DSGVO auf einen Blick

Die neue EU-Datenschutz-Grundverordnung (DSGVO) regelt europaweit den Umgang mit personenbezogenen Daten natürlicher Personen durch private Unternehmen sowie öffentliche Stellen und muss bis 25. Mai 2018 umgesetzt sein.	Die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ist grundsätzlich verboten und nur dann erlaubt, wenn entweder eine klare Rechtsgrundlage gegeben ist oder wenn die betroffene Person ausdrücklich ihre Zustimmung gegeben hat („Rechtmäßigkeit der Verarbeitung)

Was versteht man unter personenbezogenen Daten?

Unter personenbezogenen Daten versteht man alle Angaben, mit denen man einen Menschen eindeutig bestimmen kann.
Es gibt dann noch die Unterscheidung „personenbezogene Daten besonderer Kategorien“ (sog. sensiblen Daten), die einer noch strengeren Regelung bei der Verarbeitung unterliegen.

Wer ist von der DSGVO betroffen?

Im Prinzip ist **JEDES** Unternehmen – unabhängig von seiner Größe - betroffen, das personenbezogene Daten natürlicher Personen regelmäßig erhebt, verarbeitet und speichert. Als „Verantwortlicher“ gilt hierbei die natürliche oder juristische Person, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet. Der Verantwortliche haftet dafür, dass bei jedem Verarbeitungsvorgang die Vorschriften der Verordnung eingehalten werden und hat dies durch angemessene technische und organisatorische Maßnahmen (**TOM**) zu gewährleisten (s. Beispiele unten unter dem „WIE“).

Was hat die Umsetzung dieser Verordnung mit Prozessmanagement zu tun?

Wer bereits Prozessmanagement betreibt, darf sich freuen. Die Frage, welche Daten wie und wo verarbeitet werden, sollte dann nämlich ziemlich leicht zu beantworten sein. Aus den vorhandenen Dokumentationen können nun gezielt folgende Informationen aufgelistet werden: Wo werden welche Daten zu welchem Zweck wie erhoben, verarbeitet, und weitergegeben und wie (lange) werden diese gespeichert?

Wo bzw. in welchen Prozessen werden personenbezogene Daten verarbeitet?	Verarbeitungstätigkeit auf Grundlage eines Fachprozesses.
Beispiele Verarbeitungstätigkeiten: ▪ E-Mailverarbeitung ▪ Allgemeine Kundenverwaltung ▪ Lohn- und Gehaltsabrechnung	
Wer verarbeitet die Daten? Wer ist im Unternehmen der Prozessverantwortliche, die Fachabteilung, der Ansprechpartner? Oder werden die Daten extern verarbeitet? ➔ „Auftragsverarbeiter“	Verantwortlicher Ansprechpartner
Beispiele „Auftragsverarbeiter“: ▪ externe Lohnverrechnung ▪ eMail-Service ▪ CRM ▪ Cloud-Anbieter	
Welche personenbezogenen Daten werden verarbeitet? Wessen Daten werden verarbeitet?	Beschreibung der Kategorien betroffener Personen / Datenkategorien
Beispiele Datenkategorien ▪ Adress-/Kontaktdaten ▪ Bankverbindungs-/Kreditkartendaten ▪ IT-Nutzungsdaten ▪ Lohn-und Gehaltsdaten **Beispiele Personenkategorien** ▪ Bewerber- und Mitarbeiterdaten (HR) ▪ Interessenten- und Kundendaten (Marketing, Verkauf) ▪ Lieferantendaten (Einkauf, Lieferantenmanagement)	
Woher kommen die Daten? In welchem Format?	Daten-Herkunft

prozesspunktnull ▪ Saar Pfalz Park 1a ▪ 66450 Bexbach

Telefon: 06826-938409 ▪ E-Mail: info@prozesspunktnull.de ▪ http://prozesspunktnull.de

Hier muss noch vor der Datenerhebung die freiwillige und nachweisbare Einwilligung der betroffenen Person eingeholt werden!
Der Grundsatz der Richtigkeit der Datenverarbeitung verlangt zudem, dass die erhobenen personenbezogenen Daten sachlich richtig und aktuell sein müssen.

Warum werden die Daten erhoben? Eine Verarbeitung kann auch mehrere Zwecke umfassen, so dass auch mehrere Zweckbestimmungen angegeben werden können.	Zweck der Datenerhebung / Verarbeitung
Beispiele: ▪ E-Mailverarbeitung ➔ Durchführung der elektronischen Kommunikation ▪ Allgemeine Kundenverwaltung ➔ Auftragsbearbeitung, Buchhaltung, Inkasso ▪ Lohn- und Gehaltsabrechnung ➔ zur Erstellung der Lohnabrechnung; Erfüllung gesetzl. Anforderungen	Es gilt das Prinzip der Zweckbindung (man kann einmal erhobene Daten nicht für andere Zwecke nutzen)
Wie wird mit den Daten umgegangen? ➔ TOM	Datenverarbeitung
▪ Datenspeicherung: Wo werden die Daten in welchen Formaten gespeichert? ▪ Datenübermittlung: An welchen Empfänger oder Kategorien von Empfängern werden die Daten wie übermittelt? ▪ Zugriffsrechte: Wer hat alles Zugriff auf die Daten?	Grundsatz der Speicherminimierung (so wenig wie möglich)
Wann werden die Daten wieder gelöscht?	Speicherdauer
Wie lang Daten aufbewahrt werden dürfen, hängt vom Zweck ab und von gesetzlichen Aufbewahrungsfristen. Genauso wie das Ersuchen um Einwilligung muss auch der Widerruf leicht zugänglich sein.	Grundsatz der Speicherbegrenzung (so kurz wie nötig)

Was geschieht dann mit diesen Informationen?

Diese Informationen werden dann in einem Verzeichnis von Verarbeitungstätigkeiten festgehalten (VdV).
Wer nun (noch) keine Prozessdokumentation betreibt muss also zunächst eine Inventur aller Verarbeitungsvorgänge vornehmen - schriftlich (besser elektronisch). Mit dem einmaligen Anlegen des VdV ist es jedoch nicht getan. Mindestens einmal jährlich, müssen die jeweiligen Auskunftgeber (z. B. die Abteilungsleiter) bestätigen, dass die Prozesse genauso ablaufen, wie sie dokumentiert wurden. Damit das geschieht, braucht jedes Unternehmen eine Kontaktperson für das VdV (nicht zu verwechseln mit dem Datenschutzbeauftragten, der nur in bestimmten Fällen zu bestellen ist). Bei einem permanent gelebten Prozessmanagement wird die Aktualität der Prozesse bereits ständig gewährleistet.
Um unnötige Doppeldokumentation zu vermeiden, kann im Verarbeitungsverzeichnis auch auf bereits bestehende Dokumente z.B. das allgemeine Sicherheitskonzept bzw. die übergreifenden TOM verwiesen werden. Es ist jedoch zu beachten, dass diese im Bedarfsfall dann auch der Aufsichtsbehörde zur Verfügung gestellt werden müssen.

Tipps

Wenn Sie in Ihren Prozessdokumentationen bisher nur die Einheit „Daten“ verwenden, spezifizieren Sie diese an den entsprechenden Stellen als „personenbezogene Daten“.

Falls noch nicht geschehen, sollten Sie in Ihrer Prozessdokumentation noch einen entsprechenden Prozess zur Pflege des VdV aufnehmen.

Hinweis

Diese Übersicht stellt keine verbindliche Rechtsberatung dar. Sie soll einen kurzen & einfachen Überblick zu den wesentlichen Anforderungen der DSGVO geben und den Zusammenhang zum Prozessmanagement aufzeigen.
Wir nehmen gerne mit Ihnen oder für Sie Ihre Prozessdokumentationen unter die Lupe und geben Ihnen Tipps zur gesetzeskonformen Umsetzung.

Stand: 01.03.2018

prozesspunktnull ▪ Saar Pfalz Park 1a ▪ 66450 Bexbach

Telefon: 06826-938409 ▪ E-Mail: info@prozesspunktnull.de ▪ http://prozesspunktnull.de