahme von Interesse sein könnte, als Beobachter zu seinen Sitzungen einladen.“

4. Artikel 24 Absatz 3 Buchstabe p erhält folgende Fassung:

„p) unbeschadet des Artikels 17 des Beamtenstatuts Geheimhaltungsvorschriften festzulegen, um Artikel 17 der Verordnung (EG) Nr. 1987/2006, Artikel 17 des Beschlusses 2007/533/JI, Artikel 26 Absatz 9 der Verordnung (EG) Nr. 767/2008, Artikel 4 Absatz 4 der Verordnung (EU) Nr. 603/2013, Artikel 37 Absatz 4 der Verordnung (EU) 2017/2226, Artikel 74 Absatz 2 der Verordnung (EU) 2018/1240, Artikel 11 Absatz 16 der Verordnung (EU) 2019/816 und Artikel 55 Absatz 2 der Verordnungen (EU) 2019/817 und (EU) 2019/818 nachzukommen;“

5. Artikel 27 wird wie folgt geändert:

a) In Absatz 1 wird folgender Buchstabe eingefügt:

„da) die Beratergruppe für Interoperabilität;“

b) Absatz 3 erhält folgende Fassung:

„(3) Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache können je einen Vertreter in die SIS-II-Beratergruppe entsenden.

Europol kann auch einen Vertreter in die VIS- und die Eurodac- sowie die EES-ETIAS-Beratergruppe entsenden.

Die Europäische Agentur für die Grenz- und Küstenwache kann auch einen Vertreter in die EES-ETIAS-Beratergruppe entsenden.

Eurojust, Europol und die Europäische Staatsanwaltschaft können je einen Vertreter in die ECRIS-TCN-Beratergruppe entsenden.

Europol, Eurojust und die Europäische Agentur für die Grenz- und Küstenwache können je einen Vertreter in die Beratergruppe für Interoperabilität entsenden.“

Artikel 60

Änderung der Verordnung (EU) 2018/1862

Die Verordnung (EU) 2018/1862 wird wie folgt geändert:

1. In Artikel 3 werden die folgenden Nummern angefügt:

„18. „ESP“ das durch Artikel 6 Absatz 1 der Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates (*) geschaffene Europäische Suchportal;

19. „gemeinsamer BMS“ den durch Artikel 12 Absatz 1 der Verordnung (EU) 2019/818 eingerichteten gemeinsamen Dienst für den Abgleich biometrischer Daten;

20. „CIR“ den durch Artikel 17 Absatz 1 der Verordnung (EU) 2019/818 eingerichteten gemeinsamen Speicher für Identitätsdaten;

21. „MID“ den durch Artikel 25 Absatz 1 der Verordnung (EU) 2019/818 eingerichteten Detektor für Mehrfachidentitäten.

(*) Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862 und (EU) 2019/816 (ABl. L 135 vom 22.5.2019, S. 85).“.

2. Artikel 4 wird wie folgt geändert:

a) Absatz 1 Buchstaben b und c erhalten folgende Fassung:

„b) einem nationalen System (im Folgenden „N.SIS“) in jedem einzelnen Mitgliedstaat, das aus den nationalen, mit dem zentralen SIS kommunizierenden Datensystemen besteht, einschließlich mindestens einem nationalen oder gemeinsamen Back-up-N.SIS;

c) einer Kommunikationsinfrastruktur zwischen der CS-SIS, der Back-up-CS-SIS und der NI-SIS (im Folgenden „Kommunikationsinfrastruktur“), die ein verschlüsseltes virtuelles Netz speziell für SIS-Daten und den Austausch von Daten zwischen SIRENE-Büros nach Artikel 7 Absatz 2 zur Verfügung stellt, und

d) einer sicheren Kommunikationsinfrastruktur zwischen der CS-SIS und den zentralen Infrastrukturen des ESP, des gemeinsamen BMS und des MID.“

b) Folgende Absätze werden angefügt:

„(8) Unbeschadet der Absätze 1 bis 5 können SIS-Daten zu Personen und Ausweispapieren auch über das ESP abgefragt werden.

(9) Unbeschadet der Absätze 1 bis 5 können SIS-Daten zu Personen und Ausweispapieren auch über die sichere Kommunikationsinfrastruktur gemäß Absatz 1 Buchstabe d übermittelt werden. Diese Übermittlungen sind auf das Maß beschränkt, in dem die Daten für die in der Verordnung (EU) 2019/818 genannten Zwecke erforderlich sind.“

3. In Artikel 7 wird folgender Absatz eingefügt:

„2a. Die SIRENE-Büros gewährleisten außerdem die manuelle Verifizierung verschiedener Identitäten gemäß Artikel 29 der Verordnung (EU) 2019/818. In dem für die Erfüllung dieser Aufgabe erforderlichem Maße können die SIRENE-Büros für die in den Artikeln 21 und 26 der Verordnung (EU) 2019/818 genannten Zwecke auf die im CIR und im MID gespeicherten Daten zugreifen.“.

4. In Artikel 12 Absatz 1 wird folgender Unterabsatz angefügt:

„Die Mitgliedstaaten stellen sicher, dass jeder Zugriff auf personenbezogene Daten über das ESP ebenfalls protokolliert wird, damit die Rechtmäßigkeit der Abfrage und die Rechtmäßigkeit der Datenverarbeitung kontrolliert und eine Eigenkontrolle durchgeführt sowie die Datenintegrität und -sicherheit gewährleistet werden kann.“.

5. In Artikel 44 Absatz 1 wird folgender Buchstabe angefügt:

„f) die Verifizierung verschiedener Identitäten und die Bekämpfung von Identitätsbetrug gemäß Kapitel V der Verordnung (EU) 2019/818.“.

6. Artikel 74 Absatz 7 erhält folgende Fassung:

„(7) Für die Zwecke des Artikels 15 Absatz 4 und der Absätze 3, 4 und 6 des vorliegenden Artikels speichert eu-LISA die Daten nach Artikel 15 Absatz 4 und nach Absatz 3 des vorliegenden Artikels in dem in Artikel 39 der Verordnung (EU) 2019/818 genannten zentralen Speicher für Berichte und Statistiken; dies darf eine Identifizierung einzelner Personen nicht ermöglichen.

eu-LISA gestattet der Kommission und den Stellen nach Absatz 6 des vorliegenden Artikels, maßgeschneiderte Berichte und Statistiken zu erhalten. Auf Anfrage gewährt eu-LISA den Mitgliedstaaten, der Kommission, Europol und der Europäischen Agentur für die Grenz- und Küstenwache Zugang zu dem zentralen Speicher für Berichte und Statistiken gemäß Artikel 39 der Verordnung (EU) 2019/818.“.

Artikel 61

Änderungen der Verordnung (EU) 2019/816

Die Verordnung (EU) 2019/816 wird wie folgt geändert:

1. In Artikel 1 wird folgender Buchstabe angefügt:

„c) werden die Bedingungen festgelegt, unter denen das ECRIS-TCN durch die Speicherung von Identitätsdaten, Reisedokumentendaten und biometrischen Daten in dem CIR zur Erleichterung und Unterstützung bei der korrekten Identifizierung von im ECRIS-TCN erfassten Personen unter den Voraussetzungen und für die Zwecke des Artikels 20 der Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates (*) beiträgt.

(*) Verordnung (EU) 2019/818 des Europäischen Parlaments und des Rates vom 20. Mai 2019 zur Errichtung eines Rahmens für die Interoperabilität zwischen EU-Informationssystemen (polizeiliche und justizielle Zusammenarbeit, Asyl und Migration) und zur Änderung der Verordnungen (EU) 2018/1726, (EU) 2018/1862, und (EU) 2019/816 (ABl. L 135 vom 22.5.2019, S. 85).“.

2. Artikel 2 erhält folgende Fassung:

„*Artikel 2*

Anwendungsbereich

Diese Verordnung gilt für die Verarbeitung von Identitätsangaben zu in Mitgliedstaaten verurteilten Drittstaatsangehörigen zum Zwecke der Ermittlung der Mitgliedstaaten, in denen solche Verurteilungen ergangen sind. Mit Ausnahme von Artikel 5 Absatz 1 Buchstabe b Ziffer ii gelten die für Drittstaatsangehörige geltenden Bestimmungen dieser Verordnung auch für Unionsbürger, die auch die Staatsangehörigkeit eines Drittstaats besitzen und in den Mitgliedstaaten verurteilt worden sind. Diese Verordnung dient auch zum Zwecke der Erleichterung und Unterstützung bei der korrekten Identifizierung von Personen gemäß dieser Verordnung und der Verordnung (EU) 2019/818.“.

3. Artikel 3 wird wie folgt geändert:

a) Nummer 8 wird gestrichen.

b) Die folgenden Nummern werden eingefügt

„19. „CIR“ den durch Artikel 17 Absatz 1 der Verordnung (EU) 2019/818 eingerichteten gemeinsamen Speicher für Identitätsdaten;

20. „ECRIS-TCN-Daten“ sämtliche Daten, die gemäß Artikel 5 im Zentralsystem und im CIR gespeichert sind;

21. „ESP“ das durch Artikel 6 Absatz 1 der Verordnung (EU) 2019/818 eingerichtete Europäische Suchportal.“.

4. Artikel 4 Absatz 1 wird wie folgt geändert:

a) Buchstabe a erhält folgende Fassung:

„a) ein Zentralsystem;“

b) Folgender Buchstabe wird eingefügt:

„aa) das CIR;“;

c) Folgender Buchstabe wird angefügt:

„e) einer Kommunikationsinfrastruktur zwischen dem Zentralsystem und den zentralen Infrastrukturen des ESP und des CIR .“.

5. Artikel 5 wird wie folgt geändert:

a) In Absatz 1 erhält der Einleitungssatz folgende Fassung:

„1. Die Zentralbehörde des Urteilsmitgliedstaats erstellt für jeden verurteilten Drittstaatsangehörigen einen Datensatz im ECRIS-TCN. Dieser Datensatz enthält folgende Angaben:“;

b) Folgender Absatz wird eingefügt:

„(1a) Der CIR enthält die Daten nach Absatz 1 Buchstabe b und folgende Daten nach Absatz 1 Buchstabe a: Nachname (Familienname), Vornamen, Geburtsdatum, Geburtsort (Gemeinde und Staat), Staatsangehörigkeit(en), Geschlecht, gegebenenfalls frühere Namen, Pseudonyme und/oder Aliasnamen (sofern vorhanden); falls verfügbar, Art und Nummer der Reisedokumente der Person sowie Bezeichnung der ausstellenden Behörde. Der CIR kann die in Absatz 3 genannten Daten enthalten. Die übrigen ECRIS-TCN-Daten werden im Zentralsystem gespeichert.“.

6. Artikel 8 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Jeder Datensatz wird so lange im Zentralsystem und im CIR gespeichert, wie die Daten zu den Verurteilungen der betreffenden Person in den Strafregistern gespeichert sind.“;

b) Absatz 2 erhält folgende Fassung:

„(2) Nach Ablauf der in Absatz 1 genannten Speicherfrist löscht die Zentralbehörde des Urteilsmitgliedstaats den Datensatz, einschließlich Fingerabdruckdaten oder Gesichtsbildern, aus dem Zentralsystem und aus dem CIR. Die Löschung erfolgt nach Möglichkeit automatisch und in jedem Fall spätestens einen Monat nach Ablauf der Speicherfrist.“;

7. In Artikel 9 wird wie folgt geändert:

a) In Absatz 1 werden die Wörter „in das ECRIS-TCN“ durch die Wörter „in das Zentralsystem und in das CIR“ ersetzt.

b) In den Absätzen 2, 3 und 4 werden die Wörter „im Zentralsystem“ durch die Wörter „im Zentralsystem und im CIR“ und die Wörter „aus dem Zentralsystem“ durch die Wörter „aus dem Zentralsystem und aus dem CIR“ ersetzt.

8. Artikel 10 Absatz 1 Buchstabe j wird gestrichen.

9. In Artikel 12 Absatz 2 werden die Wörter „im Zentralsystem“ durch die Wörter „im Zentralsystem und im CIR“ ersetzt.

10. In Artikel 13 Absatz 2 werden die Wörter „des Zentralsystems“ durch die Wörter „des Zentralsystems, des CIR“ und die Wörter „dem Zentralsystem“ durch die Wörter „dem Zentralsystem und dem CIR“ ersetzt.

11. In Artikel 21 Absatz 2 werden die Wörter „das Zentralsystem“ durch die Wörter „das Zentralsystem und den CIR“ ersetzt.

12. Artikel 24 wird wie folgt geändert:

a) Absatz 1 erhält folgende Fassung:

„(1) Die in das Zentralsystem und in den CIR eingegebenen Daten dürfen nur zum Zweck der Ermittlung der Mitgliedstaaten, in denen Strafregisterinformationen zu Drittstaatsangehörigen vorliegen, verarbeitet werden. Die in den CIR eingegebenen Daten werden zur Erleichterung und Unterstützung bei der korrekten Identifizierung von gemäß dieser Verordnung im ECRIS-TCN erfassten Personen ebenfalls gemäß der Verordnung (EU) 2019/818 verarbeitet.“;

b) Folgender Absatz wird angefügt:

„(3) Unbeschadet des Absatzes 2 ist der Zugang zum Zwecke der Abfrage der im CIR gespeicherten Daten ebenfalls den dazu ordnungsgemäß ermächtigten Bediensteten der nationalen mitgliedstaatlichen Behörden und den dazu ordnungsgemäß ermächtigten Bediensteten der Stellen der Union vorbehalten, die für die in den Artikeln 20 und 21 der Verordnung (EU) 2019/818 genannten Aufgaben zuständig sind. Dieser Zugang ist auf das Maß beschränkt, in dem die Daten für die Wahrnehmung ihrer Aufgaben zu diesen Zwecken erforderlich sind, und steht in einem angemessenen Verhältnis zu den verfolgten Zielen“.

13. Artikel 32 Absatz 2 erhält folgende Fassung:

„(2) Für die Zwecke von Absatz 1 speichert eu-LISA die Daten nach Absatz 1 in dem zentralen Speicher für Berichte und Statistiken nach Artikel 39 der Verordnung (EU) 2019/818.“.

14. In Artikel 33 Absatz 1 werden die Wörter „des Zentralsystems“ durch die Wörter „des Zentralsystems und des CIR“ ersetzt.

15. Artikel 41 Absatz 2 erhält folgende Fassung:

„(2) Die Zentralbehörden legen für Urteile, die vor dem Tag des Beginns der Dateneingabe gemäß Artikel 35 Absatz 1 ergangen sind, wie folgt individuelle Datensätze im Zentralsystem und im CIR an:

a) alphanumerische Daten werden bis zum Ablauf der in Artikel 35 Absatz 2 genannten Frist in das Zentralsystem und in CIR eingegeben;

b) Fingerabdruckdaten werden innerhalb von zwei Jahren nach der Inbetriebnahme gemäß Artikel 35 Absatz 5 in das Zentralsystem und in CIR eingegeben."

KAPITEL X

Schlussbestimmungen

Artikel 62

Berichte und Statistiken

(1) Das dazu ordnungsgemäß ermächtigte Personal der zuständigen mitgliedstaatlichen Behörden, der Kommission und von eu-LISA hat Zugang zur Zahl der Abfragen pro ESP-Nutzerprofil ausschließlich zur Erstellung von Berichten und Statistiken.

Es darf nicht möglich sein, einzelne Personen anhand der Daten zu identifizieren.

(2) Die folgenden Daten zum CIR dürfen von dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen mitgliedstaatlichen Behörden, der Kommission und von eu-LISA ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden:

a) Zahl der Abfragen für die Zwecke der Artikel 20, 21 und 22;

b) Staatsangehörigkeit, Geschlecht und Geburtsjahr der Person;

c) Art des Reisedokuments und aus drei Buchstaben bestehender Code des ausstellenden Staates;

d) Zahl der Abfragen mit und ohne biometrische Daten.

Die Identifizierung einzelner Personen auf der Grundlage der Daten darf nicht möglich sein.

(3) Die folgenden Daten zum MID dürfen von dazu ordnungsgemäß ermächtigten Bediensteten der zuständigen mitgliedstaatlichen Behörden, der Kommission und von eu-LISA ausschließlich zur Erstellung von Berichten und Statistiken abgefragt werden:

a) Zahl der Abfragen mit und ohne biometrische Daten;

b) Zahl der Verknüpfungen, aufgeschlüsselt nach Verknüpfungsart, und die EU-Informationssysteme, die die verknüpften Daten enthalten;

c) Zeitraum, für den eine gelbe und rote Verknüpfung im System verblieben ist.

Die Identifizierung einzelner Personen auf der Grundlage der Daten darf nicht möglich sein.

(4) Die ordnungsgemäß ermächtigten Bediensteten der Europäischen Agentur für die Grenz- und Küstenwache können zur Durchführung von Risikoanalysen und Schwachstellenbeurteilungen nach den Artikeln 11 und 13 der Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates ([38]) auf die in den Absätzen 1, 2 und 3 des vorliegenden Artikels genannten Daten zugreifen.

(5) Die ordnungsgemäß ermächtigten Bediensteten von Europol können auf die in den Absätzen 2 und 3 des vorliegenden Artikels genannten Daten zur Durchführung von strategischen, themenbezogenen und operativen Analysen nach Artikel 18 Absatz 2 Buchstaben b und c der Verordnung (EU) 2016/794 zugreifen.

(6) Für die Zwecke der Absätze 1, 2 und 3 speichert eu-LISA die in diesen Absätzen genannten Daten im CRRS. Die Identifizierung einzelner Personen auf der Grundlage der im CRRS enthaltenen Daten darf nicht möglich sein; jedoch müssen die Daten den in den Absätzen 1, 2 und 3 genannten Behörden die Möglichkeit geben, anpassbare Berichte und Statistiken abzurufen, um die Effizienz von Grenzübertrittskontrollen zu steigern, Behörden bei der Bearbeitung von Visumanträgen zu unterstützen und eine faktengestützte Gestaltung der Migrations- und Sicherheitspolitik der Union zu fördern.

(7) Auf Anfrage werden der Agentur der Europäischen Union für Grundrechte relevante Informationen von der Kommission zur Verfügung gestellt, damit sie die Auswirkungen dieser Verordnung auf die Grundrechte bewerten kann.

([38]) Verordnung (EU) 2016/1624 des Europäischen Parlaments und des Rates vom 14. September 2016 über die Europäische Grenz- und Küstenwache und zur Änderung der Verordnung (EU) 2016/399 des Europäischen Parlaments und des Rates sowie zur Aufhebung der Verordnung (EG) Nr. 863/2007 des Europäischen Parlaments und des Rates, der Verordnung (EG) Nr. 2007/2004 des Rates und der Entscheidung des Rates 2005/267/EG (ABl. L 251 vom 16.9.2016, S. 1).

Artikel 63

Übergangszeitraum für die Nutzung des Europäischen Suchportals

(1) Während eines Zeitraums von zwei Jahren nach dem Datum der Inbetriebnahme des ESP gelten die Pflichten nach Artikel 7 Absätze 2 und 4 nicht, und die Benutzung des ESP ist fakultativ.

(2) Der Kommission wird die Befugnis übertragen, gemäß Artikel 69 einen delegierten Rechtsakt zur Änderung dieser Verordnung zu erlassen, durch die der in Absatz 1 des vorliegenden Artikels genannte Zeitraum einmal um höchstens ein Jahr verlängert wird, wenn eine Bewertung der praktischen Umsetzung des ESP ergeben hat, dass eine solche Verlängerung insbesondere angesichts der Auswirkungen, die die Inbetriebnahme des ESP auf die Organisation und die Dauer der Grenzübertrittskontrollen hätte, notwendig ist.

Artikel 64

Übergangszeit für die Bestimmungen über den Zugriff auf den gemeinsamen Speicher für Identitätsdaten zu Zwecken der Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten

Artikel 22 gilt ab dem Tag der Inbetriebnahme des CIR gemäß Artikel 68 Absatz 3.

Artikel 65

Übergangszeitraum für die Prüfung auf Mehrfachidentitäten

(1) Für die Dauer eines Jahres, nachdem eu-LISA den Abschluss des Tests des MID nach Artikel 68 Absatz 4 Buchstabe b mitgeteilt hat, und vor der Inbetriebnahme des MID ist die ETIAS-Zentralstelle für die Prüfung der im EES, im VIS, in Eurodac und im SIS gespeicherten Daten auf Mehrfachidentitäten zuständig. Die Prüfungen auf Mehrfachidentitäten werden ausschließlich anhand biometrischer Daten durchgeführt.

(2) Wenn die Abfrage eine oder mehrere Übereinstimmungen ergibt und die Identitätsdaten der verknüpften Dateien gleich oder ähnlich sind, wird eine weiße Verknüpfung nach Artikel 33 erstellt.

Wenn die Abfrage eine oder mehrere Übereinstimmungen ergibt und die Identitätsdaten der verknüpften Dateien nicht als ähnlich angesehen werden können, wird eine gelbe Verknüpfung nach Artikel 30 erstellt, und das Verfahren nach Artikel 29 gelangt zur Anwendung.

Wenn mehrere Übereinstimmungen gemeldet werden, wird zwischen jedem Datenelement, das zu einer Übereinstimmung geführt hat, eine Verknüpfung erstellt.

(3) Wenn eine gelbe Verknüpfung erstellt wird, gewährt der MID der ETIAS-Zentralstelle Zugang zu den in den verschiedenen EU-Informationssystemen gespeicherten Identitätsdaten.

(4) Wenn eine Verknüpfung zu einer Ausschreibung im SIS erstellt wird, bei der es sich nicht um eine Ausschreibung nach Artikel 3 der Verordnung (EU) 2018/1860, den Artikeln 24 und 25 der Verordnung (EU) 2018/1861 oder Artikel 38 der Verordnung (EU) 2018/1862 handelt, gewährt der MID dem SIRENE-Büro des Mitgliedstaats, der die Ausschreibung eingegeben hat, Zugang zu den in den verschiedenen Informationssystemen gespeicherten Identitätsdaten.

(5) Die ETIAS-Zentralstelle beziehungsweise - in den in Absatz 4 dieses Artikels genannten Fällen - das SIRENE-Büro des Mitgliedstaats, der die Ausschreibung eingegeben hat, greift auf die in der Identitätsbestätigungsdatei enthaltenen Daten zu, prüft die verschiedenen Identitäten, aktualisiert die Verknüpfung gemäß den Artikeln 31, 32 und 33 und fügt diese zur Identitätsbestätigungsdatei hinzu.

(6) Die ETIAS-Zentralstelle unterrichtet die Kommission gemäß Artikel 67 Absatz 3 erst, sobald alle gelben Verknüpfungen manuell überprüft und deren Status entweder in grüne, weiße oder rote Verknüpfungen aktualisiert worden sind.

(7) Die Mitgliedstaaten unterstützen die ETIAS-Zentralstelle gegebenenfalls bei der Prüfung auf Mehrfachidentitäten gemäß diesem Artikel.

(8) Der Kommission wird die Befugnis übertragen, gemäß Artikel 69 einen delegierten Rechtsakt zur Änderung dieser Verordnung zu erlassen, durch die der in Absatz 1 dieses Artikels genannte Zeitraum um sechs Monate verlängert wird, wobei zweimal eine weitere Verlängerung um jeweils sechs Monate möglich ist. Eine solche Verlängerung wird nur gewährt, wenn eine Bewertung der geschätzten Zeit für den Abschluss der Prüfung auf Mehrfachidentitäten nach diesem Artikel ergibt, dass die Prüfung auf Mehrfachidentitäten aus Gründen, auf die die ETIAS-Zentralstelle keinen Einfluss hat, nicht vor Ende des Zeitraums gemäß Absatz 1 dieses Artikels oder einer laufenden Verlängerung abgeschlossen werden kann, und dass keine korrektiven Maßnahmen getroffen werden können. Die Bewertung wird spätestens drei Monate vor Auslaufen eines solchen Zeitraums oder einer solchen laufenden Verlängerung durchgeführt.

Artikel 66

Kosten

(1) Die Kosten im Zusammenhang mit der Einrichtung und dem Betrieb des ESP, des gemeinsamen BMS, des CIR und des MID gehen zulasten des Gesamthaushaltsplans der Union.

(2) Die Kosten im Zusammenhang mit der Integration der bestehenden nationalen Infrastrukturen, deren Anbindung an die einheitlichen nationalen Schnittstellen und dem Hosting der einheitlichen nationalen Schnittstellen gehen zulasten des Gesamthaushaltsplans der Union.

Hiervon ausgenommen sind die Kosten für

a) die Projektverwaltungsstelle der Mitgliedstaaten (Sitzungen, Dienstreisen, Büroräume),

b) das Hosting nationaler IT-Systeme (Räume, Implementierung, Stromversorgung, Kühlung),

c) den Betrieb nationaler IT-Systeme (Betreiber- und Unterstützungsverträge),

d) Konzipierung, Entwicklung, Implementierung, Betrieb und Wartung nationaler Kommunikationsnetze.

(3) Unbeschadet der Zuweisung weiterer Finanzierungsmittel für diesen Zweck aus anderen Quellen des Gesamthaushaltsplans der Union werden 32 077 000 EUR aus der Dotation von 791 000 000 EUR mobilisiert, die gemäß Artikel 5 Absatz 5 Buchstabe b der Verordnung (EU) Nr. 515/2014 vorgesehen ist, um die Kosten für die Umsetzung dieser Verordnung abzudecken, wie das in den Absätzen 1 und 2 dieses Artikels vorgesehen ist.

(4) Von der in Absatz 3 genannten Dotation werden 22 861 000 EUR eu-LISA, 9 072 000 EUR Europol und 144 000 EUR der Agentur der Europäischen Union für die Aus- und Fortbildung auf dem Gebiet der Strafverfolgung (CEPOL) zugewiesen, um diese Stellen bei der Wahrnehmung ihrer jeweiligen Aufgaben nach dieser Verordnung zu unterstützen. Die Umsetzung erfolgt im Wege der indirekten Mittelverwaltung.

(5) Die Kosten im Zusammenhang mit den benannten Behörden gehen zulasten der jeweils benennenden Mitgliedstaaten. Die Kosten für die Anbindung jeder benannten Behörde an den CIR gehen zulasten der einzelnen Mitgliedstaaten.

Die Kosten, die Europol entstehen, einschließlich der Kosten für die Anbindung an den CIR, gehen zulasten von Europol.

Artikel 67

Mitteilungen

(1) Die Mitgliedstaaten teilen eu-LISA die Behörden gemäß den Artikeln 7, 20, 21 und 26 mit, die das ESP, den CIR beziehungsweise den MID nutzen dürfen oder Zugang zum ESP, zum CIR beziehungsweise zum MID haben.

Innerhalb von drei Monaten nach dem Datum, an dem die einzelnen Interoperabilitätskomponenten gemäß Artikel 68 ihren Betrieb aufgenommen haben, wird eine konsolidierte Liste dieser Behörden im *Amtsblatt der Europäischen Union* veröffentlicht. Werden Änderungen an der Liste vorgenommen, so veröffentlicht eu-LISA einmal im Jahr eine aktualisierte konsolidierte Liste.

(2) eu-LISA teilt der Kommission den erfolgreichen Abschluss der Tests nach Artikel 68 Absatz 1 Buchstabe b, Absatz 2 Buchstabe b, Absatz 3 Buchstabe b, Absatz 4 Buchstabe b, Absatz 5 Buchstabe b und Absatz 6 Buchstabe b mit.

(3) Die ETIAS-Zentralstelle teilt der Kommission den erfolgreichen Abschluss des Übergangszeitraums nach Artikel 65 mit.

(4) Die Kommission stellt den Mitgliedstaaten und der Öffentlichkeit die gemäß Absatz 1 mitgeteilten Informationen über eine fortlaufend aktualisierte öffentliche Website bereit.

Artikel 68

Aufnahme des Betriebs

(1) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt das ESP seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 8 Absatz 2, Artikel 9 Absatz 7 und Artikel 43 Absatz 5 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des ESP festgestellt, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden und den Stellen der Union, die das ESP nutzen können, durchgeführt hat;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 8 Absatz 1 validiert und der Kommission mitgeteilt;

Abfragen der Interpol-Datenbanken über das ESP erfolgen erst, wenn die technischen Vorkehrungen die Einhaltung von Artikel 9 Absatz 5 ermöglichen. Eine Unmöglichkeit der Einhaltung von Artikel 9 Absatz 5 führt dazu, dass eine Abfrage der Interpol-Datenbanken über das ESP unterbleibt, die Aufnahme des Betriebs des ESP wird aber nicht verzögert.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(2) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt der gemeinsamer BMS seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 13 Absatz 5 und Artikel 43 Absatz 5 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des gemeinsamen BMS, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden durchgeführt hat, festgestellt;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 13 validiert und der Kommission mitgeteilt;

d) eu-LISA hat den erfolgreichen Abschluss des Tests nach Absatz 5 Buchstabe b festgestellt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(3) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt der CIR seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 43 Absatz 5 und Artikel 74 Absatz 10 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des CIR, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden durchgeführt hat, festgestellt;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 18 validiert und der Kommission mitgeteilt;

d) eu-LISA hat den erfolgreichen Abschluss des Tests nach Absatz 5 Buchstabe b festgestellt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(4) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt der MID seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 28 Absätze 5 und 7, Artikel 32 Absatz 5, Artikel 33 Absatz 6, Artikel 43 Absatz 5 und Artikel 49 Absatz 6 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des MID, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden und der ETIAS-Zentralstelle durchgeführt hat, festgestellt;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 34 validiert und der Kommission mitgeteilt;

d) die ETIAS-Zentralstelle hat ihre Mitteilung an die Kommission gemäß Artikel 67 Absatz 3 getätigt;

e) eu-LISA hat den erfolgreichen Abschluss der Tests nach Absatz 1 Buchstabe b, Absatz 2 Buchstabe b, Absatz 3 Buchstabe b und Absatz 4 Buchstabe b festgestellt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(5) Die Kommission bestimmt im Wege eines Durchführungsrechtsaktes, ab welchem Zeitpunkt die Mechanismen und Verfahren für die automatische Datenqualitätskontrolle sowie die gemeinsamen Datenqualitätsindikatoren und die Mindestqualitätsstandards für Daten zu nutzen sind, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 37 Absatz 4 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests der Mechanismen und Verfahren für die automatische Datenqualitätskontrolle, der gemeinsamen Datenqualitätsindikatoren und der Mindestqualitätsstandards für Daten, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden durchgeführt hat, festgestellt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(6) Die Kommission beschließt im Wege eines Durchführungsrechtsaktes, zu welchem Zeitpunkt der CRRS seinen Betrieb aufnimmt, sobald folgende Voraussetzungen erfüllt wurden:

a) Die Maßnahmen nach Artikel 39 Absatz 5 und Artikel 43 Absatz 5 wurden angenommen;

b) eu-LISA hat den erfolgreichen Abschluss eines umfangreichen Tests des CRRS, den sie in Zusammenarbeit mit den mitgliedstaatlichen Behörden durchgeführt hat, festgestellt;

c) eu-LISA hat die technischen und rechtlichen Vorkehrungen für die Erhebung und Übermittlung der Daten nach Artikel 39 validiert und der Kommission mitgeteilt.

Die Kommission legt den in Unterabsatz 1 genannten Zeitpunkt so fest, dass er innerhalb von 30 Tagen nach dem Erlass des Durchführungsrechtsakts liegt.

(7) Die Kommission unterrichtet das Europäische Parlament und den Rat über die Ergebnisse der gemäß Absatz 1 Buchstabe b, Absatz 2 Buchstabe b, Absatz 3 Buchstabe b, Absatz 4 Buchstabe b, Absatz 5 Buchstabe und Absatz 6 Buchstabe b durchgeführten Tests.

(8) Die Mitgliedstaaten, die ETIAS-Zentraleinheit und Europol beginnen mit der Nutzung der einzelnen Interoperabilitätskomponenten ab dem von der Kommission gemäß den Absätzen 1, 2, 3 bzw. 4 jeweils festgelegten Zeitpunkt.

Artikel 69

Ausübung der Befugnisübertragung

(1) Die Befugnis zum Erlass delegierter Rechtsakte wird der Kommission unter den in diesem Artikel festgelegten Bedingungen übertragen.

(2) Die Befugnis zum Erlass delegierter Rechtsakte gemäß Artikel 28 Absatz 5, Artikel 39 Absatz 5, Artikel 49 Absatz 6, Artikel 63 Absatz 2 und Artikel 65 Absatz 8 wird der Kommission für einen Zeitraum von fünf Jahren ab dem 11. Juni 2019 übertragen. Die Kommission erstellt spätestens neun Monate vor Ablauf des Zeitraums von fünf Jahren einen Bericht über die Befugnisübertragung. Die Befugnisübertragung verlängert sich stillschweigend um Zeiträume gleicher Länge, es sei denn, das Europäische Parlament oder der Rat widersprechen einer solchen Verlängerung spätestens drei Monate vor Ablauf des jeweiligen Zeitraums.

(3) Die Befugnisübertragung gemäß Artikel 28 Absatz 5, Artikel 39 Absatz 5, Artikel 49 Absatz 6, Artikel 63 Absatz 2 und Artikel 65 Absatz 8 kann vom Europäischen Parlament oder vom Rat jederzeit widerrufen werden. Der Beschluss über den Widerruf beendet die Übertragung der in diesem Beschluss angegebenen Befugnisse. Er wird am Tag nach seiner Veröffentlichung im *Amtsblatt der Europäischen Union* oder zu einem im Beschluss über den Widerruf angegebenen späteren Zeitpunkt wirksam. Die Gültigkeit von delegierten Rechtsakten, die bereits in Kraft sind, wird von dem Beschluss über den Widerruf nicht berührt.

(4) Vor dem Erlass eines delegierten Rechtsakts konsultiert die Kommission die von den einzelnen Mitgliedstaaten benannten Sachverständigen, im Einklang mit den in der Interinstitutionellen Vereinbarung über bessere Rechtsetzung vom 13. April 2016 festgelegten Grundsätzen.

(5) Sobald die Kommission einen delegierten Rechtsakt erlässt, übermittelt sie ihn gleichzeitig dem Europäischen Parlament und dem Rat.

(6) Ein delegierter Rechtsakt, der gemäß Artikel 28 Absatz 5, Artikel 39 Absatz 5, Artikel 49 Absatz 6, Artikel 63 Absatz 2 und Artikel 65 Absatz 8 erlassen wurde, tritt nur in Kraft, wenn weder das Europäische Parlament noch der Rat innerhalb einer Frist von zwei Monaten nach Übermittlung dieses Rechtsakts an das Europäische Parlament und den Rat Einwände erhoben haben oder wenn vor Ablauf dieser Frist das Europäische Parlament und der Rat beide der Kommission mitgeteilt haben, dass sie keine Einwände erheben werden. Auf Initiative des Europäischen Parlaments oder des Rates wird diese Frist um zwei Monate verlängert.

Artikel 70

Ausschussverfahren

(1) Die Kommission wird von einem Ausschuss unterstützt. Dieser Ausschuss ist ein Ausschuss im Sinne der Verordnung (EU) Nr. 182/2011.

(2) Wird auf diesen Absatz Bezug genommen, so gilt Artikel 5 der Verordnung (EU) Nr. 182/2011.

Gibt der Ausschuss keine Stellungnahme ab, so erlässt die Kommission den Durchführungsrechtsakt nicht, und Artikel 5 Absatz 4 Unterabsatz 3 der Verordnung (EU) Nr. 182/2011 findet Anwendung.

Artikel 71

Beratergruppe

eu-LISA setzt eine Beratergruppe für Interoperabilität ein. Während der Konzept- und Entwicklungsphase der Interoperabilitätskomponenten findet Artikel 54 Absätze 4, 5 und 6 Anwendung.

Artikel 72

Schulung

eu-LISA nimmt Aufgaben im Zusammenhang mit Schulungen in der technischen Nutzung der Interoperabilitätskomponenten gemäß der Verordnung (EU) 2018/1726 wahr.

Die mitgliedstaatlichen Behörden und die Stellen der Union stellen ihren Bediensteten, die zur Verarbeitung von Daten mittels der Interoperabilitätskomponenten ermächtigt sind, ein geeignetes Schulungsprogramm zu Datensicherheit, Datenqualität, Datenschutzvorschriften, Datenverarbeitungsverfahren und den Informationspflichten gemäß Artikel 32 Absatz 4, Artikel 33 Absatz 4 und Artikel 47 zur Verfügung.

Gegebenenfalls werden auf Unionsebene gemeinsame Schulungskurse zu diesen Themen organisiert, um die Zusammenarbeit und den Austausch bewährter Verfahren zwischen den Bediensteten der mitgliedstaatlichen Behörden und der Stellen der Union, die zur Verarbeitung von Daten mittels der Interoperabilitätskomponenten ermächtigt sind, zu verbessern. Besonderes Augenmerk gilt dem Verfahren der Prüfung auf Mehrfachidentitäten, einschließlich der manuellen Verifizierung verschiedener Identitäten und der damit einhergehenden Notwendigkeit, angemessene Schutzmechanismen für Grundrechte beizubehalten.

Artikel 73

Handbuch

Die Kommission stellt in enger Zusammenarbeit mit den Mitgliedstaaten, eu-LISA und anderen zuständigen Stellen der Union ein Handbuch für die Umsetzung und den Betrieb der Interoperabilitätskomponenten zur Verfügung. Das Handbuch enthält technische und operative Leitlinien, Empfehlungen und bewährte Verfahren. Die Kommission nimmt dieses Handbuch in Form einer Empfehlung an.

Artikel 74

Überwachung und Bewertung

(1) eu-LISA stellt sicher, dass Verfahren vorhanden sind, um die Entwicklung der Interoperabilitätskomponenten und ihrer Anbindung an die einheitliche nationale Schnittstelle anhand von Zielen für Planung und Kosten sowie die Funktionsweise der Interoperabilitätskomponenten anhand von Zielen für die technische Leistung, Kostenwirksamkeit, Sicherheit und Qualität des Dienstes zu überwachen

(2) Bis zum 12. Dezember 2019 und danach alle sechs Monate während der Entwicklungsphase der Interoperabilitätskomponenten übermittelt eu-LISA dem Europäischen Parlament und dem Rat einen Bericht über den Stand der Entwicklung der Interoperabilitätskomponenten und ihrer Anbindung an die einheitliche nationale Schnittstelle. Sobald die Entwicklung abgeschlossen ist, wird dem Europäischen Parlament und dem Rat ein Bericht übermittelt, in dem detailliert dargelegt wird, wie die Ziele, insbesondere für die Planung und die Kosten, erreicht wurden, und in dem etwaige Abweichungen begründet werden.

(3) Vier Jahre nach Inbetriebnahme der einzelnen Interoperabilitätskomponenten gemäß Artikel 68 und danach alle vier Jahre übermittelt eu-LISA dem Europäischen Parlament, dem Rat und der Kommission einen Bericht über die technische Funktionsweise der Interoperabilitätskomponenten einschließlich ihrer Sicherheit.

(4) Ferner erstellt die Kommission ein Jahr nach jedem Bericht von eu-LISA eine Gesamtbewertung der Interoperabilitätskomponenten, die Folgendes beinhaltet:

a) eine Beurteilung der Anwendung dieser Verordnung;

b) eine Analyse der Ergebnisse, gemessen an den Zielen dieser Verordnung und ihrer Auswirkungen auf die Grundrechte, einschließlich insbesondere einer Bewertung der Auswirkungen der Interoperabilitätskomponenten auf das Recht auf Nichtdiskriminierung;

c) eine Bewertung des Funktionierens des Web-Portals, einschließlich Zahlen zur Nutzung des Web-Portals und der Zahl von Anfragen, denen entsprochen wurde;

d) eine Beurteilung, ob die grundlegenden Prinzipien der Interoperabilitätskomponenten weiterhin Gültigkeit haben;

e) eine Beurteilung der Sicherheit der Interoperabilitätskomponenten;

f) eine Beurteilung der Nutzung des CIR zu Zwecken der Identifizierung;

g) eine Beurteilung der Nutzung des CIR zu Zwecken der Verhinderung, Aufdeckung und Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten;

h) eine Beurteilung etwaiger Auswirkungen, auch etwaiger unverhältnismäßiger Auswirkungen auf den Verkehrsfluss an den Grenzübergangsstellen, und der Auswirkungen auf den Gesamthaushalt der Union;

i) eine Beurteilung der Abfrage der Interpol-Datenbanken über das ESP, einschließlich Informationen über die Zahl der Übereinstimmungen in Interpol-Datenbanken und Informationen zu allen festgestellten Problemen;

Die Gesamtbewertung gemäß Unterabsatz 1 dieses Absatzes schließt etwaige erforderliche Empfehlungen ein. Die Kommission übermittelt den Bewertungsbericht dem Europäischen Parlament, dem Rat, dem Europäischen Datenschutzbeauftragten und der Agentur der Europäischen Union für Grundrechte.

(5) Die Kommission übermittelt dem Europäischen Parlament und dem Rat bis zum 12. Juni 2020 und danach jedes Jahr, bis die Durchführungsrechtsakte der Kommission nach Artikel 68 erlassen wurden, einen Bericht über den Stand der Vorbereitungen für die vollumfängliche Durchführung dieser Verordnung. Dieser Bericht enthält auch genaue Angaben über die angefallenen Kosten und Informationen über sämtliche Risiken, die Auswirkungen auf die Gesamtkosten haben könnten.

(6) Zwei Jahre nach Inbetriebnahme des MID gemäß Artikel 68 Absatz 4 nimmt die Kommission eine Analyse der Auswirkungen des MID auf das Recht auf Nichtdiskriminierung vor. Nach diesem ersten Bericht ist die Analyse der Auswirkungen des MID auf das Recht auf Nichtdiskriminierung Teil der in Absatz 4 Buchstabe b des vorliegenden Artikels genannten Analyse.

(7) Die Mitgliedstaaten und Europol stellen eu-LISA und der Kommission die für die Ausarbeitung der Berichte nach den Absätzen 3 bis 6 erforderlichen Informationen zur Verfügung. Diese Informationen dürfen nicht zu einer Beeinträchtigung der Arbeitsverfahren führen oder Angaben enthalten, die Rückschlüsse auf Quellen, Bedienstete oder Ermittlungen der benannten Behörden ermöglichen.

(8) eu-LISA stellt der Kommission die Informationen zur Verfügung, die zur Durchführung der in Absatz 4 genannten Gesamtbewertung erforderlich sind.

(9) Die Mitgliedstaaten und Europol erstellen unter Einhaltung der nationalen Rechtsvorschriften über die Veröffentlichung von sensiblen Informationen und unbeschadet der erforderlichen Einschränkungen zum Schutz der Sicherheit und der öffentlichen Ordnung, zur Verhinderung von Kriminalität und zur Gewährleistung, dass keine nationalen Ermittlungen beeinträchtigt werden, Jahresberichte über die Wirksamkeit des Zugangs zu im CIR gespeicherten Daten zum Zwecke der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten; diese Berichte enthalten Informationen und Statistiken über

a) den genauen Zweck der Abfrage, einschließlich über die Art der terroristischen Straftat oder sonstigen schweren Straftaten;

b) die hinreichenden Anhaltspunkte für den begründeten Verdacht, dass ein Verdächtiger, ein Täter oder ein Opfer unter die Verordnung (EU) Nr. 603/2013 fällt;

c) die Zahl der Anträge auf Zugang zum CIR zu Zwecken der Verhinderung, Aufdeckung oder Untersuchung terroristischer Straftaten oder sonstiger schwerer Straftaten;

d) die Anzahl und die Art von Fällen, in denen die Identität einer Person festgestellt werden konnte;

e) die Notwendigkeit für und die Anwendung des Dringlichkeitsverfahrens in Ausnahmefällen, darunter in Fällen, in denen bei der nachträglichen Überprüfung durch die zentrale Zugangsstelle festgestellt wurde, dass das Dringlichkeitsverfahren nicht gerechtfertigt war.

Die Jahresberichte der Mitgliedstaaten und von Europol werden der Kommission bis zum 30. Juni des Folgejahres vorgelegt.

(10) Zur Verwaltung von Anträgen der Nutzer auf Zugang gemäß Artikel 22 und zur Erleichterung der Erhebung der in den Absätzen 7 und 9 des vorliegenden Artikels aufgeführten Informationen für die Zwecke der Erstellung der in jenen Absätzen genannten Berichte und Statistiken wird den Mitgliedstaaten eine technische Lösung bereitgestellt. Die Kommission erlässt Durchführungsrechtsakte zur Festlegung der Spezifikationen der technischen Lösung. Diese Durchführungsrechtsakte werden gemäß dem in Artikel 70 Absatz 2 genannten Prüfverfahren erlassen.

Artikel 75

Inkrafttreten und Anwendbarkeit

Diese Verordnung tritt am zwanzigsten Tag nach ihrer Veröffentlichung im *Amtsblatt der Europäischen Union* in Kraft.

Die Bestimmungen dieser Verordnung über das ESP gelten ab dem von der Kommission gemäß Artikel 68 Absatz 1 bestimmten Zeitpunkt.

Die Bestimmungen dieser Verordnung über den gemeinsamen BMS gelten ab dem von der Kommission gemäß Artikel 68 Absatz 2 bestimmten Zeitpunkt.

Die Bestimmungen dieser Verordnung über den CIR gelten ab dem von der Kommission gemäß Artikel 68 Absatz 3 bestimmten Zeitpunkt.

Die Bestimmungen dieser Verordnung über den MID gelten ab dem von der Kommission gemäß Artikel 68 Absatz 4 bestimmten Zeitpunkt.

Die Bestimmungen dieser Verordnung über die Mechanismen und Verfahren für die automatische Datenqualitätskontrolle, die gemeinsamen Datenqualitätsindikatoren und die Mindestqualitätsstandards gelten ab dem von der Kommission gemäß Artikel 68 Absatz 5 bestimmten Zeitpunkt.

Die Bestimmungen dieser Verordnung über den CRRS gelten ab dem von der Kommission gemäß Artikel 68 Absatz 6 bestimmten Zeitpunkt.

Artikel 6, 12, 17, 25, 38, 42, 54, 56, 58, 66, 67, 69, 70, 71, 73 und 74 Absatz 1, gelten ab dem 11. Juni 2019.

Diese Verordnung gilt für Eurodac ab dem Tag der Anwendbarkeit der Neufassung der Verordnung (EU) Nr. 603/2013.

Diese Verordnung ist in allen ihren Teilen verbindlich und gilt gemäß den Verträgen unmittelbar in den Mitgliedstaaten.

Geschehen zu Brüssel am 20. Mai 2019.

Im Namen des Europäischen Parlaments	*Im Namen des Rates*
Der Präsident	*Der Präsident*
A. TAJANI	G. CIAMBA

ISSN 1977-0642 (elektronische Ausgabe)
ISSN 1725-2539 (Papierausgabe)

Amt für Veröffentlichungen der Europäischen Union
2985 Luxemburg
LUXEMBURG

DE