EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung

Voraussetzungen für die Rechtmäßigkeit der Verarbeitung

Welche Grundsätze sind bei der Verarbeitung von personenbezogenen Daten einzuhalten?

Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz:

Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Dies setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung der personenbezogenen Daten leicht zugänglich und verständlich in klarer und einfacher Sprache abgefasst sind. Der Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung sowie die Auskunft darüber, welche sie betreffende personenbezogene Daten verarbeitet werden.

Zweckbindung:

Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden. Als nicht unvereinbar gilt eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Zwecke oder für statistische Zwecke.

Datenminimierung:

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. Dazu zählt auch, dass Verantwortliche durch technische Voreinstellungen sicherzustellen haben, dass grundsätzlich nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden.

Richtigkeit:

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Es sind alle angemessenen Maßnahmen zu treffen, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

Speicherbegrenzung:

Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. Daher sollte der Verantwortliche Fristen für die Löschung oder regelmäßige Überprüfungen vorsehen. Eine längere Speicherung ist vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen für ausschließlich im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke zulässig.

Integrität und Vertraulichkeit:

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Durch geeignete technische und organisatorische Maßnahmen soll insbesondere auch gewährleistet werden, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die die Geräte, mit denen diese verarbeitet werden, benutzen können.

Achtung:
Der Verantwortliche ist für die Einhaltung der genannten Grundsätze verantwortlich und muss deren Einhaltung **nachweisen** können (**„Rechenschaftspflicht"**).

Unter welchen Voraussetzungen ist die Verarbeitung rechtmäßig?

Bei Einhaltung der oben genannten Grundsätze ist die Verarbeitung - sofern es sich nicht um „sensible Daten" (= besondere Kategorie von personenbezogenen Daten) handelt - rechtmäßig, wenn mindestens eine der folgenden Bedingungen erfüllt ist:

- Die betroffene Person hat ihre **Einwilligung** zur Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben. Die Einwilligung muss durch eine eindeutige bestätigende Handlung erfolgen, mit der freiwillig, für den konkreten Fall, in informierter Weise und unmissverständlich bekundet wird, dass die betroffene Person 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.

  Hinweis:
  Für die Zulässigkeit der Verarbeitung **„sensibler Daten"** ist eine **„ausdrückliche Einwilligung"** erforderlich.

Besonderheiten bei Einwilligungserklärungen von Kindern

Die **Einwilligung eines Kindes**, die sich auf ein Angebot von Diensten der Informationsgesellschaft, die einem Kind direkt gemacht werden, bezieht, ist nach der DSGVO nur rechtmäßig, wenn das Kind das sechszehnte Lebensjahr vollendet hat. Die Mitgliedstaaten können eine niedrigere Altersgrenze vorsehen, die jedoch nicht unter dem dreizehnten Lebensjahr liegen darf: Das österreichische Datenschutzgesetz (DSG) setzt diese Altersgrenze mit dem **vollendeten 14. Lebensjahr** fest. In sonstigen Fällen hat die Einwilligung durch den Träger der elterlichen Verantwortung oder mit dessen Zustimmung zu erfolgen.

- Die Verarbeitung ist für die **Erfüllung eines Vertrages**, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen.
- Die Verarbeitung ist zur **Erfüllung einer rechtlichen Verpflichtung** erforderlich, der der Verantwortliche unterliegt (z.B. arbeits(zeit)rechtlichen oder steuerrechtlichen Verpflichtungen).
- Die Verarbeitung ist erforderlich, um **lebenswichtige Interessen** der betroffenen Person oder einer anderen natürlichen Person zu schützen.
- Die Verarbeitung ist für die **Wahrnehmung einer Aufgabe** erforderlich, die im **öffentlichen Interesse** oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.
- Die Verarbeitung ist zur **Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten** erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen (dies insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt).

Hinweis: Nach dem Erwägungsgrund 47 der DSGVO kann die Datenverarbeitung zum Zweck der Direktwerbung ein berechtigtes Interesse darstellen

Unter welchen Voraussetzungen ist eine Weiterverarbeitung für einen anderen Zweck zulässig (z.B. Kundendaten, die für eine Vertragsabwicklung erhoben wurden, sollen für Marketingzwecke verwendet werden)?

Ohne Rücksicht auf die Vereinbarkeit der Zwecke der Verarbeitung ist eine Weiterverarbeitung ausschließlich zulässig, wenn:

- eine Einwilligung dafür vorliegt, oder
- eine gesetzliche Grundlage die Weiterverarbeitung vorsieht.

In allen sonstigen Fällen muss die **Weiterverarbeitung mit den Zwecken**, für die die personenbezogenen Daten ursprünglich erhoben worden sind, **vereinbar** sein. Um diese Vereinbarkeit festzustellen ist Folgendes zu berücksichtigen:

- jede Verbindung zwischen den ursprünglichen und neu beabsichtigten Zwecken
- der Zusammenhang, in dem die Daten erhoben wurden
- die Art der Daten (insbesondere ob sensible oder strafrechtlich relevante Daten vorliegen)
- mögliche Folgen der Weiterverarbeitung für betroffene Personen
- das Vorhandensein angemessener Garantien (z.B. Pseudonymisierung)

Liegt eine solche Vereinbarkeit mit den ursprünglichen Zwecken vor, ist keine andere gesonderte Rechtsgrundlage erforderlich, als diejenige für die

Erhebung der personenbezogenen Daten.

> **Beispiel**: Kundendaten, die für eine Vertragsabwicklung erhoben wurden, werden für eine postalische Werbung für ein ähnliches Produkt verwendet. Nach einem Autokauf wird vom Verkäufer eine Erinnerung bezüglich der Erneuerung der § 57a KFG-Plakette an den Käufer übermittelt.

Die Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt als vereinbarer und rechtmäßiger Verarbeitungsvorgang.

Beabsichtigt der Verantwortliche die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten, so muss er der betroffenen Person vor dieser Weiterverarbeitung **Informationen über diesen anderen Zweck** und alle anderen maßgeblichen Informationen zur Verfügung stellen.

Verarbeitung von „sensiblen Daten“

Die Verarbeitung von **„sensiblen Daten“** ist untersagt.

Dieses Verbot gilt ausschließlich in folgenden Fällen nicht (dh die Verarbeitung sensibler Daten ist **in folgenden Fällen zulässig**):

- Vorliegen einer ausdrücklichen Einwilligung
- Vorliegen einer gesetzlichen Grundlage (einschließlich Kollektivverträge und Betriebsvereinbarungen) zur Ausübung von Rechten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes
- Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person (und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben)
- Datenverarbeitung durch eine politische, weltanschaulich, religiös oder gewerkschaftlich ausgerichtete Stiftung, Vereinigung oder sonstige Organisation ohne Gewinnerzielungsabsicht im Rahmen ihrer rechtmäßigen Tätigkeit auf der Grundlage geeigneter Garantien
- die personenbezogenen Daten wurden durch die betroffene Person offensichtlich öffentlich gemacht
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit
- aufgrund eines erheblichen öffentlichen Interesses auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaats
- Gesundheitsvorsorge, Arbeitsmedizin, medizinische Diagnostik, Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich (auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaates oder eines Vertrages mit einem Angehörigen eines Gesundheitsberufs). Die Daten müssen von Fachpersonal, dass nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einem Berufsgeheimnis unterliegt, oder Personen, die ebenfalls nach dem Unionsrecht oder dem Recht eines Mitgliedstaats oder den Vorschriften nationaler zuständiger Stellen einer Geheimhaltungspflicht unterliegen, verarbeitet werden.
- aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke (auf der Grundlage des Unionsrechts oder des Rechts eines Mitgliedstaates).

Für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten sind die Mitgliedstaaten befugt, zusätzliche Bedingungen, einschließlich Beschränkungen, einzuführen oder aufrecht zu erhalten.

Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten

Die Verarbeitung personenbezogener Daten über **strafrechtliche Verurteilungen und Straftaten** darf nach der DSGVO nur unter behördlicher Aufsicht vorgenommen werden oder wenn dies nach dem Unionsrecht oder dem Recht der Mitgliedstaaten zulässig ist: Gemäß dem österreichischen Datenschutzgesetz (DSG) ist die Verarbeitung von personenbezogenen Daten über **gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen**, insbesondere auch über den **Verdacht** der Begehung von Straftaten, sowie über **strafrechtliche Verurteilungen** oder **vorbeugende Maßnahmen** unter Einhaltung der Vorgaben der DSGVO zulässig, wenn

- eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verarbeitung solcher Daten besteht oder
- sich sonst die Zulässigkeit der Verarbeitung dieser Daten aus gesetzlichen Sorgfaltspflichten ergibt oder die Verarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten (sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen) erforderlich ist, und die Art und Weise, in der die Datenverarbeitung vorgenommen wird, die Wahrung der Interessen der betroffenen Person nach der DSGVO und dem DSG gewährleistet.

Geldstrafen

Verstöße gegen die Grundsätze und die Regeln betreffend die Rechtmäßigkeit der Verarbeitung sind mit Geldbußen bis zu 20 Mio EUR oder im Falle eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres bedroht.

Relevante Artikel der DSGVO: Art 5 - 10

Relevante Erwägungsgründe: 39ff

Relevante Bestimmungen des DSG: § 4 Abs 3 und 4

Stand: 11.03.2021