

Datenschutz-Grundverordnung –Teil 5: Was zur DSGVO-Analyse noch dazugehört

In welchem Ausmaß einzelne Unternehmen betroffen sind, sollte einer genaueren Betrachtung unterzogen werden. Hier einige Begriffe, die man im Zusammenhang mit der DSGVO betrachten muss.

11.04.2018, 15:05



Alexander Limbach/Shutterstock
© ALEXANDER LIMBACH_SHUTTERSTOCK

Einwilligung

Als Einwilligung der betroffenen Person gilt jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Diese Einwilligung kann schriftlich, elektronisch oder auch mündlich erfolgen, etwa auch durch Anklicken eines Kästchens auf einer Internetseite, durch die Auswahl technischer Einstellungen für Dienste der Informationsgesellschaft oder andere Erklärungen oder Verhaltensweisen, die im jeweiligen Kontext eindeutig das Einverständnis der betroffenen Person zur Datenverarbeitung signalisieren. Stillschweigen, bereits vorangekreuzte Kästchen oder Untätigkeit können keine Einwilligung darstellen. Wenn die Verarbeitung mehreren Zwecken dient, ist für jeden Zweck der Verarbeitung eine gesonderte Einwilligung nötig. Eine „ausdrückliche“ Einwilligung ist nur bei der Verarbeitung von sensiblen Daten erforderlich. Aus Beweisgründen ist anzuraten, auch bei der Zustimmungserklärung von nicht-sensiblen Daten schriftliche Einwilligungserklärungen oder sonstige nachweisbare Zustimmungserklärungen einzuholen.

Datenschutzbeauftragter

Verantwortliche und Auftragsverarbeiter können der Verpflichtung zur Bestellung eines Datenschutzbeauftragten unterliegen. Eine freiwillige Bestellung ist jederzeit möglich. Die Aufgaben sind:

- Die Unterrichtung und Beratung der Unternehmer und Mitarbeiter.
- Die Überwachung und Überprüfung der Einhaltung der Datenschutzvorschriften und Strategien für den Schutz personenbezogener Daten, einschließlich der Zuweisung von Zuständigkeiten, Sensibilisierung und Schulung der Mitarbeiter.
- Beratungen – auf Anfrage - im Zusammenhang mit der Datenschutz-Folgenabschätzung und der Überwachung ihrer Durchführung.
- Die Zusammenarbeit mit der Aufsichtsbehörde und Anlaufstelle für diese.

Der Datenschutzbeauftragte kann ein Dienstnehmer oder ein Selbstständiger sein.

Folgenabschätzung

Eine Datenschutz-Folgenabschätzung muss gemacht werden, wenn neue Technologien verwendet werden oder wenn aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen besteht. Das sind z.B.:

- Die systematische und umfassende Bewertung persönlicher Aspekte, die die Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, die Zuverlässigkeit oder das Verhalten, den Aufenthaltsort oder Ortswechsel natürlicher Personen betreffen, auf Basis automatisierter Verarbeitung: Hiermit
- sind vor allem Profiling-Maßnahmen angesprochen.
- Eine umfangreiche Verarbeitung sensibler Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen oder Straftaten.
- Eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche: z.B. mittels Videoüberwachung. Die Datenschutz-Folgenabschätzung muss zumindest Folgendes enthalten:
 - eine systematische Beschreibung der geplanten Verarbeitungsvorgänge,
 - die Beschreibung der Verarbeitungszwecke,
 - eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Datenverarbeitung,
 - eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen,
 - die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Datenschutz sichergestellt wird,
 - die vom Datenschutzbeauftragten erteilten Empfehlungen und die dazu getroffenen Entscheidungen,
 - den Standpunkt der Betroffenen bzw. deren Vertreter. Wird der Standpunkt nicht eingeholt, muss dies begründet werden.
 - Ebenso muss begründet werden, wenn die endgültige Entscheidung des Verantwortlichen vom Standpunkt der Betroffenen oder ihrer Vertreter abweicht.

Betroffenenrechte

Die Rechte der von einer Datenanwendung betroffenen Person gegenüber dem Verantwortlichen sind:

- Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person.
- Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.
- Auskunftsrecht.
- Recht auf Berichtigung.
- Recht auf Löschung
- Recht auf Einschränkung der Verarbeitung.
- Recht auf Datenübertragbarkeit.
- Widerspruchsrecht.

Auskunftspflicht

Verantwortliche müssen betroffenen Personen gegenüber eine Auskunft über deren personenbezogene Daten geben. Auskünfte sind schriftlich zu erteilen und das in einer leicht verständlichen Form. Die Auskunft muss kostenlos erfolgen und das binnen eines Monats ab Eingang der Anfrage.

Websites, Webshops

IP-Adressen gelten als personenbezogene Daten. Werden solche Daten auf Websites verarbeitet, gilt die DSGVO. Für Webshop-Betreiber gilt sie auf jeden Fall. Rechtmäßig sind die Daten verarbeitet, wenn sie für die Erfüllung eines Vertrags, z.B. für einen Online-Einkauf, unbedingt erforderlich sind. Marketingmaßnahmen nach einem Kauf sind bereits nicht mehr zur Vertragserfüllung notwendig. Außer der Betroffene hat eingewilligt z.B. Newsletter zu erhalten. Diese Erklärungen müssen inhaltlich und optisch von Texten abgekoppelt sein - Checkboxes müssen aktiv angekreuzt werden. Es gibt umfangreiche Informationspflichten bereits zum Zeitpunkt der Datenerhebung. Werden Daten nicht unmittelbar vom Betroffenen erhoben, sondern von Dritten, gibt es besondere Informationspflichten.

Sensible Daten

Das sind personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Profiling

Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen. Das Profiling unterliegt den Vorschriften der DSGVO, wie etwa den Grundsätzen für die Verarbeitung, der Rechtmäßigkeit der Verarbeitung, der Informations- und Auskunftspflicht und besonderen Regeln, wenn damit eine automatisierte Generierung von Einzelentscheidungen verbunden ist.

Berichtigung, Löschung, Einschränkung

Diese Pflichten betreffen den Verantwortlichen. Auftragsverarbeiter müssen solche Anträge an die Verantwortlichen weiterleiten. Der Antrag kann von jeder betroffenen Person formlos gestellt werden, auch mündlich. Per Telefon werden wahrscheinlich Zweifel an der Identität bestehen, anders bei einer persönlichen Anfrage.

- **Berichtigung:** Die Daten sind unrichtig, (z.B. falsches Geburtsdatum) oder sie sind unter Berücksichtigung des Zwecks der Verarbeitung unvollständig.
- **Löschung:** Die Daten sind für die Zwecke, für die sie erhoben wurden, nicht mehr nötig oder die betroffene Person widerruft ihre Einwilligung. Die betroffene Person hat Widerspruch gegen die Verarbeitung eingelegt und es liegen keine vorrangigen berechtigten Gründe für die Verarbeitung vor. Die Daten wurden unrechtmäßig verarbeitet. Oder die Löschung der Daten ist zur Erfüllung einer rechtlichen Verpflichtung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten erforderlich.
- **Einschränkung:** Die betroffene Person hat die Richtigkeit der Daten bestritten, solange der Verantwortliche die Richtigkeit der Daten noch überprüft. Oder sie hat Widerspruch gegen die Verarbeitung eingelegt, solange noch nicht feststeht, ob die berechtigten Gründe des Verantwortlichen gegenüber denen des Betroffenen überwiegen. Obwohl die Verarbeitung unrechtmäßig ist, will die betroffene Person lieber eine Einschränkung statt einer Löschung. Der Verantwortliche benötigt die Daten nicht länger, der Betroffene jedoch für seine Rechtsansprüche schon.

Meldung „data breach“

Eine Verletzung des Schutzes personenbezogener Daten bedeutet eine Sicherheitsverletzung, die zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten führt. Das wäre z.B. durch einen Hackangriff oder den Verlust eines Datenträgers. Eine Verletzung muss sofort an die Aufsichtsbehörde und im Falle eines voraussichtlich hohen Risikos auch an die betroffenen Personen gemeldet werden. Ein Auftragsverarbeiter muss eine solche Verletzung dem Verantwortlichen melden.

Geldstrafen

Gibt es keine Einigung zwischen betroffenen Personen und Unternehmen, kann sich die Person an die Datenschutzbehörde wenden, die ein Verfahren einleitet. Ein erlittener Schaden muss nachgewiesen, vor Gericht eingeklagt und verhandelt werden. Geldbußen für Verstöße gegen diese Verordnung sollen in jedem Einzelfall wirksam, verhältnismäßig und abschreckend sein. Die Verletzung der Betroffenenrechte ist mit bis zu 20 Millionen Euro oder vier Prozent des letztjährigen weltweiten Jahresumsatzes sanktioniert.

Tipp!

3 Vertiefungs-Webinar zur Datenschutz-Grundverordnung

- [Datenschutz-Grundverordnung – Anwendungsbereich \(Teil 1 der Serie\)](#)
- [Datenschutz-Grundverordnung – Wofür ein Verantwortlicher haftet \(Teil 2 der Serie\)](#)
- [Datenschutz-Grundverordnung – Wüber betroffene Personen bei der Erhebung der Daten informiert werden müssen \(Teil 3 der Serie\)](#)
- [Datenschutz-Grundverordnung: Verarbeitungsverzeichnis: Wer es führen muss und was es enthält! \(Teil 4 der Serie\)](#)

Das könnte Sie auch interessieren



„Die Kanäle wie auch die Anforderungen der Kunden ändern sich laufend. Man muss am Ball bleiben.“

Interview mit Dr. Heidrun Unterweger, E-Commerce Expertin, POSITIVconsult > mehr



„In dem Moment, wo in den gesammelten Daten Muster gefunden werden können, tun sich noch mehr Möglichkeiten auf.“

Interview mit Martin Puaschitz, Fachgruppenobmann UBIT [› mehr](#)



Vor 20 Jahren gab es viele Bewerber und keinen Markt für Green Jobs. Heute ist es umgekehrt.

Dipl.-Ing. Gudrun Schindler, Leiterin Career Center der Universität für Bodenkultur im Interview.

[› mehr](#)