17. April 2018
ej/uh

Das neue Datenschutzrecht

Sehr geehrte Mandanten,

die Datenschutz-Grundverordnung (DS-GVO) ersetzt zum 25.05.2018 die bisherigen Regelungen. Unternehmen sind daher gezwungen, ihre datenschutzrelevanten Prozesse im Hinblick auf die neuen Anforderungen zu überprüfen und bis zum 25.05.2018 an der DS-GVO auszurichten. Mit diesem Rundschreiben möchten wir Ihnen einen groben Überblick über die Vorschriften der Datenschutz-Grundverordnung (DS-GVO) geben, die ab dem 25.05.2018 in Kraft tritt.

Die DS-GVO gilt für alle Unternehmen.

Verantwortlicher ist der Unternehmer bzw. Geschäftsführer. Datenschutz ist – wie auch bisher – Chefsache.

Anwendungsbereich

Dreh- und Angelpunkt des Datenschutzes ist nach wie vor die Verarbeitung personenbezogener Daten. Erfasst sind von dieser umfassenden Definition alle Informationen, die aus Sicht des datenverarbeitenden Unternehmens einer natürlichen Person zugeordnet werden können.

In räumlicher Hinsicht ist nach Art. 3 Abs. 1 DS-GVO die Verordnung auf alle Verarbeiter mit Niederlassungen in der Europäischen Union verpflichtend.

An den Prinzipien Transparenz, Richtigkeit, Vertraulichkeit, Datenminimierung und Zweckbindung wird festgehalten (Art. 5 ff DS-GVO).

Der Verantwortliche ist für die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten (Art. 5 Abs. 1 DS-GVO) zuständig und muss deren Einhaltung nachweisen (Rechenschaftspflicht). Inhalt dieser Rechenschaftspflicht ist, dass die Unternehmen jederzeit den Nachweis erbringen können müssen, dass sie bei der Verarbeitung von personenbezogenen Daten die technisch-organisatorischen Anforderungen und die Datenschutz-Grundsätze der DS-GVO einhalten.

Folge dieser Rechenschaftspflicht und der daraus folgenden Dokumentationspflichten ist eine Beweislastumkehr gegenüber den Aufsichtsbehörden und in zivilrechtlichen Streitigkeiten wegen Datenschutzverstößen. Dies bedeutet, dass das Unternehmen sich entlasten muss. **Dies setzt voraus, dass eine Dokumentation vorgelegt werden kann, welche belegt, dass das Unternehmen die datenschutzrechtlichen Grundsätze beachtet hat**.

In der Datenschutz-Dokumentation sollten folgende Punkte erfasst sein:

- Die Grundsätze für die Verarbeitung personenbezogener Daten im Unternehmen;
- Risiko- und Datenschutz-Folgeabschätzungen zu allen relevanten Verarbeitungstätigkeiten im Unternehmen;
- Bereits eventuell identifizierte Datenschutz-Risiken;
- Interne Datenschutz- und IT-Sicherheitsrichtlinien;
- Nachweise über die jeweils durchgeführten Datenschutz-Schulungen von Mitarbeitern und deren Dokumentation;
- Regeln für Kontrollen, Optimierung und Anpassung aller Datenschutz-Maßnahmen.

Im Ergebnis können diese Anforderungen zur Folge haben, dass im Unternehmen ein Datenschutz-Management-System notwendig wird. Künftig sind die Verantwortlichen verpflichtet, ein schriftliches oder elektronisches Verzeichnis aller Verarbeitungstätigkeiten im Unternehmen **(Verfahrensverzeichnis)** zu führen (Art. 30 Abs. 1 DS-GVO).

Das Verfahrensverzeichnis hat folgende Pflichtangaben zu enthalten:

- Name und Kontaktdaten des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

- Die jeweiligen Zwecke der Verarbeitung;

- Die „Kategorien von betroffenen Personen“ (z.B. Beschäftigte, Kunden und deren Mitarbeiter usw.) und die „Kategorien von personenbezogenen Daten“ (z.B. Namen, Anschriften, E-Mail-Adressen, Personalstammdaten, Standortdaten, Gesundheitsdaten usw.);

- „Kategorien von Empfängern“, gegenüber denen personenbezogene Daten offengelegt worden sind oder noch offengelegt werden, einschließlich von Empfängern in Drittländern;

- Übermittlung von personenbezogenen Daten in Drittländer;

- „Wenn möglich“ die Fristen für die Löschung der personenbezogenen Daten. Da die DS-GVO keine statischen Löschfristen kennt, sind solche Fristen insoweit anzugeben, wie sie sich mit angemessenem Aufwand anhand des – individuell zu erstellenden Löschkonzepts – ermitteln lassen;

- „Wenn möglich“ eine allgemeine Beschreibung der technisch organisatorischen Maßnahmen, die das Unternehmen nach Artikel 32 DS-GVO vorsieht. Die Beschreibung im Verzeichnis muss grundsätzlich so konkret sein, dass sie der Aufsichtsbehörde die Beurteilung ihrer Geeignetheit erlaubt. Mit der Formulierung „wenn möglich“ begrenzt die DS-GVO den damit verbundenen Aufwand auf ein verhältnismäßiges Maß.

Nach den Neuregelungen im DS-GVO sind u.a. folgende Maßnahmen einzurichten (Art. 32 DS-GVO):

- Maßnahmen, die die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste sicherstellen;

- Maßnahmen, die die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei Zwischenfällen rasch wieder herstellen (Datensicherung);

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;

- Ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Die Maßnahmen in der Summe müssen ein „angemessenes“ Schutzniveau bieten.

Rechte der Betroffenen

Die Betroffenen können folgende Rechte formlos (also auch mündlich) geltend machen:

Pflicht zur Information

Der Verantwortliche muss auf Anträge des Betroffenen grundsätzlich innerhalb eines Monats antworten (Art. 12 Abs. 3 DS-GVO).

Grundsätzlich sind folgende Informationen mitzuteilen (Art. 13 DS-GVO):

Angaben über:

- Die Kontaktdaten des Verantwortlichen;

- Den Datenschutzbeauftragten;

- Die Zwecke der Datenverarbeitung;

- Die Empfänger der Daten;

- Gegebenenfalls bestehende Absicht der Übermittlung der Daten in ein Drittland;

- Die Dauer der Speicherung der Daten;

- Hinweise auf die Rechte der DS-GVO nach Art. 15 bis 18 (z.B. Auskunft und Berichtigung oder Löschung);

Recht auf Auskunft

Vereinzelt können Auskünfte verlangt werden über:

- Den Zweck der Verarbeitung;
- Die Kategorie der verarbeiteten Daten;
- Die Empfänger oder Kategorien von Empfängern gegenüber denen die Daten offengelegt werden, insbesondere wenn die Offenlegung außerhalb der EU stattfindet;
- Die Dauer der Speicherung der Daten oder die Kriterien für die Festlegung dieser Dauer;
- Das Bestehen eines Rechts auf Berichtigung oder Löschung der Daten oder auf Einschränkung der Verarbeitung oder Widerspruch gegen diese;
- Das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
- Die Herkunft der Daten, wenn die Daten nicht bei den Betroffenen selbst erhoben werden;
- Das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling;

Recht auf Erhalt einer Kopie

Neu ist das Recht, von dem Verantwortlichen eine kostenlose Kopie aller verarbeiteten Daten zu verlangen (Art. 15 Abs. 3 DS-GVO).

Pflicht zur Löschung

Betroffene haben das Recht, die Löschung von Daten in bestimmten Fällen zu verlangen (Art. 17 Abs. 1 DS-GVO).

- Die Daten sind für die ursprünglichen Zwecke nicht mehr erforderlich;

- Widerruf der Einwilligung anderer Rechtsgrundlagen für die Datenverarbeitung;

- Grundsätzlich bei Widerspruch gegen die Verarbeitung;

- Bei Widerspruch gegen die Verwendung der Daten, um Drittwerbung zu betreiben;

- Bei Unrechtmäßigkeit der Verarbeitung;

- Bei Bestehen einer Rechtspflicht zur Löschung aus Unionsrecht oder Recht der Mitgliedsstaaten;

Pflicht zur Benachrichtigung

Datenempfänger sind über Berichtigungen, Löschungen und Sperrungen zu informieren.

Recht auf Sperrung

Als milderes Mittel als Löschung und Berichtigung besteht das Recht zur Sperrung der Datennutzung.

Recht auf Datenübertragbarkeit

Dieses Recht hat zum Inhalt, dass die betroffene Person hiernach das Recht hat, von demjenigen Verantwortlichen, der aktuell im Besitz ihrer personenbezogenen Daten ist, diese heraus zu verlangen.

Rechtsfolgen bei Datenschutzverstößen

Verstöße können sich ergeben aus:

- Dem Nichtvorhandensein der notwendigen Dokumentation;

- Einer Verarbeitung ohne Rechtsfertigungsgrundlage, wie z.B. dem Fehlen der wirksamen Einwilligung;

- Der Nichtgewährung der Rechte der Betroffenen;

- Bei Verstößen gegen allgemeine Grundsätze der Datenverarbeitung.

In Zukunft muss bei einem Verstoß **zwingend** ein Bußgeld festgesetzt werden. Den Aufsichtsbehörden steht insoweit kein Ermessen mehr zu.

Datenschutzbeauftragter

Wenn mindestens 10 Personen ständig mit dem automatisierten Verarbeiten personenbezogener Daten beschäftigt sind, ist ein „Datenschutzbeauftragter" zu bestellen (Art. 37 DS-GVO). Dem Datenschutzbeauftragten obliegen die folgenden Mindestaufgaben (Art. 39 DS-GVO):

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten;

- Überwachung der Einhaltung der DS-GVO;

- Zuweisung von Zuständigkeiten;

- Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeitern und der diesbezüglichen Überprüfungen;

- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung;

- Zusammenarbeit mit der Aufsichtsbehörde.

Wir werden Sie in den kommenden Wochen regelmäßig per E-Mail zum Inhalt der Datenschutz-Grundverordnung informieren.

Mit freundlichen Grüßen

Eugen Jakoby