Infoblatt

DATENSCHUTZ

SELF TRACKING

Der Schutz personenbezogener Daten ist in Deutschland und in der EU ein Grundrecht. Es wird zwar nicht direkt im Grundgesetz genannt, fällt jedoch unter das ‚Recht auf informationelle Selbstbestimmung', das sich von der Menschenwürde und der allgemeinen Handlungsfreiheit ableitet. Gesetzlich ist Datenschutz vor allem in der EU-Datenschutz-Grundverordnung (DSGVO) und im Bundesdatenschutzgesetz geregelt. Über die Zugänglichkeit der ‚personenbezogenen Daten' darf nach der DSGVO grundsätzlich jede*r selbst entscheiden, wobei unter bestimmten Voraussetzungen eine Datenverarbeitung auch ohne Einwilligung der betroffenen Person zulässig sein kann. Unter ‚personenbezogene Daten' fallen alle Informationen über eine natürliche Person. Besonderen Schutzes bedürfen sensible Daten wie Informationen über die Gesundheit.

Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dazu gehören selbstverständlich Abbildungen und Stimme, aber auch Details wie z. B. Name, Adresse, Geburtsdatum, Alter, Gewicht, Augenfarbe oder Geburtsort eines Menschen.

Wann dürfen personenbezogene Daten verarbeitet werden?

- Personenbezogene Daten dürfen nur dann erfasst, gespeichert, ausgewertet oder weitergegeben werden, wenn der Betroffene seine **Einwilligung** hierzu erteilt hat oder die Datenverarbeitung durch eine gesetzliche Regelung erlaubt ist. Beispielsweise ist eine Datenverarbeitung, die für die Erfüllung eines Vertrages mit der betroffenen Person notwendig ist, gesetzlich auch ohne gesonderte Einwilligung erlaubt.

  Hinweis: Das ist letztlich auch der rechtliche Ausgangspunkt für die Frage, welche Daten eine App wirklich braucht und wo die Nutzenden das Recht haben müssen, frei zu entscheiden.

- Jugendliche unter 16 Jahren können nicht selbst wirksam einwilligen, sondern brauchen die Einwilligung ihrer Eltern.

  Hinweis: In der Arbeit mit Jugendlichen kann man prüfen, ob beim Erwerb der App bzw. bei den Datenfreigaben eine Altersabfrage erfolgt und wie diese gestaltet ist. Zudem bietet dieser Aspekt die Möglichkeit auf die Geschäftsfähigkeit einzugehen.

- Die Einwilligung kann widerrufen werden.

  Hinweis: Die Widerrufsmöglichkeit sollte einfach und transparent gestaltet sein, was man anhand ausgewählter Beispiele überprüfen könnte.

Prüfen: Welche Daten braucht eine App wirklich? Tipps und Hinweise

- **Zugriffsrechte** von Apps überprüfen. Meist können hier manuell Anpassungen vorgenommen werden. Das findet man bei Smartphones unter: Einstellungen → Apps und Benachrichtigungen → App-Berechtigungen oder App-Info.
- In den **AGB** oder Datenschutzbestimmungen nachlesen, wo die Daten gespeichert, an wen die Daten weitergegeben und welche Zugriffsrechte der App eingeräumt werden.
- Nicht genutzte **Apps löschen,** da diese auch weiterhin auf Daten zugreifen und diese verarbeiten können.
- Umsichtig mit **Cookies** in Surfing-Apps umgehen. Cookies verschaffen sich nämlich Zugriff auf Daten, wie die ID des genutzten Geräts, die auch den Standort verrät, und zuvor besuchte Websites und Social Communities.
  - Wenn möglich, lediglich temporäre Cookies zulassen, da diese nur für die einzelne Online-Sitzung gespeichert und am Ende wieder gelöscht werden.
  - Tracking-Cookies von Drittanbietern in den Browsereinstellungen deaktivieren. Diese Cookies speichern nämlich Informationen über mehrere Sitzungen hinweg.
  - Cookies in den Browsereinstellungen regelmäßig löschen.

Was macht ein Algorithmus?

Algorithmen sind Rechenvorgänge zur Lösung eines Problems in Form von Handlungsanweisungen und bilden die Grundlage von Computerprogrammen. Sie können viele simple Rechenschritte in kürzester Zeit durchführen und so große Datenmengen aufbereiten und analysieren.