Was passiert mit meinen Daten? Warum ist Datenschutz wichtig?

Was ist Datenschutz?

Für manche Menschen ist Datenschutz ein schwieriges Thema – abstrakt und in jedem Fall technisch. Einige fragen sich vielleicht, inwiefern Datenschutz für das tägliche Leben überhaupt relevant ist. Andererseits schützen wir unsere Daten im Alltag ganz selbstverständlich: Wir haben Vorhänge vor unseren Fenstern, schließen die Türe, wenn wir etwas Sensibles besprechen, und geben manche Informationen nur an ausgewählte Personen weiter, während wir andere Daten lieber ganz für uns behalten.

In einer digitalen Umgebung wird der Schutz von Daten durch die Festlegung von Regeln erreicht, die bestimmen, wer auf Informationen zugreifen darf. Der Unterschied, zum Beispiel zum Schließen der Vorhänge, besteht darin, dass im digitalen Raum oft jemand anders für den Umgang mit den Daten zuständig ist als die Person, um deren Privatsphäre es geht; wir sind beim Schutz unserer Daten vor unbefugtem Zugriff häufig auf Dritte angewiesen. Oft wissen wir nicht einmal, ob unsere „digitalen Vorhänge“ offen oder zugezogen sind.

Warum ist Datenschutz wichtig?

Der Schutz unserer Daten als ein Aspekt unserer Privatsphäre ist wesentlich für unser menschliches Dasein. Es ist eine grundlegende Erkenntnis aus der Psychologie, dass sich Menschen unter (potenzieller) Beobachtung anders verhalten als wenn sie unbeobachtet sind. Unsere Privatsphäre dient uns als Raum der Selbstbestimmung und Freiheit, in dem wir gesellschaftliche Normen auch durchbrechen und mit neuem Verhalten und Denken experimentieren können. Sie ist ein Ort der Ruhe

und Entspannung. In der Privatsphäre sollten Selbsteinschätzung und freie Kommunikation möglich sein.[1] Der Datenschutz als Teil des Schutzes der Privatsphäre sollte dies gewährleisten können. Dementsprechend sichert der Datenschutz die Freiheit des Einzelnen, indem er die Erhebung und Verarbeitung persönlicher Daten verbietet und sie nur unter bestimmten Bedingungen zulässt.

Datenschutz hat aber auch eine überindividuelle oder strukturelle Dimension.[2] Informationsbeziehungen sind Machtbeziehungen; wer über Informationen, d. h. Daten, verfügt, kann Macht ausüben. Das Individuum muss vor asymmetrischen Machtverhältnissen geschützt werden. Das Ziel des Datenschutzes ist also auch struktureller Natur, da es dabei auch um die Begrenzung von Machtungleichgewichten geht.

Was hat der Datenschutz mit Apps zu tun?

Apps, kurz für englisch „applications“ (deutsch: Anwendungen), sind die Programme auf unseren Handys und Tablets. Wenn wir eine App nutzen wollen, müssen wir häufig bestimmte Informationen angeben, beispielsweise unseren Namen, eine E-Mail-Adresse und unser Geburtsdatum, manchmal auch Geschlecht, Postadresse oder Zahlungsdaten. Darüber hinaus sammeln Apps oft Daten, ohne dass wir diese aktiv bereitstellen. Wenn wir eine App installieren, erlauben wir ihr in der Regel den Zugriff auf eine Vielzahl von Funktionen auf unserem Mobilgerät, beispielsweise Standortdaten, Aktivitätssensoren, Mikrofon oder Kamera. Die App sammelt dann bestimmte Daten, während wir das Gerät nutzen. Davon profitieren die App-Anbieter, da ihnen die Informationen helfen, ihre Produkte zu verbessern. Das bedeutet aber auch, dass App-Anbieter jede Menge Informationen abrufen können: Wann benutze ich mein Smartphone, Tablet usw.? Wie nutze ich mein Gerät? Wo befinde ich mich? Aus diesen Daten lässt sich ein Bild der nutzenden Person zeichnen.

Wie werden unsere Daten geschützt?

Unsere Daten sind durch eine Reihe gesetzlicher Vorschriften geschützt. Der Datenschutz ist grundsätzlich in Artikel 8 der Europäischen Menschenrechtskonvention (EMRK), auf europäischer Ebene in Artikel 7 und Artikel 8 der Charta der Grundrechte der Europäischen Union (GrCh) und durch mehrere Rechte im deutschen Grundgesetz geregelt. Diese verschiedenen Grundrechte sind durch die Datenschutzgrundverordnung (DSGVO) auf Ebene der Europäischen Union und in Deutschland durch das Bundesdatenschutzgesetz und die länderspezifischen Datenschutzgesetze (zum Beispiel das Bayerische Datenschutzgesetz) abgedeckt. Die Gesetze gelten, sobald ein öffentlicher oder nicht-öffentlicher Akteur personenbezogene Daten verarbeitet. Der Begriff „Verarbeitung“ ist dabei weit gefasst. Tatsächlich bezieht er sich auf jeglichen Umgang mit Daten, einschließlich der Erhebung und Löschung von Daten.[3]

Die DSGVO verbietet grundsätzlichen die Verarbeitung personenbezogener Daten. Eine Verarbeitung ist nur in Ausnahmefällen zulässig, falls eine der im Gesetz genannten Voraussetzungen erfüllt ist.

Womit erkläre ich mich einverstanden, wenn ich auf „Ich stimme zu“ klicke?

Nach europäischem Recht ist jede Verarbeitung personenbezogener Daten (zum Beispiel Gesundheitsdaten) grundsätzlich unzulässig. Sie ist nur in Ausnahmefällen rechtmäßig, wenn bestimmte Bedingungen erfüllt sind. Die Einwilligung ist eine von sechs möglichen Bedingungen, unter denen die Verarbeitung personenbezogener Daten erlaubt ist (Art. 6 und Art. 9(2) lit. a DSGVO).

„Einwilligung“ ist in der DSGVO definiert als „jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist“
(Art. 4 Nr. 11 DSGVO).

Wann liegt eine Einwilligung vor?

Eine Einwilligung kann nur dann frei und damit gültig sein, wenn die betroffene Person eine echte Wahl hat und keine Gefahr der Täuschung, Einschüchterung, Nötigung oder anderer negativer Folgen besteht.[4] Gemäß Art. 7 Abs. 2 DSGVO müssen Datenbeauftragte sicherstellen, dass Betroffene ihre Einwilligung jederzeit widerrufen können und der Widerruf genauso einfach ist wie die Erteilung der Einwilligung.

Eine Weitergabe von Daten an Dritte – zum Beispiel im Rahmen von Datenhandel – darf nur erfolgen, wenn eine Einwilligung erteilt wurde. Aus diesem Grund muss die Zustimmung zur Datenschutzerklärung die Möglichkeit der Weitergabe an Dritte beinhalten. Wenn Sie mit der Weitergabe der Daten an Dritte nicht einverstanden sind, sollten Sie Ihre Einwilligung nicht erteilen. Dies bedeutet jedoch oft auch, dass der entsprechende Dienst, zum Beispiel die Nutzung einer Social-Media-Plattform oder Online-Handel, nicht möglich ist.

Die DSGVO bietet ein höheres Schutzniveau für besonders sensible Daten, beispielsweise Gesundheitsdaten. Auch hier geht ein grundsätzliches Verbot der Verarbeitung dieser besonderen personenbezogenen Daten mit einer Reihe von Zulässigkeitstatbeständen einher (Art. 9 (2) DSGVO). Dies bedeutet, dass unter bestimmten Umständen auch die Verarbeitung dieser besonders sensiblen Daten rechtmäßig sein kann.

Daten als Währung?

Viele Online-Dienste, zum Beispiel Social-Media-Plattformen wie Facebook oder Instagram, sind auf den ersten Blick „kostenlos“, weil für die Nutzung keine Gebühren entstehen. Allerdings sind sie nur scheinbar „kostenlos“, denn die anbietenden Unternehmen verdienen mit den Nutzerdaten Geld, insbesondere durch Werbung. Nutzende Personen stimmen bei der Registrierung normalerweise der Verarbeitung ihrer Daten zu. Die Nutzung solcher Online-Dienste ist also nicht wirklich kostenlos, da man mit den zur Verfügung gestellten Daten „bezahlt“.

Ein besonders wirksames Schutzinstrument der DSGVO ist das „Koppelungsverbot“. Mit anderen Worten: Unternehmen können nicht verlangen, dass die Nutzung der Dienste eines Unternehmens nur

unter der Voraussetzung möglich ist, dass Personen ihre persönlichen Daten zur Verfügung stellen.[5] Wenn also eine Person freiwillig in die Nutzung eines bestimmten Dienstes einwilligt und ein Unternehmen versucht, die Dienstleistung daran zu koppeln, dass die Person auch in die Bereitstellung personenbezogener Daten einwilligt, gilt der Vertrag nicht als freiwillig und ist ungültig. Die Möglichkeit, Daten als Währung zu verwenden, wird somit effektiv verhindert, da die Verarbeitung personenbezogener Daten typischerweise nicht für die Auftragserfüllung erforderlich ist. Eine aktuelle Entwicklung ist das sogenannte „Zahl oder Zustimmung"-Modell, das vor allem von Facebook/Meta eingeführt wurde. Dabei haben Nutzer:innen die Wahl, entweder der Erhebung und Verarbeitung ihrer personenbezogenen Daten (hauptsächlich für zielgerichtete Werbung) zuzustimmen oder für einen Dienst ohne Datenerhebung und -verarbeitung zu bezahlen.[6]

1. Trepte, 2012, Privatsphäre aus psychologischer Sicht, in Schimdt/Weichter (Hrsg.), Datenschutz, Bundeszentrale für politische Bildung, 62.↑
2. Lewinski, 2012, Zur Geschichte von Privatsphäre und Datenschutz, in Schimdt/Weichter (Hrsg.), Datenschutz, Bundeszentrale für politische Bildung, S. 32.↑
3. Tinnefeld/Buchner/Petri/Hansen, Einführung in das Datenschutzrecht, 2024, Kap. 2 Rn. 42ff.↑
4. Datenschutzgruppe 29, WP259 rev.01 , S. 8.↑
5. Tinnefeld/Buchner/Petri/Hansen, Einführung in das Datenschutzrecht, 2024, Kap4. Rn. 41ff.↑
6. D'Amico, A., Pelekis, D. ., Teixeira Santos, C., & Duivenvoorde, B. (2024). Meta's Pay-or-Okay Model: An analysis under EU Data Protection, Consumer and Competition Law. Technology and Regulation, 2024, 254-272. https://doi.org/10.71265/tkk29041↑