Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Justiz- und Polizeidepartement EJPD

Bundesamt für Justiz BJ

FAQ Datenschutzrecht

1. Februar 2023

1 Entscheid des Bundesrates 2
1.1 Was hat der Bundesrat am 31. August 2022 entschieden? 2
1.2 Warum tritt das neue Datenschutzrecht erst am 1. September 2023 in Kraft? 2
2 Zweck und Inhalt des Datenschutzrechts 2
2.1 Was ist der Sinn und Zweck des Datenschutzrechts? 2
2.2 Was regelt das Datenschutzrecht? 2
3 Wesentliche Neuerungen der Totalrevision des Datenschutzrechts 2
3.1 Warum war eine Revision des Datenschutzrechts notwendig? 2
3.2 Was sind die Bestrebungen der Totalrevision des Datenschutzgesetzes? 2
3.2.1 Wie wurde die Transparenz für die Betroffenen verbessert? 3
3.2.2 Wie wurde die Unabhängigkeit und die Aufsichtskompetenz des EDÖB gestärkt? 3
3.2.3 Was passiert, wenn jemand gegen die Datenschutzvorschriften verstösst? 3
3.2.4 Was beinhaltet die Datenschutz-Folgenabschätzung? 4
3.2.5 Was ist eine automatisierte Einzelfallentscheidung und welche Rechte hat die betroffene Person dabei? 4
3.2.6 Was ist unter «Profiling» zu verstehen und inwiefern geniesst die betroffene Person hierbei einen erhöhten Schutz? 4
3.2.7 Wozu berechtigt das Recht auf Datenherausgabe und Datenübertragung? 5
4 Internationale Entwicklungen des Datenschutzes 5
4.1 Welche Bedeutung hat die EU-Richtlinie 2016/680 für die Schweiz? 5
4.2 Welche Bedeutung hat die Datenschutz-Grundverordnung der EU für die Schweiz? 5
4.3 Erfüllt das schweizerische Datenschutzrecht die europäischen Standards? 5
4.4 Was sind die Folgen, wenn die EU-Kommission das Datenschutzniveau der Schweiz nicht als angemessen anerkennt? 6
4.5 Wo steht die Schweiz mit der Ratifikation der modernisierten Datenschutz-Konvention 108+ des Europarates? 6
4.6 Warum soll die Schweiz der modernisierten Datenschutz-Konvention 108+ des Europarates beitreten? 6

1 Entscheid des Bundesrates

1.1 Was hat der Bundesrat am 31. August 2022 entschieden?

Der Bundesrat setzt mit seinem Entscheid das neue Datenschutzgesetz (DSG) und die entsprechenden Ausführungsbestimmungen in der neuen Datenschutzverordnung (DSV) und der neuen Verordnung über Datenschutzzertifizierungen (VDSZ) auf den 1. September 2023 in Kraft.

1.2 Warum tritt das neue Datenschutzrecht erst am 1. September 2023 in Kraft?

Mit der Inkraftsetzung des neuen Datenschutzrechts auf den 1. September 2023 kommt der Bundesrat einem Anliegen aus der Wirtschaft nach. Mit der Übergangsfrist von einem Jahr erhalten die Datenbearbeitungsverantwortlichen genügend Zeit, die notwendigen Vorkehrungen für die Umsetzung des neuen Datenschutzrechts zu treffen.

2 Zweck und Inhalt des Datenschutzrechts

2.1 Was ist der Sinn und Zweck des Datenschutzrechts?

Das Datenschutzrecht konkretisiert das Grundrecht auf informationelle Selbstbestimmung gemäss Art. 13 Abs. 2 BV. Mit dem Datenschutzrecht soll die Privatsphäre der Menschen geschützt werden. Das Datenschutzrecht sorgt dafür, dass dieses Grundrecht nicht nur im Verhältnis zum Staat, sondern auch unter Privaten wirksam wird (Art. 35 Abs. 3 BV).

2.2 Was regelt das Datenschutzrecht?

Das Datenschutzrecht legt die Grundsätze für die Bearbeitung von Personendaten fest. Es regelt die Pflichten derjenigen, welche die persönlichen Daten bearbeiten und verankert die Rechte der betroffenen Person. Damit diese Regeln in der Praxis auch angewendet werden, wird der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte (EDÖB) mit der Aufsicht über die bundesrechtlichen Datenschutzvorschriften beauftragt.

3 Wesentliche Neuerungen der Totalrevision des Datenschutzrechts

3.1 Warum war eine Revision des Datenschutzrechts notwendig?

Die Revision des Datenschutzrechts war notwendig, um der technologischen Entwicklung und der digitalen Transformation unserer Gesellschaft gerecht zu werden. Die neuen Bestimmungen stellen zudem die Vereinbarkeit mit dem europäischen Recht sicher und ermöglichen es, die modernisierte Datenschutzkonvention 108+ des Europarats zu ratifizieren. Diese Anpassungen im neuen Datenschutzrecht sind wichtig, damit die EU die Schweiz weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkennt und die grenzüberschreitende Datenbekanntgabe auch künftig ohne zusätzliche Anforderungen möglich bleibt. Zu nennen sind hier insb. die Umsetzung der Anforderungen der modernisierten Datenschutzkonvention 108+ des Europarates, die Umsetzung der Schengen-relevanten Richtlinie (EU) 2016/680 zum Datenschutz in Strafsachen sowie die Annäherung an die EU-Datenschutz-Grundverordnung 2016/679 (DSGVO).

3.2 Was sind die Bestrebungen der Totalrevision des Datenschutzgesetzes?

Mit der Totalrevision soll die Selbstbestimmung der betroffenen Personen über ihre persönlichen Daten gestärkt werden. Zu nennen sind insbesondere folgende Verbesserungen:

- Generelle Verbesserung der Transparenz;
- Stärkung der Aufsichtskompetenzen und der Unabhängigkeit des EDÖB;
- Verschärfung der Strafbestimmungen.

- Berücksichtigung des Datenschutzes bereits bei der Planung der Datenbearbeitung ("*privacy by design*") und durch datenschutzfreundliche Voreinstellungen ("*privacy by default*");
- Pflicht, Datenschutz-Folgenabschätzungen durchzuführen
- Das Recht auf Datenherausgabe und -übertragung
- Förderung der Datensicherheit und Meldung der Verletzungen der Datensicherheit

Die Revision soll zudem die Selbstregulierung bei den Verantwortlichen fördern. Dies erfolgt über Verhaltenskodizes, welche die Tätigkeit der Verantwortlichen erleichtern und die Einhaltung des Gesetzes verbessern sollen. Diese Kodizes werden von Berufs-, Branchen- und Wirtschaftsverbänden oder Bundesorganen erarbeitet und können dem EDÖB vorgelegt werden.

3.2.1 Wie wurde die Transparenz für die Betroffenen verbessert?

Die Menschen sollen mehr Transparenz darüber haben, wer ihre Personendaten bearbeitet und zu welchem Zweck die Bearbeitung erfolgt, damit sie ihre Rechte nach dem Datenschutzgesetz geltend machen können. Zu diesem Zweck wurde die aktive Informationspflicht der Verantwortlichen sowie das Auskunftsrecht der Betroffenen gestärkt. Neu ist auch eine Informationspflicht bei automatisierten Einzelentscheidungen (z.B. durch Algorithmen) vorgesehen.

3.2.2 Wie wurde die Unabhängigkeit und die Aufsichtskompetenz des EDÖB gestärkt?

Die Leiterin oder der Leiter des EDÖB wird neu von der Vereinigten Bundesversammlung gewählt. Ausserdem verfügt der EDÖB inskünftig über ein eigenes Budget. Damit wird seine Unabhängigkeit gestärkt. Auch die Aufsichtskompetenz des EDÖB wird gestärkt. Gemäss dem neuen Datenschutzgesetz eröffnet der EDÖB von Amtes wegen oder auf Anzeige hin eine Untersuchung, wenn genügend Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte. Kommt der EDÖB zum Schluss, dass eine Verletzung der Datenschutzvorschriften vorliegt, so kann er nicht nur eine Empfehlung, sondern neu eine anfechtbare Verfügung erlassen. Er kann zum Beispiel die Anpassung, den Unterbruch oder den Abbruch einer Datenbearbeitung oder die Löschung oder Vernichtung von Personendaten verfügen.

3.2.3 Was ändert sich bei den Strafbestimmungen des Datenschutzgesetzes?

Neben einer starken Datenschutzaufsicht sollen strengere Strafbestimmungen für eine bessere Einhaltung des Datenschutzgesetzes sorgen. Im neuen Datenschutzgesetz werden deshalb die bisherigen Straftatbestände erweitert und die bisherige Bussenobergrenze für Verstösse wird von Fr. 10'000.- auf Fr. 250'000.- erhöht. Die Verfolgung und die Beurteilung strafbarer Handlungen obliegen weiterhin den Kantonen. Allerdings kann der EDÖB bei der zuständigen Strafverfolgungsbehörde Anzeige erstatten und im Verfahren die Rechte einer Privatklägerschaft wahrnehmen.

Wie bisher erfassen die Strafbestimmungen im neuen Datenschutzgesetz in erster Linie natürliche Personen. Dies ist aber keine Besonderheit des Datenschutzrechts. Die Adressaten von Strafbestimmungen sind im schweizerischen Strafrecht primär Menschen und nicht Unternehmen. Allerdings sollen bei der Verletzung von datenschutzrechtlichen Pflichten, welche nur ein Unternehmen treffen, gerade nicht die einfachen Mitarbeitenden, sondern die Leitungspersonen strafrechtlich verantwortlich gemacht werden. Das bedeutet: Verantwortlich sind vor allem der Geschäftsherr, die Organe oder die Mitglieder eines Organs, die geschäftsführenden Gesellschafter sowie die tatsächlich leitenden Personen. Es braucht in jedem Fall eine selbstständige Entscheidungsbefugnis in einem bestimmten Unternehmensbereich.

3.2.4 Was ist die Datenschutz-Folgenabschätzung?

Wer eine Datenbearbeitung plant, die ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Personen mit sich bringen kann, muss grundsätzlich eine Datenschutz-Folgenabschätzung erstellen. Ein hohes Risiko liegt namentlich bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten (wie z.B. Gesundheitsdaten) oder bei der systematischen Überwachung umfangreicher öffentlicher Bereiche vor. In der Datenschutz-Folgenabschätzung müssen die geplante Bearbeitung beschrieben, die Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen bewertet sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte aufgezeigt werden. Ergibt sich aus der Datenschutz-Folgenabschätzung, dass bei der geplanten Bearbeitung trotz der vom Verantwortlichen vorgesehenen Massnahmen ein hohes Restrisiko für die Persönlichkeit oder die Grundrechte der betroffenen Person bleibt, so muss grundsätzlich eine Stellungnahme des EDÖB eingeholt werden.

3.2.5 Was ist eine automatisierte Einzelentscheidung und welche Rechte hat die betroffene Person dabei?

Eine automatisierte Einzelentscheidung liegt vor, wenn die Entscheidung ausschliesslich auf einer automatisierten Datenbearbeitung beruht und wenn sie für die betroffene Person mit einer Rechtsfolge verbunden ist oder sie erheblich beeinträchtigt. Bei einer automatisierten Einzelentscheidung werden also sowohl die inhaltliche Beurteilung eines Sachverhalts als auch die darauf basierende Entscheidung durch eine Maschine bzw. einen Algorithmus getroffen, ohne dass eine natürliche Person mitwirkt. Dabei muss die automatisierte Einzelentscheidung im Sinne des neuen Datenschutzgesetzes eine gewisse Komplexität aufweisen. Simple Wenn-Dann-Entscheidungen oder Ja/Nein-Abfragen objektiver Kriterien, die auf Bedingungen beruhen, welche für die betroffene Person offensichtlich sind, gehören nicht dazu (z.B. der Bezug von Geld aus einem bestehenden Guthaben am Bancomaten).

Das neue Datenschutzgesetz schreibt vor, dass die betroffene Person über eine automatisierte Einzelentscheidung informiert werden muss. Ausserdem wird der betroffenen Person das Recht eingeräumt, auf Antrag ihren Standpunkt darzulegen und zu verlangen, dass der Entscheid von einer natürlichen Person überprüft wird. Schliesslich müssen der betroffenen Person im Rahmen ihres Auskunftsrechts Angaben über das Vorliegen einer automatisierten Einzelentscheidung sowie zur Logik, auf der die Entscheidung beruht, gemacht werden.

3.2.6 Was ist unter «Profiling» zu verstehen und inwiefern geniesst die betroffene Person hierbei einen erhöhten Schutz?

«Profiling» bezeichnet jede Art der automatisierten Bearbeitung von Personendaten, mit welcher bestimmte persönliche Aspekte einer natürlichen Person bewertet werden, indem z.B. Aspekte bezüglich Arbeitsleistung, wirtschaftlicher Lage, Gesundheit, persönlicher Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person analysiert oder vorhersagt werden. Vereinfacht gesagt, geht es beim Profiling um eine Art Einschätzung oder Beurteilung einer Person. Dabei kann es sich um die Analyse von Persönlichkeitsmerkmalen, aber auch um eine Prognose über zukünftige Verhaltensweisen oder Eigenschaften einer Person handeln. Anders als beim Begriff der automatisierten Einzelentscheidung (siehe Frage 3.2.5) muss die Datenbearbeitung beim Profiling nicht vollständig automatisiert sein. Das Eingreifen eines Menschen schliesst eine Aktivität nicht von der Profiling-Definition aus, solange die Datenbearbeitung im Wesentlichen automatisiert abläuft.

Als «Profiling mit hohem Risiko» gilt ein Profiling, das ein hohes Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringt, indem es zu einer Verknüpfung

von Daten führt, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt. Mit anderen Worten liegt ein Profiling mit hohem Risiko dann vor, wenn das Profiling ein Persönlichkeitsprofil nach geltendem Datenschutzgesetz zum Ergebnis hat. Dabei besteht die Gefahr, dass eine Vielzahl (auch nicht besonders schützenswerter) Daten durch ein Profiling zu einem Bild über die betroffene Person verknüpft werden, das als solches ein erhöhtes Risiko für die Persönlichkeits- und Grundrechte mit sich bringt. Die betroffene Person hat häufig keinen Einfluss auf dieses Bild und kann weder dessen Richtigkeit noch Verwendung kontrollieren.

Für private Datenbearbeiter gelten bei der Durchführung eines Profilings mit hohem Risiko strengere Rechtsfolgen (z.B. höhere Anforderungen an die Einwilligung). Für Bundesorgane kommen strengere Rechtsfolgen schon bei einem «gewöhnlichen» Profiling zum Zug. Insbesondere sind sie grundsätzlich nur dann zu einem Profiling befugt, wenn dies in einer formell-gesetzlichen Grundlage vorgesehen ist.

3.2.7 Wozu berechtigt das Recht auf Datenherausgabe und Datenübertragung?

Jede Person kann vom Verantwortlichen unter bestimmten Voraussetzungen die Herausgabe der Personendaten, die sie ihm bekanntgegeben hat, in einem gängigen elektronischen Format verlangen. Sie kann zudem vom Verantwortlichen verlangen, dass er ihre Personendaten einem anderen Verantwortlichen überträgt, wenn dies keinen unverhältnismässigen Aufwand erfordert. Dies wird auch als Recht auf Datenportabilität bezeichnet. Damit wird gleichzeitig die Stellung der betroffenen Person als selbstbestimmte Konsumentin von digitalen Dienstleistungen gestärkt und der freie Wettbewerb unter den unterschiedlichen Anbietern gefördert.

4 Internationale Entwicklungen des Datenschutzes

4.1 Welche Bedeutung hat die EU-Richtlinie 2016/680 für die Schweiz?

Die EU-Richtlinie 2016/680 stellt eine Weiterentwicklung des Schengen-Besitzstands dar, welche die Schweiz aufgrund des Schengen-Assoziierungsabkommens übernehmen musste. Sie hat einen spezifischen Geltungsbereich und regelt Datenbearbeitungen durch Behörden zum Zweck der Strafverfolgung, Strafvollstreckung und der Abwehr von Gefahren für die öffentliche Sicherheit.

4.2 Welche Bedeutung hat die Datenschutz-Grundverordnung der EU für die Schweiz?

Die Datenschutz-Grundverordnung regelt allgemein den Schutz von Daten, die von privaten Personen oder Behörden der EU-Mitgliedstaaten bearbeitet werden. Anders als die EU-Richtlinie 2016/680 zum Datenschutz in Strafsachen ist die EU-Datenschutz-Grundverordnung keine Weiterentwicklung des Schengen-Besitzstandes und ist für die Schweiz nicht direkt verbindlich. Allerdings gilt die EU-Datenschutz-Grundverordnung auch für Unternehmen in der Schweiz, wenn sie Personen in der EU Waren oder Dienstleistungen anbieten oder wenn sie das Verhalten von Personen in der EU beobachten. Zudem ist es für die Schweiz wichtig, dass sie von der EU auch unter der Datenschutz-Grundverordnung weiterhin als Drittstaat mit einem angemessenen Datenschutzniveau anerkannt wird.

4.3 Erfüllt das schweizerische Datenschutzrecht die europäischen Standards?

Die Schweiz verfügt bereits seit dem Jahre 2000 über einen Angemessenheitsbeschluss der EU, der ein gleichwertiges Datenschutzniveau anerkennt. Die Angemessenheit gegenüber den europäischen Datenschutzvorschriften wird regelmässig überprüft. Das neue Recht ermöglicht eine Annäherung des Schweizer Schutzniveaus an den EU-Standard.

4.4 Was sind die Folgen, wenn die EU-Kommission das Datenschutzniveau der Schweiz nicht als angemessen anerkennt?

Fehlt ein Angemessenheitsbeschluss vonseiten der EU, so sind Datenübermittlungen in die Schweiz nur möglich, sofern geeignete Garantien vorgesehen sind oder bestimmte Ausnahmetatbestände vorliegen. Dies führt zu hohen administrativen Hürden, die den freien Datenfluss und die damit einhergehende Innovation hemmen und somit nachteilige Konsequenzen für den Schweizer Wirtschaftsstandort haben.

4.5 Wo steht die Schweiz mit der Ratifikation der modernisierten Datenschutz-Konvention 108+ des Europarates?

Die Schweiz wird das Änderungsprotokoll mit dem Inkrafttreten des revidierten DSG ratifizieren. Die modernisierte Datenschutz-Konvention 108+, wird am 11. Oktober 2023 in Kraft treten, sofern bis zu diesem Zeitpunkt mindestens 38 Vertragsstaaten dem Protokoll angehören.

4.6 Warum soll die Schweiz der modernisierten Datenschutz-Konvention 108+ des Europarates beitreten?

Bis heute haben rund 50 Staaten die Datenschutz-Konvention 108 des Europarats ratifiziert, darunter auch die Schweiz. Es ist das erste verbindliche völkerrechtliche Instrument im Bereich des Datenschutzes und datiert aus dem Jahr 1981. Der Europarat hat nun auch diese Konvention dem digitalen Zeitalter angepasst. Mit der Ratifizierung der revidierten Konvention kann die Schweiz gegenüber ihren internationalen Vertragspartnern ein gutes Datenschutzniveau behalten und stärkt damit den Wirtschaftsstandort Schweiz. Mit der Totalrevision des Datenschutzgesetzes DSG sollen die Anforderungen der neuen Konvention 108 erfüllt werden. Inhaltlich sind sie den neuen EU-Datenschutzbestimmungen und den Bestrebungen der Schweiz sehr ähnlich.