# Gruppenarbeit zum Thema „Wearables“

## Aufgabe 1

Rufen Sie das Glossar der App Stadt | Land | DatenFluss über die Wissensbasis auf und lesen Sie den Glossareintrag zum Thema „Wearables“.

## Aufgabe 2

Finden Sie gemeinsam Antworten auf folgende Fragen:

- Was genau versteht man unter Wearables?
- Woher kommt der Name?
- Welche Wearables gibt es bereits?

Notieren Sie sich für die ein- bis zweiminütige Kurzpräsentation ggf. Stichpunkte.

# Gruppenarbeit zum Thema „Fitness-Tracker“

## Aufgabe 1

Rufen Sie das Glossar der App Stadt | Land | DatenFluss über die Wissensbasis auf und lesen Sie den Glossareintrag zum Thema „Fitness-Tracker“.

## Aufgabe 2

Finden Sie gemeinsam Antworten auf folgende Fragen:

- Wie funktioniert die Datenübertragung bei Fitness-Trackern?
- Wie stehen die Begriffe „Fitness-Tracker“ und „Wearable“ zueinander?

Notieren Sie sich für die ein- bis zweiminütige Kurzpräsentation ggf. Stichpunkte.

# Gruppenarbeit zum Thema „Smartwatch“

## Aufgabe 1

Rufen Sie das Glossar der App Stadt | Land | DatenFluss über die Wissensbasis auf und lesen Sie den Glossareintrag zum Thema „Smartwatch“.

## Aufgabe 2

Finden Sie gemeinsam Antworten auf folgende Fragen:

- Was ist der Unterschied zwischen einer Smartwatch und einem Fitnessarmband?
- Welche Technologien nutzen Smartwatches?

Notieren Sie sich für die ein- bis zweiminütige Kurzpräsentation ggf. Stichpunkte.

# Gruppenarbeit zum Thema „Self-Tracking“

## Aufgabe 1

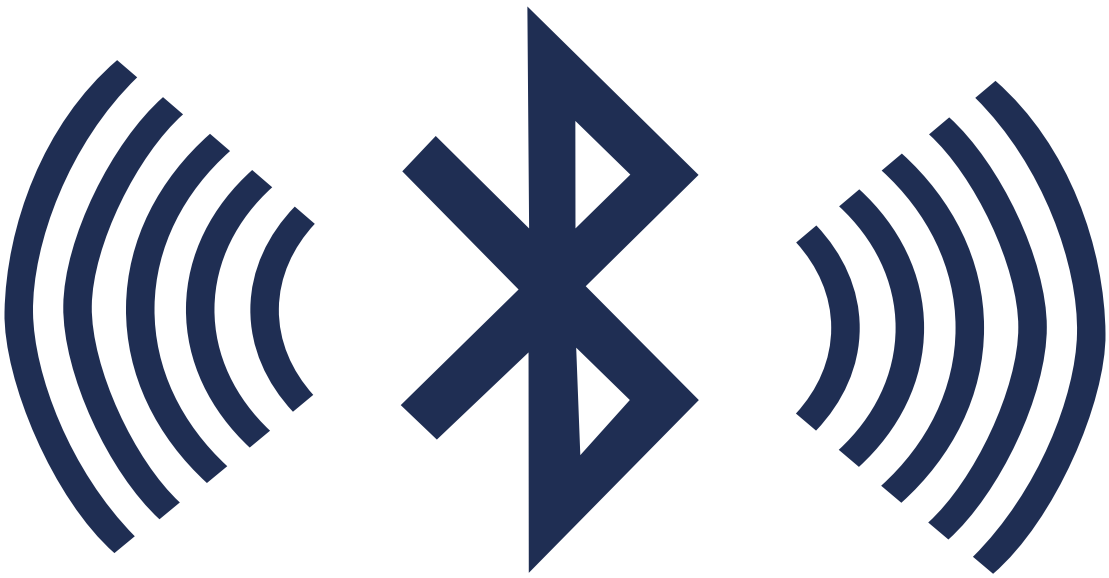
Rufen Sie das Glossar der App Stadt | Land | DatenFluss über die Wissensbasis auf und lesen Sie den Glossareintrag zum Thema „Self-Tracking“.

## Aufgabe 2

Finden Sie gemeinsam Antworten auf folgende Fragen:

- Was bedeutet Self-Tracking genau?
- Welche Ziele können mit Self-Tracking verfolgt werden?

Notieren Sie sich für die ein- bis zweiminütige Kurzpräsentation ggf. Stichpunkte.



**Symbolbilder für das Tafelbild „Funktionsweise“**



# Lernsequenz „Wen interessieren welche Daten?“

# 11 Alltagstipps für die Nutzung von Fitness-Trackern

1. Recherchieren Sie schon vor dem Kauf, ob der Anbieter Wert auf Datenschutz und Datensicherheit legt. Dazu bieten sich neben den Herstellerseiten auch unabhängige Tests und Vergleichsportale an.

2. Manche Hersteller von Fitness-Trackern teilen die Gesundheitsdaten mit anderen Firmen, ohne ihre Kund*innen explizit darauf hinzuweisen. Ein weiteres Problem: Meistens werden die Fitness-Daten in der Server-Cloud gespeichert. Wenn die Cloud gehackt wird, geraten persönliche Gesundheitsdaten in die Hände von Unbefugten. Es gibt aber auch Fitness-Tracker, die ihre Daten nur lokal, also auf dem Gerät, speichern. Solche Geräte sind zu empfehlen, wenn man auf Datensparsamkeit Wert legt.

3. Generell sollten Sie prüfen, welche Berechtigungen Smartphone-Apps von Ihnen verlangen. Verlangen sie zum Beispiel den Zugriff auf Smartphone-Funktionen, die für eine Nutzung als Fitness-Tracker nicht zwingend notwendig sind, wägen Sie noch einmal ab.

4. Wägen Sie generell ab: Sind Ihnen die Möglichkeiten, die das Gerät bietet, so wichtig, dass eine Weiterverarbeitung u. a. sensibler Daten für Sie in Ordnung ist?

5. Die Datenübertragung muss verschlüsselt ablaufen. Auch beim Zugang zu den Fitnessportalen gilt: Sichere Passwörter sind Pflicht. Zur Unterstützung bei der sicheren Passwortvergabe gibt es unterschiedliche Passwort-Verwaltungs-Tools. Sie generieren sichere Passwörter mit zufällig zusammengewürfelten Buchstaben, Zahlen und Sonderzeichen. Da sich diese Passwörter nur schwer merken lassen, ist die zweite Aufgabe dieser Tools das Verwalten der verschiedenen Passwörter. Sie legen eine Art Passwort-Datenbank an, für deren Zugang man selbst ein so-genanntes Master-Passwort benötigt. Die hinterlegten Passwörter werden zusätzlich einzeln verschlüsselt, wobei verschiedene Algorithmen zum Einsatz kommen.

6. Bei der Eröffnung eines Kontos in der Fitness-App ist es nicht immer notwendig, alle vorgegebenen Angaben zu machen. Sie müssen nicht mit Klarnamen, Ihrem genauen Geburtsdatum oder Ihrer Haupt-Mailadresse operieren.

7. Nehmen Sie nicht die Abkürzung über Facebook oder Google-Konten bei der Anmeldung, da sonst Ihre Daten auch bei diesen Plattformen landen können.

8. Die Geräte sammeln schützenswerte Daten. Deshalb ist es wichtig, auf die Geschäftsbedingungen der Anbieter zu achten. Außerdem werden die Geräte oft mit einem Standardpasswort – beispielsweise „00000“ – ausgeliefert. Bei solchen Voreinstellungen haben Hacker*innen leichtes Spiel, weshalb man bei neuen Geräten zügig das Passwort ändern sollte.

9. Führen Sie regelmäßig Updates durch, um sicherzustellen, dass die App auf dem aktuellen Stand ist. Über Updates werden häufig auch Sicherheitslücken geschlossen. Haben Sie die Einstellung gewählt, dass die Updates automatisch aufgespielt werden, lohnt es sich, in regelmäßigen Abständen die Protokolle anzuschauen. Gleiches gilt für Änderungen der AGBs, die oft intransparent kommuniziert werden.

10. Denken Sie daran, dass Sie Ihr Wearable nicht rund um die Uhr tragen müssen. Setzen Sie es bewusst ein, zum Beispiel beim Sport.

11. Überlegen Sie immer, welche Ihrer Trackingdaten Sie in Sozialen Netzwerken teilen und welche besser nicht.

1.

Recherchieren Sie schon vor dem Kauf eines Fitness-Trackers, ob der Anbieter Wert auf Datenschutz und Datensicherheit legt. Dazu bieten sich neben den Herstellerseiten auch un-abhängige Tests und Vergleichsportale an.

2.

Manche Hersteller von Fitness-Trackern teilen die Gesundheitsdaten mit anderen Firmen, ohne ihre Kund*innen explizit darauf hinzuweisen. Ein weiteres Problem: Meistens werden die Fitness-Daten in der Server-Cloud gespeichert. Wenn die Cloud gehackt wird, geraten persönliche Gesundheitsdaten in die Hände von Unbefugten.

Es gibt aber auch Fitness-Tracker, die ihre Daten nur lokal, also auf dem Gerät, speichern. Solche Geräte sind zu empfehlen, wenn man auf Datensparsamkeit Wert legt.

3.

Generell sollten Sie prüfen, welche Berechtigungen Smartphone-Apps von Ihnen verlangen. Verlangen sie zum Beispiel den Zugriff auf Smartphone-Funktionen, die für eine Nutzung als Fitness-Tracker nicht zwingend notwendig sind, wägen Sie noch einmal ab.

4.

Wägen Sie generell ab: Sind Ihnen die Möglichkeiten, die das Gerät bietet, so wichtig, dass eine Weiterverarbeitung u. a. sensibler Daten für Sie in Ordnung ist?

5.

Die Datenübertragung muss verschlüsselt ablaufen. Auch beim Zugang zu den Fitness-portalen gilt: Sichere Passwörter sind Pflicht. Zur Unterstützung bei der sicheren Passwort-vergabe gibt es unterschiedliche Passwort-Verwaltungs-Tools. Sie generieren sichere Passwörter mit zufällig zusammengewür-felten Buchstaben, Zahlen und Sonderzei-chen. Da sich diese Passwörter nur schwer merken lassen, ist die zweite Aufgabe die-ser Tools das Verwalten der verschiedenen Passwörter. Sie legen eine Art Passwort-Datenbank an, für deren Zugang man selbst ein sogenanntes Master-Passwort benötigt. Die hinterlegten Passwörter werden zusätzlich einzeln verschlüsselt, wobei verschiedene Algorithmen zum Einsatz kommen.

6.

Bei der Eröffnung eines Kontos in der Fitness-App ist es nicht immer notwendig, alle vorgegebenen Angaben zu machen. Sie müssen nicht mit Klarnamen, Ihrem genauen Geburtsdatum oder Ihrer Haupt-Mailadresse operieren.

7.

Nehmen Sie nicht die Abkürzung über Facebook oder Google-Konten bei der Anmeldung, da sonst Ihre Daten auch bei diesen Plattformen landen können.

8.

Die Geräte sammeln schützenswerte Daten. Deshalb ist es wichtig, auf die Geschäftsbedingungen der Anbieter zu achten. Außerdem werden die Geräte oft mit einem Standardpasswort – beispielsweise „00000“ – ausgeliefert. Bei solchen Voreinstellungen haben Hacker*innen leichtes Spiel, weshalb man bei neuen Geräten zügig das Passwort ändern sollte.

9.

Führen Sie regelmäßig Updates durch, um sicherzustellen, dass die App auf dem aktuellen Stand ist. Über Updates werden häufig auch Sicherheitslücken geschlossen. Haben Sie die Einstellung gewählt, dass die Updates automatisch aufgespielt werden, lohnt es sich, in regelmäßigen Abständen die Protokolle anzuschauen. Gleiches gilt für Änderungen der AGBs, die oft intransparent kommuniziert werden.

10.

Denken Sie daran, dass Sie Ihr Wearable nicht rund um die Uhr tragen müssen. Setzen Sie es bewusst ein, zum Beispiel beim Sport.

11.

Überlegen Sie immer, welche Ihrer Tracking-daten Sie in sozialen Netzwerken teilen und welche besser nicht.