Stand: Dezember 2017

Die EU-Datenschutzgrundverordnung und ihre Auswirkungen auf die Schweiz[1]

Inhalt

[1] *Achtung: Dieser Text wird mit Blick auf die Entwicklungen auf nationaler und europäischer Ebene ergänzt und geändert. Zurzeit laufen Abklärungen, um die Position und die Auslegung der zuständigen Behörden und Aufsichtsbehörden zu ermitteln (G29, Europäische Kommission, Aufsichtsbehörden der Mitgliedstaaten der Union).*

Einleitung

Im Januar 2012 schlug die Europäische Kommission eine Reihe legislativer Massnahmen vor zur Aktualisierung und Modernisierung der Datenschutzrichtlinie von 1995 (Richtlinie 95/46/EG) und des Rahmenbeschlusses von 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (Rahmenbeschluss 2008/977/JI). Ziel dieser Reform ist es, EU-weit einheitliche, an das digitale Zeitalter angepasste Regeln zu schaffen, die Rechtssicherheit zu verbessern und das Vertrauen der Bürgerinnen und Bürger und Unternehmen in den digitalen Binnenmarkt zu stärken. Die Reform umfasst eine Mitteilung der Kommission, die deren Ziele darlegt, sowie zwei Rechtsakte: eine Datenschutz-Grundverordnung (DSGVO) über den Datenschutz und eine Richtlinie für den Bereich Polizei und Justiz.

Am 14. April 2016 schloss das Europäische Parlament seine mehr als vierjährige Arbeit mit der Annahme der vorgeschlagenen Texte ab. Die sich aus der Datenschutz-Grundverordnung ergebenden Vorschriften werden ab dem 25. Mai 2018 in allen Mitgliedstaaten unmittelbar anwendbar sein. Die EU-Länder haben bis zum 6. Mai 2018 Zeit, die Richtlinie in ihrem nationalen Recht umzusetzen.

Die Datenschutz-Grundverordnung (DSGVO)

Die 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 oder DSGVO) wurde vom Europäischen Parlament am 14. April 2016 angenommen und tritt am **25. Mai 2018** in Kraft. Ab diesem Zeitpunkt ist die DSGVO für alle Akteure, die auf dem Gebiet der Europäischen Union tätig sind, unmittelbar anwendbar. Nach EU-Recht ist eine Verordnung in ihrer Gesamtheit verbindlich, sobald sie in Kraft tritt (sie kann nicht selektiv angewendet werden). Sie ist in der gesamten EU unmittelbar anwendbar, ohne dass eine Umsetzung in den einzelnen Mitgliedstaaten erforderlich ist – dies im Gegensatz zur Richtlinie. Die neuen Bestimmungen sehen unter anderem vor, dass die Bürgerinnen und Bürger mehr Kontrolle über ihre Personendaten haben, dass die Unternehmen stärker zur Verantwortung gezogen werden, dass gleichzeitig deren Meldepflichten abgebaut werden und dass die Rolle der Datenschutzbehörden gestärkt wird. **Dieses für Europa grundlegende Dokument wird auf eine Vielzahl von Schweizer Unternehmen direkte Auswirkungen haben**.

Sachlicher Anwendungsbereich (Art. 2 DSGVO)

Gegenüber der Richtlinie 95/46/EG hat sich der sachliche Anwendungsbereich grundsätzlich nicht verändert. Die DSGVO *„gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen“* (Art. 2 § 1 DSGVO). Sie betrifft alle personenbezogenen Daten, die sich auf identifizierte oder identifizierbare natürliche Personen beziehen, und unterscheidet nicht zwischen der Bearbeitung durch eine natürliche oder eine juristische Person des öffentlichen oder privaten Rechts. Artikel 2 § 2 DSGVO sieht vier Ausnahmen vor. Die DSGVO *„findet keine Anwendung auf die Verarbeitung personenbezogener Daten:*

a) *im Rahmen einer Tätigkeit, die nicht in den Anwendungsbereich des Unionsrechts fällt,*
b) *durch die Mitgliedstaaten im Rahmen von Tätigkeiten, die in den Anwendungsbereich von Titel V Kapitel 2 EUV fallen,*
c) *durch natürliche Personen zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten,*

d) *durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit.“*

Räumlicher Anwendungsbereich (Art. 3 DSGVO)

Gegenüber der Richtlinie 95/46/EG wurde der Anwendungsbereich erweitert. Er umfasst nun das **Kriterium der Zielgruppe (extraterritoriale Anwendung)**. Diese Erweiterung steht auch im Einklang mit der Rechtsprechung des Europäischen Gerichtshofs (EuGH), der sich 2014 im Fall von Google Spanien für die extraterritoriale Anwendung der Richtlinie ausgesprochen hat (C-131-12).

Artikel 3 DSGVO regelt Folgendes:

> *(1) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten, soweit diese im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, unabhängig davon, ob die Verarbeitung in der Union stattfindet.*
>
> *(2) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht*
>
> *a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;*
>
> *b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.*
>
> *(3) Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten durch einen nicht in der Union niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedstaats unterliegt.*

Die Anwendung der DSGVO hängt daher von den beiden folgenden Kriterien ab:

1. **dem Kriterium der Niederlassung** (= Ort der Niederlassung des Verantwortlichen oder Auftragsbearbeiters; Artikel 3 § 1): Der Verantwortliche oder Auftragsbearbeiter hat seine Niederlassung **in der Europäischen Union.** In diesem Fall findet die Verordnung automatisch Anwendung, unabhängig davon, ob die Bearbeitung in der Union stattfindet oder nicht. In der Causa Weltimmo v. NAIH (C-230/14) hat der EuGH den Begriff der Niederlassung relativ breit und flexibel ausgelegt.

2. **dem Kriterium des Zielmarktes** (= Wohnort der von Datenbearbeitung betroffenen Person; Art. 3 § 2): Die Niederlassung des Verantwortlichen befindet sich **ausserhalb der Europäischen Union,** aber die Bearbeitung betrifft Waren oder Dienstleistungen, die für Personen in der Union bestimmt sind, oder die Bearbeitung betrifft die Beobachtung des Verhaltens einer betroffenen Person, soweit deren Verhalten in der Union erfolgt. Bei Letzterem bezieht sich der europäische Gesetzgeber vor allem auf die Beobachtung des Verhaltens von Internetnutzerinnen und -nutzern. **In der Praxis findet die DSGVO wohl dann Anwendung, wenn eine in einem Mitgliedstaat der EU niedergelassene Person, unabhängig von ihrer Staatsangehörigkeit, direkt von einer Datenbearbeitung betroffen ist.**

Bei der Beurteilung, ob die Verordnung zur Anwendung kommt, ist stets der Einzelfall und insbesondere die Absicht des Verantwortlichen zu berücksichtigen, Personen im Gebiet der Union Waren oder Dienstleistungen anzubieten oder ihr Verhalten zu beobachten.

Rechte der betroffenen Personen

Eines der Ziele der europäischen Reform besteht darin, die **Kontrollmöglichkeiten betroffener Personen und die Erkennbarkeit** zu erhöhen. Artikel 12 DSGVO verpflichtet den Verantwortlichen, Verfahren und Mechanismen vorzusehen, die es den betroffenen Personen ermöglichen, ihre Rechte auszuüben. In dieser Bestimmung ist der Grundsatz der Transparenz wie folgt verankert: Jede Information, die sich an die Öffentlichkeit oder an betroffene Personen richtet, muss einfach zugänglich und leicht verständlich sein. Sie muss prägnant und transparent sein sowie einfach und klar formuliert, insbesondere in Bezug auf Kinder. In der Regel werden Informationen schriftlich und unentgeltlich zur Verfügung gestellt. Die Verordnung regelt auch die damit zusammenhängenden Fristen. Alle in Artikel 12 aufgeführten Modalitäten gelten für alle in der Verordnung aufgeführten Rechte, nämlich:

- **Recht auf Information** (Art. 13 und 14 DSGVO)
  Werden personenbezogene Daten über eine betroffene Person bei dieser selbst erhoben, so liefert der Verantwortliche ihr zum Zeitpunkt der Erhebung der Daten eine Reihe von Informationen. Der Verantwortliche muss die betroffene Person aber auch dann informieren, wenn die Daten nicht bei dieser selbst erhoben wurden.

- **Auskunftsrecht** (Art. 15 DSGVO)
  Die betroffene Person hat das Recht, vom Verantwortlichen eine Bestätigung zu verlangen, dass personenbezogene Daten über sie bearbeitet werden bzw. dass keine Daten bearbeitet werden. Im Fall einer Bearbeitung hat sie das Recht, Zugang zu diesen Daten und zu einer Reihe zusätzlicher Informationen nach den Buchstaben a–h zu erhalten. Dieses Recht umfasst auch das Recht, eine Kopie der bearbeiteten Daten zu erhalten.

- **Recht auf Berichtigung** (Art. 16 DSGVO)
  Die betroffene Person hat das Recht zu verlangen, dass ihre Daten so rasch wie möglich berichtigt oder ergänzt werden.

- **Recht auf Löschung („Recht auf Vergessenwerden“)** (Art. 17 DSGVO)
  Die betroffene Person hat das Recht zu verlangen, dass sie betreffende Daten so schnell wie möglich gelöscht werden, wenn einer der in § 1 genannten Gründe vorliegt. Wurden die Daten an andere Stellen übermittelt, so kommt das „Recht auf Vergessenwerden“ zum Tragen: Der Verantwortliche muss alle angemessenen Massnahmen treffen, um die anderen Stellen davon in Kenntnis zu setzen, dass die betroffene Person die Löschung aller Verbindungen zu ihren persönlichen Daten beziehungsweise die Löschung aller Kopien oder Reproduktionen dieser Daten verlangt hat.

- **Recht auf Einschränkung der Bearbeitung** (Art. 18 DSGVO)
  Die betroffene Person hat in bestimmten gesetzlich vorgesehenen Fällen das Recht, vom Verantwortlichen die Einschränkung der Bearbeitung ihrer Daten zu verlangen. Wird eine solche Einschränkung verlangt, so kann der Verantwortliche die Daten nur noch aufbewahren. Andere Bearbeitungen dieser Daten dürfen grundsätzlich nicht mehr erfolgen.

- **Recht auf Mitteilung** (Art. 19 DSGVO)
  Dieser Artikel verpflichtet den Verantwortlichen, der betroffenen Person jede Berichtigung, Löschung oder Einschränkung der Datenbearbeitung mitzuteilen.

- **Recht auf Datenübertragbarkeit** (Art. 20 DSGVO)
  Die betroffene Person hat das Recht, die Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten, und sie hat das Recht, diese Daten einem anderen Verantwortlichen zu übermitteln, beispielsweise um den Dienstleistungsanbieter zu wechseln. Dieses Recht kann nur ausgeübt werden, wenn die Datenbearbeitung auf der Einwilligung der betroffenen Person oder auf einem Vertrag beruht.

- **Widerspruchsrecht** (Art. 21 DSGVO)
  Die betroffene Person hat jederzeit das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, der Bearbeitung von sie betreffenden personenbezogenen Daten gestützt auf ein öffentliches oder berechtigtes Interesse zu widersprechen; dies gilt auch für ein auf diese Bestimmung gestütztes Profiling. Die betroffene Person hat auch jederzeit das Recht, der Bearbeitung ihrer Daten zu Direktmarketing-Zwecken zu widersprechen.

- **Recht auf Verzicht auf eine automatisierte Entscheidung im Einzelfall** (Art. 22 DSGVO)
  Die betroffene Person hat das Recht, nicht einer Entscheidung unterworfen zu werden, die ausschliesslich auf einer automatischen Bearbeitung beruht, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt. Dies gilt ausdrücklich auch für Profiling.

- **Recht auf Benachrichtigung über Datenschutzverletzungen** (Art. 34 DSGVO)
  Der Verantwortliche ist verpflichtet, die betroffene Person über Verletzungen des Schutzes personenbezogener Daten zu informieren, sofern damit ein hohes Risiko für die persönlichen Rechte und Freiheiten verbunden ist.

Die Verordnung sieht auch einen besonderen Schutz für Kinder vor, da diese sich der Risiken, Folgen und Rechte im Bereich des Datenschutzes weniger bewusst sind. Artikel 8 DSGVO sieht vor, dass im Fall von Diensten der Informationsgesellschaft, die einem Kind direkt angeboten werden, die Zustimmung zur Bearbeitung der Daten des Kindes vom Träger der elterlichen Verantwortung erteilt oder genehmigt werden muss (die Mitgliedstaaten können die Altersgrenze zwischen 13 und 16 Jahren frei festlegen).

Anwendbarkeit auf Schweizer Unternehmen (Art. 3 und 27 DSGVO)

Aus dem Wortlaut der Verordnung und den Erwägungen geht hervor, dass die DSGVO in den folgenden Fällen auf Schweizer Unternehmen anwendbar ist:

Niederlassung in der EU (Artikel 3 § 1; Erwägung 22):

- Bearbeitung personenbezogener Daten im Zusammenhang mit der Tätigkeit **einer europäischen Zweigstelle eines schweizerischen Unternehmens** in der Europäischen Union;

- **Auftragsbearbeiter:**

  - Bearbeitung personenbezogener Daten für ein Schweizer Unternehmen durch einen Auftragsbearbeiter im EU-Gebiet, unabhängig davon, ob er Daten von betroffenen Personen in der Schweiz oder in der EU bearbeitet;
  - Bearbeitung personenbezogener Daten in der EU durch ein Schweizer Unternehmen im Auftrag eines europäischen Unternehmens;
  - Bearbeitung personenbezogener Daten durch ein Schweizer Unternehmen als Auftragsbearbeiter im Auftrag eines europäischen Unternehmens.

Zielgruppe in der EU (Artikel 3 § 2; Erwägungen 23 und 24):

- Bearbeitung personenbezogener Daten von Personen mit Aufenthalt in der EU durch ein Unternehmen mit Sitz in der Schweiz, soweit es diese Daten für seine **Waren- und Dienstleistungsangebote** in der EU bearbeitet, unabhängig davon, ob eine Zahlung erforderlich ist oder nicht (Art. 3 § 2 Buchstabe a) DSGVO);

> Beispiel 1: Ein in der Schweiz ansässiges Unternehmen verkauft Uhren über einen Online-Shop an Personen mit Wohnsitz in Frankreich, Belgien, Portugal, Finnland und Griechenland. Die DSGVO ist anwendbar, weil das Schweizer Unternehmen seine Waren Personen in der EU anbietet.

Die DSGVO enthält keine genaue Definition des Begriffs Waren- und Dienstleistungsangebot. In der Erwägung 23 heisst es, es müsse festgestellt werden, *„ob der Verantwortliche oder Auftragsverarbeiter offensichtlich beabsichtigt, betroffenen Personen in einem oder mehreren Mitgliedstaaten der Union Dienstleistungen anzubieten.“* Um dies festzustellen, ist es notwendig, eine Reihe von Hinweisen zu berücksichtigen, wie zum Beispiel *„die Verwendung einer Sprache oder Währung, die in einem oder mehreren Mitgliedstaaten gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren und Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von Kunden oder Nutzern, die sich in der Union befinden.“*
In einem speziellen Zusammenhang (siehe verbundene Rechtssachen C-585/08 und C-144/09) hat der EuGH bereits geprüft, ob das Angebot von Waren und Dienstleistungen als an den Mitgliedstaat der Union gerichtet angesehen werden kann. In diesem Zusammenhang hat er auch folgende Faktoren berücksichtigt: die Angabe einer Telefonnummer mit internationaler Vorwahl, die Wegbeschreibung aus einem Mitgliedstaat zu dem Ort, wo der Dienst angeboten wird (z. B. Beschreibung der Anreise aus dem Ausland zu einem Hotel in der Schweiz), die Erwähnung auf der Website einer internationalen Kundschaft mit Sitz in verschiedenen EU-

Mitgliedstaaten, die Nutzung einer anderen First-Level-Domain als derjenigen des Mitgliedstaats, in dem der Dienst angeboten wird (z. B. www.beispiel.ch ist auch unter www.beispiel.fr und www.beispiel.eu abrufbar).

„Die blosse Zugänglichkeit der Website des Verantwortlichen, des Auftragsverarbeiters oder eines Vermittlers in der Union, einer E-Mail-Adresse oder anderer Kontaktdaten oder die Verwendung einer Sprache, die in dem Drittland, in dem der Verantwortliche niedergelassen ist, allgemein gebräuchlich ist, [ist] hierfür [aber] kein ausreichender Anhaltspunkt."

Die Auflistung dieser Faktoren ist allerdings nicht abschliessend und die Frage muss immer von Fall zu Fall analysiert werden.

- Bearbeitung personenbezogener Daten von Personen mit Wohnsitz in der EU durch ein in der Schweiz ansässiges Unternehmen, soweit diese Daten zum Zweck der **Beobachtung des Verhaltens** der betroffenen Personen innerhalb der Union bearbeitet werden (Art. 3 § 2 Bst. b DSGVO).

  In Bezug auf die Beobachtung des Verhaltens und die Bestimmung, ob eine Bearbeitung als solche gilt, hält die Erwägung 24 fest: *„Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von betroffenen Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, einschließlich der möglichen nachfolgenden Verwendung von Techniken zur Verarbeitung personenbezogener Daten, durch die ein Profil von einer natürlichen Person erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen."*

  Es geht insbesondere um verhaltensbasierte Werbung, wie sie die Artikel-29-Datenschutzgruppe in ihrer Stellungnahme 2/2010 zur Werbung auf Basis von Behavioural Targeting definiert wird: *„Werbung, die auf der Beobachtung des Verhaltens von Personen über einen Zeitraum hinweg basiert. Werbung auf Basis von Behavioural Targeting versucht, die Charakteristika dieses Verhaltens durch die Handlungen (wiederholte Besuche von Websites, Interaktionen, Schlüsselwörter, Produktion von Online-Inhalten usw.) zu untersuchen, um ein konkretes Profil zu erstellen und den betroffenen Personen dann Werbung zu senden, die auf ihre aus den Daten erschlossenen Interessen zugeschnitten ist."*

Beispiel 2: Ein Hotelier im Engadin erstellt von seinen italienischen, schwedischen, deutschen und polnischen Gästen Profile, um ihnen Angebote für andere Aufenthalte machen zu können. Die DSGVO ist anwendbar, soweit das Profil auf der Grundlage eines Verhaltens in der EU erstellt wird.

Beispiel 3: Der Betreiber einer Website setzt Webtracking ein, um die Besucherbewegungen auf einer Website oder das Surfverhalten von Internetnutzern zu und Rückschlüsse auf deren Interessen, Vorlieben oder Gewohnheiten zu erhalten. Die DSGVO ist wahrscheinlich anwendbar.

Pflichten der unter die Verordnung fallenden Unternehmen

Eine der wichtigsten Neuerungen gegenüber der Richtlinie 95/46/EG ist die Verankerung des Grundsatzes der **Rechenschaftspflicht** („accountability") des Verantwortlichen (vgl. Art. 5 § 2 DSGVO), wonach dieser die Einhaltung der allgemeinen Grundsätze (vgl. Art. 5 § 1 DSGVO) aktiv nachweisen können muss. Auf dieser Grundlage wurde das Prinzip der **Beweislastumkehr** eingeführt[2]. Die Verordnung sieht insbesondere die folgenden Pflichten vor:

- Artikel 24 DSGVO hält fest, dass der Grundsatz der Verantwortlichkeit mit dem risikobasierten Ansatz einhergeht, wonach der Verantwortliche die Wahrscheinlichkeit und den Grad der Gefährdung der Rechte und Freiheiten von Personen zu Beginn einer Bearbeitung objektiv beurteilen muss. Der Verantwortliche muss daher Kontrollmechanismen und -systeme innerhalb seiner Einrichtung etablieren, um sicherzustellen, dass die Konformität der Bearbeitung während des gesamten Vorgangs gewährleistet ist, und um dies nachweisen zu können.

- Artikel 25 DSGVO verlangt, dass der Datenschutz bei Produkten und Dienstleistungen bereits in der Planungsphase berücksichtigt werden: Die Grundsätze des Datenschutzes müssen schon bei der technischen Ausgestaltung berücksichtigt werden („privacy by design"); Produkte und Dienstleistungen müssen mit datenschutzfreundlichen Voreinstellungen angeboten werden („privacy by default").

- Artikel 30 DSGVO sieht vor, dass jeder Verantwortliche oder sein Vertreter ein **Register** der unter seiner Verantwortung ausgeführten Bearbeitungstätigkeiten (in elektronischer Form) führen muss. Der Inhalt des Registers ist in Artikel 30 § 1 DSGVO detailliert beschrieben. Dieses Register muss der Aufsichtsbehörde auf Anfrage zur Verfügung gestellt werden. Unternehmen mit weniger als 250 Beschäftigten sind – mit einigen Ausnahmen – von dieser Pflicht ausgenommen (vgl. Art. 30 § 5 DSGVO).

- Artikel 35 DSGVO sieht die Durchführung einer **Datenschutz-Folgenabschätzung** vor, wenn die Bearbeitung ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen zur Folge haben kann.[3] In den Fällen, in denen diese Voranalyse zur Identifizierung spezifischer Risiken führt, ist der Verantwortliche verpflichtet, vor der Bearbeitung die Datenschutzbehörde zu konsultieren; ist ein Datenschutzverantwortlicher ernannt worden, so ist dieser zu konsultieren. In bestimmten Fällen ist eine Datenschutz-Folgenabschätzung obligatorisch (vgl. Artikel 35 § 3). Die inhaltlichen Mindestanforderungen sind in Artikel 35 § 7 aufgeführt.

Die **Sicherheit der Bearbeitungsvorgänge** ist in der Verordnung als Grundprinzip verankert:

- Artikel 32 DSGVO verpflichtet den Verantwortlichen, angemessene organisatorische und technische Massnahmen zu treffen, um ein dem Risiko angemessenes Schutzniveau zu

[2] Das Bayrische Landesdatenschutzamt hat ein Selbsteinschätzungstool für Unternehmen veröffentlicht: https://www.lda.bayern.de/tool/start.html

[3] Um die für die Bearbeitung Verantwortlichen bei der Durchführung von Datenschutz-Folgenabschätzungen zu unterstützen, stellt die Commission Nationale de l'Informatique et des Libertés (CNIL) auf ihrer Website kostenlos die Software PIA zur Verfügung: https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil

gewährleisten. Dabei muss er den Stand der Technik, die Implementierungskosten, die Art, den Umfang, die Umstände und den Zweck der Bearbeitung sowie die Risiken für die Rechte und Freiheiten natürlicher Personen berücksichtigen. Die Verordnung nennt beispielsweise die Verschlüsselung oder Pseudonymisierung und Mittel zur dauerhaften Gewährleistung der Vertraulichkeit, der Integrität, der Verfügbarkeit und der Belastbarkeit der Systeme. Darüber hinaus muss der Verantwortliche Massnahmen treffen, *„um sicherzustellen, dass [dem Verantwortlichen und dem Auftragsbearbeiter] unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet"* (vgl. Art. 32 § 4).

Daraus leitet sich neu die **Pflicht ab, der Aufsichtsbehörde Verletzungen des Schutzes personenbezogener Daten zu melden**. In einigen Fällen muss die Verletzung auch der betroffenen Person gemeldet werden:

- Artikel 33 DSGVO sieht ein Meldesystem bei Verletzungen des Schutzes personenbezogener Daten vor („data breaches"). Die Verletzung wird definiert als *„Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden"* (Art. 4 § 12 DSGVO). Könnte die Verletzung Risiken für die Rechte und Freiheiten natürlicher Personen zur Folge haben, muss der Verantwortliche dies der Aufsichtsbehörde unverzüglich bzw. möglichst innerhalb von 72 Stunden melden (Art. 33 § 1). Der Auftragsbearbeiter muss den Verantwortlichen über jede Verletzung unverzüglich informieren, sobald er davon Kenntnis hat. Der Inhalt der Meldung ist in Artikel 33 § 3 DSGVO geregelt. Schliesslich muss der Verantwortliche jede Verletzung des Schutzes personenbezogener Daten dokumentieren, einschliesslich aller mit der Verletzung zusammenhängenden Fakten, der Auswirkungen und der ergriffenen Abhilfemassnahmen. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der Bestimmungen nach diesem Artikel ermöglichen.

- Artikel 34 DSGVO regelt die Modalitäten der Mitteilung einer Verletzung des Datenschutzes an die betroffenen Personen. Hier gibt es jedoch keine Fristen. Die Idee dahinter besteht darin, es den betroffenen Personen zu ermöglichen, gegebenenfalls geeignete Massnahmen zu ergreifen, um die negativen Auswirkungen, die sich aus der Verletzung ergeben können, zu stoppen oder abzuschwächen.

In drei bestimmten Fällen (vgl. Art. 37 DSGVO) ist die Benennung eines Datenschutzbeauftragten zwingend, und zwar 1) für Behörden oder öffentliche Stellen, 2) für Unternehmen, die Bearbeitungen durchführen, die eine umfangreiche regelmässige und systematische Überwachung der betroffenen Personen erfordern, 3) für Unternehmen, die sensible Datenbearbeitungsvorgänge durchführen.[4] Darüber hinaus erlaubt es die Verordnung, im Unionsrecht oder im Recht eines Mitgliedstaats die Benennung eines Datenschutzbeauftragten in Fällen vorzuschreiben, die in der DSGVO nicht vorgesehen sind. Eine Unternehmensgruppe kann auch einen einzigen Beauftragten benennen; diese Möglichkeit besteht auch für Behörden und öffentliche Stellen unter Berücksichtigung ihrer

[4] Vgl. Schema „dois-je désigner un dpd"

Organisationsstruktur und ihrer Grösse (Art. 37 § 2 und 3). Die Eigenschaften, über die der behördliche Datenschutzbeauftragte verfügen muss, sind in Artikel 37 § 5 festgelegt.

Schliesslich fördert die Verordnung die Ausarbeitung von **Verhaltensregeln** (Art. 40 und 41 DSGVO), um die ordnungsgemässe Umsetzung der Verordnung zu unterstützen. Die Verhaltensregeln müssen entsprechend den Besonderheiten der verschiedenen Datenbearbeitungssektoren und den spezifischen Bedürfnissen der Unternehmen entwickelt werden. Die Verhaltensregeln werden der nach Artikel 55 DSGVO zuständigen Datenschutzbehörde vorgelegt; diese gibt eine Stellungnahme zur Konformität mit der Verordnung ab. Mit den Artikeln 42 ff. wird ein Zertifizierungsmechanismus eingeführt, der die Verantwortlichen und Auftragsbearbeiter bei der Einhaltung der Vorschriften unterstützt.

Pflicht der Verantwortlichen oder Auftragsbearbeiter, die nicht in der Union niedergelassen sind, einen Vertreter zu benennen (Art. 27 DSGVO)

Kommt Artikel 3 § 2 DSGVO zur Anwendung, so verpflichtet Artikel 27 DSGVO den Verantwortlichen und den Auftragsbearbeiter, die nicht in der Union niedergelassen sind, schriftlich einen Vertreter zu benennen, sofern die Verordnung für ihre Bearbeitungstätigkeiten gilt. Dieser Vertreter muss in einem der Mitgliedstaaten ansässig sein, in dem die natürlichen Personen ihren Wohnsitz haben, deren personenbezogene Daten im Zusammenhang mit einem Waren- oder Dienstleistungsangebot bearbeitet werden oder deren Verhalten beobachtet wird (Art. 27 § 3).

Gemäss der Erwägung 80 DSGVO ist der Vertreter insbesondere die Kontaktstelle für die Aufsichtsbehörden (vgl. Art. 58 DSGVO) und die betroffenen Personen, und zwar in allen Fragen der Bearbeitung personenbezogener Daten. Der Vertreter muss ein **Register** aller Kategorien von Tätigkeiten zur Bearbeitung personenbezogener Daten erstellen, die unter seiner Verantwortung durchgeführt werden (vgl. Art. 30 DSGVO). Er kann auch Durchsetzungsverfahren unterworfen werden, wenn der Verantwortliche oder der Auftragsbearbeiter gegen die Verordnung verstösst. Es muss aber betont werden, dass dies die Verantwortung des Verantwortlichen oder des Auftragsbearbeiters gegenüber den Behörden und den betroffenen Personen in keiner Weise beeinflusst, da die Benennung unabhängig von Gerichtsverfahren erfolgt, die gegen den Verantwortlichen oder den Auftragsbearbeiter eingeleitet werden könnten.

Artikel 27 § 2 bestimmt, dass diese Benennung nicht gilt für:

a) *„eine Verarbeitung, die gelegentlich erfolgt, nicht die umfangreiche Verarbeitung besonderer Datenkategorien im Sinne des Artikels 9 Absatz 1 oder die umfangreiche Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10 einschließt und unter Berücksichtigung der Art, der Umstände, des Umfangs und der Zwecke der Verarbeitung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, oder*

b) *Behörden oder öffentliche Stellen.“*

Sanktionen

Die DSGVO gesteht im Gegensatz zum schweizerischen Recht den Aufsichtsbehörden zu, selbst **Geldbussen** zu verhängen, wenn eine Reihe von Voraussetzungen erfüllt ist. Jede Aufsichtsbehörde muss sicherstellen, dass die für Verstösse gegen die DSGVO verhängten Sanktionen **wirksam, verhältnismässig und abschreckend** sind. Auch sieht die Verordnung eine ganze Reihe von abschreckenden Massnahmen (vgl. Art. 58 § 2 RGPD) vor, z. B. Mahnungen, Verwarnungen, förmliche Bekanntmachungen, vorübergehende oder dauerhafte Beschränkungen der Bearbeitung. Unter all diesen Instrumenten müssen die Datenschutzbehörden dasjenige auswählen, das dem Ziel der Einhaltung der Vorschriften am besten gerecht wird.

Als letztes Mittel können Verantwortliche mit Geldbussen von bis zu 20 Millionen Euro oder 4 Prozent ihres weltweiten Jahresumsatzes belegt werden. Artikel 83 DSGVO listet die Bedingungen auf, die bei der Bestimmung der Höhe der Strafe zu berücksichtigen sind.

Dabei ist jedoch zu beachten, dass gegebenenfalls auch der aus einem Gerichtsverfahren resultierende Schadenersatz sowie Zinsen zu zahlen sind.

Kontaktstellen

Insofern es sich bei der Verordnung um einen europäischen Rechtsakt handelt, raten wir Ihnen, Ihre Fragen bezüglich der Anwendung an eine europäische Datenschutzbehörde wie die deutsche Bundesbeauftragte für den Datenschutz und die Informationsfreiheit, die Datenschutzbehörde Österreichs oder die liechtensteinische Datenschutzstelle zu richten. Wir empfehlen Ihnen auch, deren Websites zu konsultieren, die praktische Leitfäden, thematische Broschüren und praktische Compliance-Tools enthalten.