INFORMATIONSBLATT DATENSCHUTZ

EU DATENSCHUTZ – GRUNDVERORDNUNG Nr. 679/2016

Die Datenschutz-Grundverordnung (in der Folge „**EU-Verordnung**“) tritt am 25. Mai 2018 in allen EU-Mitgliedstaaten unmittelbar in Geltung. Bis dahin müssen alle Datenanwendungen an die neue Rechtslage angepasst werden.

Inhaltsverzeichnis

Eingeschränkte Meldepflicht – stärkere Verantwortung für Verantwortliche

Wie der Name bereits suggeriert, ist der Verantwortliche für den gesamten Datenverarbeitungsvorgang verantwortlich und **muss auch den Nachweis erbringen können**, dass er sämtliche Pflichten erfüllt (Rechenschaftspflicht). Er fungiert als erster Ansprechpartner für betroffene Personen und Behörden. Die Verantwortung kann nicht delegiert werden, auch nicht an den Datenschutzbeauftragten.

Ernennt ein Verantwortlicher einen externen Auftragsverarbeiter (z.B. einen Cloud-Provider oder einen externen IT-Administrator), so muss er sicherstellen, dass dieser hinreichend Garantien dafür bieten, dass **geeignete technische und organisatorische Maßnahmen** so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der EU-Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Datenschutz durch Technikgestaltung und datenschutz-freundlichen Voreinstellungen

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen **Risiken für die**

Rechte und Freiheiten natürlicher Personen trifft der Verantwortliche sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Maßnahmen — wie z. B. Pseudonymisierung —, die dafür ausgelegt sind, die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der EU-Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Verzeichnis der Verarbeitungstätigkeiten

Wenngleich nicht alle Organisationen verpflichtet sind ein Verzeichnis der Verarbeitungstätigkeiten zu führen, ist dasselbe doch Herzstück und **Ausgangspunkt aller Datenschutzüberlegungen** innerhalb einer Organisation.

Das **Verzeichnis skizziert alle Flüsse personenbezogener Daten** und veranschaulicht über welche Kanäle Daten in die Organisation fließen, was mit den Daten innerhalb der Organisation passiert, und an wen die Daten betroffener Personen gegebenenfalls nach außen übermittelt werden.

Zu diesem Zweck wird jede Art der Datenverarbeitung (z.B. Marketing, Lohnbuchhaltung, Video-Überwachung) im Wesentlichen nach den folgenden **Kriterien** analysiert: (a) Zwecke der Verarbeitung, (b) Beschreibung der Datenkategorien, (c) Kategorien von betroffenen Personen, (d) Empfängerkategorien, (e) Löschungsfristen, sowie (f) eine allgemeine Beschreibung der technischen und organisatorischen Daten-Sicherheitsmaßnahmen.

Einwilligung zur Datenverarbeitung durch die betroffene Person

Die Einwilligung zur Datenverarbeitung durch die betroffene Person ist in bestimmten Fällen vom Gesetz vorgeschrieben, und zwar in jenen Fällen, in denen die Datenverarbeitung ein hohes Risiko für den Schutz der Privatsphäre darstellt. In diesen Fällen wird die Kontrollfunktion der betroffenen Person durch die Vorschrift der expliziten Einwilligung gestärkt.

Die EU-Verordnung schreibt explizit in den folgenden Fällen die Einholung durch den Verantwortlichen einer Einwilligung vor:

- Fälle in denen sogenannte **besondere Kategorien personenbezogener Daten** verarbeitet werden (siehe Art. 9 der EU-Verordnung),
- Fälle in denen personenbezogene Daten in **Drittländer** außerhalb der EU/EWR übermittelt werden, insofern als die europäische Kommission besagten Drittländern nicht die Angemessenheit des vor Ort gebotenen Datenschutz-Niveaus attestiert hat;

- Fälle in denen eine ausschließlich auf eine **automatisierte Verarbeitung** – einschließlich Profilierung – berufende Entscheidung des Verantwortlichen der betroffenen Person gegenüber eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt (Art. 22.1.c) EU-Verordnung);
- besonders invasive Fälle von **direktem Marketing** (auf jeden Fall kann die betroffene Person Widerspruch gegen direktes Marketing einlegen).

Datenschutzverletzung

Eine **Datenschutzverletzung** ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von personenbezogenen Daten führt.

Meldung an die Aufsichtsbehörde: Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst **binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, diese der zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

Meldung an die betroffenen Personen: Hat die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

Datenschutz-Folgeabschätzung

Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein **hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch.

Eine Abschätzung über die Folgen einer Datenschutz-Verletzung ist immer ratsam. In den folgenden, grob umrissenen Fällen ist sie vorgeschrieben:

- systematische und umfassende **Bewertung persönlicher Aspekte** natürlicher Personen;
- umfangreiche Verarbeitung **besonderer Kategorien** von personenbezogenen Daten (wie z.B. Daten über Gesundheit, Sexualleben, etc.), sowie Daten über strafrechtliche Verurteilungen und Straftaten;
- systematische umfangreiche **Überwachung** öffentlich zugänglicher Bereiche.

Datenschutz-Beauftragter

Eine **Verpflichtung zur Bestellung eines Datenschutzbeauftragten** besteht für Unternehmen (Verantwortliche und Auftragsverarbeiter), wenn

- die **Kerntätigkeit** in der Durchführung von Verarbeitungsvorgängen besteht, die aufgrund ihrer Art, ihres Umfanges und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von betroffenen Personen erforderlich machen, oder
- die Kerntätigkeit in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von Daten über strafrechtliche Verurteilungen oder Straftaten besteht.

Der Datenschutzbeauftragte hat eine **unabhängige Stellung**, und darf vom Verantwortlichen keine Anweisungen bezüglich der Ausübung seiner Aufgaben erhalten. Er erfüllt unter anderem folgende **Aufgaben**: Unterrichtung und Beratung des Verantwortlichen hinsichtlich seiner Verpflichtungen, Überwachung der Einhaltung der EU-Verordnung, Anlaufstelle für Aufsichtsbehörde und betroffene Personen.

Informationspflichten und Rechte der betroffenen Personen

Informationen und Betroffenenrechte sind ohne unangemessene Verzögerung, spätestens aber **innerhalb eines Monats zu erledigen** (diese Frist kann um höchstens weitere 2 Monate verlängert werden).

Die **grundlegenden Rechte der betroffenen Personen** sind folgende:

- Auskunftsrecht (z.B. Auskunft über die Art der Daten, die verarbeitet werden);
- Recht auf Berichtigung;
- Recht auf Löschung („Vergessenwerden“);
- Recht auf Einschränkung der Verarbeitung (z.B. kein direktes Marketing);
- Mitteilungspflicht bei Berichtigung, Löschung oder Einschränkung an alle Empfänger;
- Recht auf Datenübertragbarkeit;
- Widerspruchsrecht.

Befugnisse der Aufsichtsbehörde – hohe Geldbußen

Einige wesentliche **Befugnisse** der Aufsichtsbehörde (www.garanteprivacy.it/) sind:

- dem Verantwortlichen Anweisungen geben;
- Datenschutz-Überprüfungen vor Ort durchführen;

- Zugang zu allen organisationsinternen Datenschutz-Informationen;
- (Ver)Warnungen auszusprechen;
- Beschränkungen/Verbote in Bezug auf Datenverarbeitungen verhängen.

Hohe **Geldbußen**: Die EU-Verordnung sieht ausdrücklich vor, dass die Verhängung von Geldbußen in jedem Einzelfall „wirksam, verhältnismäßig und abschreckend“ sein soll.

Es sind Geldbußen von bis zu 20 Mio Euro oder Geldbußen von bis zu 4% des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres vorgesehen (zur Anwendung kommt, was höher ist).