

Merkblatt zum Datenschutz für Ehrenamtliche

Hinweis: Der Übersichtlichkeit halber werden im Folgenden nur die männlichen Formen verwendet!

Beim Umgang mit personenbezogenen Daten müssen neben anderen Gesetzen und Vorschriften hauptsächlich die Bestimmungen der Europäischen Datenschutzgrundverordnung (EU-DSGVO) sowie des Bundesdatenschutzgesetzes in seiner Form ab dem 25.05.2018 (BDSGneu) beachtet werden. Verantwortliches Handeln beim Umgang mit personenbezogenen Daten, aber auch die risikobewusste Nutzung von IT-Systemen und Anwendungen sind die zentralen Zielsetzungen. Fehlverhalten kann zu großen materiellen und immateriellen Schäden mit teilweise beträchtlichen negativen Kundeneffekten führen.

Die EU-DSGVO schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.

Kernaussagen der EU-DSGVO

Sachlicher Anwendungsbereich

Die Verordnung 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.

Örtlicher Anwendungsbereich

Die 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.

Darüber hinaus findet die EU-DSGVO auch dann Anwendung, wenn der Verantwortliche oder Auftragsverarbeiter nicht in der Union niedergelassen ist. Hierfür ist es erforderlich, dass es sich um

die Verarbeitung personenbezogener Daten von betroffenen Personen handelt, die sich in der Union befinden. Darüber hinaus muss der nicht in der Union niedergelassene Verantwortliche oder Auftragsverarbeiter Waren oder Dienstleistungen in der Union anbieten oder das Verhalten der betroffenen Personen beobachten.

Begriff „Personenbezogene Daten“ (Art. 4 Nr. 1 EU-DSGVO)

„Personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen - gleichgültig, ob Mitarbeiter, Kollege oder Kunde bzw. Lieferant oder deren Ansprechpartner.

Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind.

Beispiele hierfür sind: Adresse, Telefonnummer, Geburtsdatum, Foto, Arbeitgeber, Gehalt, IP-Adresse, Vermögen, Besitz, Urlaubsplanung, Arbeitsverhalten und Arbeitsergebnisse. Auch Daten ohne direkten Personenbezug (z.B. ohne Namensangabe) können personenbezogene Daten sein, wenn aus ihnen auf die zugehörigen Personen Bezug genommen werden kann (z.B. Personalnummer, PC-Benutzerkennung, maschinenbezogene Nutzungszeiten bei nur einem infrage kommenden Benutzer).

Begriff „Besondere Kategorien personenbezogener Daten“, auch „sensible Daten“ genannt

Besondere Kategorien personenbezogener Daten sind solche Daten aus denen sich die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit ergeben. Darüber hinaus zählen genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung ebenfalls zu den besonderen Kategorien personenbezogener Daten.

Hier gelten besondere Vorschriften, da diese Daten besonders schutzwürdig sind! In der CDU werden vorwiegend diese besonders schützenswerten Daten (Mitgliedschaft in der CDU, politische Meinung) verarbeitet.

Ausnahmen vom Verbot, mit personenbezogenen Daten umzugehen

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn die EU-DSGVO oder eine andere Rechtsvorschrift dies erlaubt oder die betroffene Person eingewilligt hat. Die Daten müssen für die Zwecke, für die sie erhoben und verarbeitet werden, z.B. im Rahmen eines Vertrags, relevant sein, müssen sachlich richtig sein und dürfen nur so lange gespeichert werden, wie es der genannte Zweck erfordert. Unrichtige oder unvollständige Daten sind zu löschen oder zu berichtigen. Nur in gesetzlich bestimmten Fällen oder mit Einwilligung des Betroffenen ist eine anderweitige Verarbeitung zulässig.

Einwilligung

Die Einwilligung des Betroffenen ist nur wirksam, wenn sie auf der freien Entscheidung des Betroffenen beruht. Er ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung sowie auf die Folgen der Verweigerung der Einwilligung hinzuweisen. Ggf. ist eine optische Hervorhebung erforderlich. Sie muss in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache verfasst werden. Der Betroffene muss darüber informiert werden, dass er seine Einwilligung jederzeit widerrufen kann. Die Einwilligung muss nicht zwingend schriftlich erfolgen, allerdings muss die Abgabe einer Einwilligung nachgewiesen werden können, so dass es sich empfiehlt, eine schriftliche Einwilligung einzuholen.

Die Einwilligung für besondere Kategorien personenbezogener Daten (sensible Daten, Begriffserläuterung siehe nachfolgend) ist gesondert erforderlich.

Rechte der Betroffenen

Jeder, dessen personenbezogene Daten verarbeitet werden, hat gegenüber dem Verantwortlichen grundsätzlich das Recht eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, hat die betroffene Person ein Recht auf Auskunft hinsichtlich bestimmter Informationen (z.B. Verarbeitungszwecke, welche Kategorien personenbezogener Daten verarbeitet werden, wer der Empfänger der personenbezogenen Daten ist etc.). Sollten Sie bei Ihrer Tätigkeit in unserem Unternehmen mit einem Auskunftersuchen konfrontiert werden, binden Sie bitte umgehend Ihren Datenschutzbeauftragten mit ein.

Jedermann hat das Recht, sich unmittelbar an die Datenschutzaufsichtsbehörde zu wenden, wenn er der Ansicht ist, bei der Verarbeitung seiner personenbezogenen Daten in seinen Rechten verletzt zu sein; das gilt auch für Beschäftigte in Unternehmen.

Datensicherheit durch entsprechende technische und organisatorische Maßnahmen

Die EU-DSGVO verlangt die Umsetzung von angemessenen technischen und organisatorischen Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dies schließt unter anderem folgende Maßnahmen ein:

- die Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Obwohl üblicherweise der Arbeitgeber die notwendigen Maßnahmen organisiert, ist jeder einzelne Mitarbeiter für die Umsetzung mit verantwortlich. Richtiges Verhalten gemäß Arbeitsvertrag und Arbeits-/Dienstanweisung ist unabdingbar.

Übermittlung in Nicht-EU-/EWR-Staaten

Die Übermittlung in Nicht-EU-/EWR-Staaten ist nur in sehr beschränkten Ausnahmen zulässig.

<p>Zu widerhandlungen gegen die EU-DSGVO bzw. das BDSGneu sind mit Bußgeld, mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe belegt.</p>

Allgemeine Verhaltensregeln beim Umgang mit Daten

nur sichere Passwörter auswählen (z.B. mit Sonderzeichen, keine Namen) und regelmäßig wechseln

Bildschirm und PC sind bei Abwesenheit vom Arbeitsplatz zu sperren

Laptops bei Reisen sorgfältig sichern, besonders im Auto, im Hotel und auf Flughäfen
keine vertraulichen Informationen per Fax schicken; falls doch erforderlich: besondere
Vorkehrungen treffen (z.B. telefonische Absprache wegen Anwesenheit des Empfängers,
Doppelkontrolle der Richtigkeit der eingegebenen Faxnummer vor Versand)
nicht einfach mit Antwortfunktion auf E-Mail mit vertraulichem Inhalt reagieren, vorher
Absenderlisten überprüfen! (Achtung: vertrauliche Informationen über E-Mail grundsätzlich
nicht versenden, wenn keine Verschlüsselung genutzt werden kann)
vertrauliche Telefonate nicht vom Handy in der Öffentlichkeit führen

Bei Fragen zum Thema Datenschutz bzw. Datensicherheit oder in Zweifelsfällen wenden Sie sich bitte an Ihren Beauftragten für den Datenschutz.