Crashkurs Datenschutz-Grundverordnung

Die zehn wichtigsten Fragen und Antworten zur Datenschutz-Grundverordnung

1) Welche Datenverarbeitungsmethoden sind betroffen?

Im Prinzip jede systematische Erfassung von Daten - gleich mit welchen Hilfsmitteln (d.h. elektronisch oder physisch) und gleich ob automatisiert oder manuell bearbeitet:

„Diese 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." **(Art. 2 DSGVO Sachlicher Anwendungsbereich)**

2) Was sind personenbezogene Daten?

Dieser Begriff ist sehr weit gefasst: Es sind alle Daten, die zu einer bestimmten Person gehören und die aufgrund auf diese bestimmte Person zu lassen.

Diese Verordnung bezeichnet mit „personenbezogenen Daten" alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person") beziehen; 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." **(Art. 4 Nr. 1 DSGVO Begriffsbestimmungen)**

3) Was ist unter Verarbeitung zu verstehen?

Auch dieser Begriff ist sehr weit gefasst und umfasst eigentlich alles, wozu man Daten überhaupt benutzen kann:

Diese Verordnung bezeichnet mit „Verarbeitung" jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;"..... **(Art. 4 Nr. 2 DSGVO Begriffsbestimmungen)**

4) Was ist bei der Verarbeitung von personenbezogenen Daten immer zu beachten?

Die nach der DSGVO zulässige Verarbeitung steht unter dem Vorbehalt, dass mehrere grundlegende Prinzipien eingehalten werden. Das wichtigste davon ist die Rechtmäßigkeit der Verarbeitung (im Einzelnen dazu Frage 5). Die weiteren Grundsätze stellen für jeden gewissenhaften und vertragstreuen Unternehmer eine Selbstverständlichkeit dar. Sie sind in Art. 5 DSGVO (Grundsätze für die Verarbeitung personenbezogener Daten) im Anhang abgedruckt und lassen sich unter den folgenden Schlagworten zusammenfassen:

- Verarbeitung nach Treu und Glauben, wie sie der Betroffene berechtigter Weise erwarten kann
- Transparenz der Datenverarbeitung
- Gebundenheit der Datenverarbeitung an den Zwecke, zu dem sie erhoben wurden
- Datensparsamkeit
- Datenrichtigkeit
- Begrenzung der Speicherdauer
- Gewährleistung der Datenintegrität und des Schutzes der Daten vor unbefugtem Zugriff
- Verantwortlichkeit und Rechenschaftspflicht gegenüber dem Betroffenen

5) Wann ist eine Verarbeitung rechtmäßig?

In den allermeisten Fällen dient die Datenverarbeitung der Vorbereitung und Durchführung von Verträgen. Art. 6 DSGVO erlaubt diese Verarbeitung und davon abgesehen – im Wesentlichen – nur, wenn der Betroffene eingewilligt hat (dazu Frage 6).

„Die Verarbeitung (der personenbezogenen Daten) ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden personenbezogenen Daten für einen oder mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;" .....**(Art. 6 DSGVO Rechtmäßigkeit der Verarbeitung)**

6) Wie muss die Einwilligung des Betroffenen ausgestaltet sein?

Der Datenverarbeiter muss gem. Art. 7 DSGVO die Einwilligung des Betroffenen nachweisen, weshalb sich eine schriftliche Einwilligung empfiehlt. Im Zusammenhang von weiteren Vertragserklärungen des Betroffenen ist diese Einwilligung davon deutlich abzusetzen.

„Abs. 1 Beruht die Verarbeitung auf einer Einwilligung, muss der Verantwortliche nachweisen können, dass die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat.

Abs. 2 Satz 1 Willigt die betroffene Person durch eine schriftliche Erklärung ein, die noch andere Sachverhalte betrifft, so muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist."..... **(Art. 7 DSGVO Bedingungen für die Einwilligung)**

7) In welchen Fällen muss die betroffene Person informiert werden?

Die Informationsverpflichtung in Art 13 DSGVO ist eine Vorschrift, die stark interpretationsbedürftig ist. Ausgangspunkt ist: ist dem Betroffenen klar oder muss im bewusst sein, dass der Unternehmer aufgrund der spezifischen Vertragsdurchführung personenbezogene Daten erhebt? Wenn, wie in den meisten Fällen, der Betroffene diese Daten dem Unternehmer selbst offenbart, wäre eine sich anschließende Informationspflicht darüber reichlich über-

flüssig. Deshalb finden „die Absätze 1, 2 und 3 keine Anwendung, wenn und soweit die betroffene Person bereits über die Informationen verfügt." **Art. 13 Abs. 4 DSGVO)**

In allen anderen Fällen gilt Folgendes: „Werden personenbezogene Daten bei der betroffenen Person erhoben, so teilt der Verantwortliche der betroffenen Person zum Zeitpunkt der Erhebung dieser Daten Folgendes mit:

- den Namen und die Kontaktdaten des Verantwortlichen sowie gegebenenfalls seines Vertreters;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke, für die die personenbezogenen Daten verarbeitet werden sollen, sowie die Rechtsgrundlage für die Verarbeitung; **(Art. 13 Abs. 1 DSGVO)**

8) Welche Rechte hat die Person, der Daten verarbeitet werden?

In Kapitel 3 (Art. 12 – 23) der DSGVO sind die Rechte der betroffenen Person aufgelistet. Dort ist also nachlesen, was ein Betroffener vom Unternehmer in Bezug auf seine verarbeiteten Daten verlangen kann. Hier gebe ich lediglich in Stickworten einen Überblick, da dieser Fall bei kleinen Betrieben – hoffentlich - eher sehr selten bis überhaupt nicht eintreten wird.

Art. 12 Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
Art. 13 Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person
Art. 14 Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden
Art. 15 Auskunftsrecht der betroffenen Person
Art. 16 Recht auf Berichtigung
Art. 17 Recht auf Löschung („Recht auf Vergessenwerden")
Art. 18 Recht auf Einschränkung der Verarbeitung
Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung
Art. 20 Recht auf Datenübertragbarkeit
Art. 21 Widerspruchsrecht
Art. 22 Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
Art. 23 Beschränkungen (der vorgenannten Rechte und Pflichten durch nationale Gesetze sofern für öffentliche Zwecke gerechtfertigt)

9) In welchen Fällen muss ein Verarbeitungsverzeichnis erstellt werden?

In der Regel nur bei Mittelbetrieben ab 250 Mitarbeiter, denn Art. 30 Abs. 5 DSG-VO befreit von der Verpflichtung nach Abs. 1 und 2 Art. 30 DSG-VO in folgenden Fällen:

(5) Die in den Absätzen 1 und 2 genannten Pflichten **gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen,** es sei denn die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, **die Verarbeitung erfolgt nicht nur gelegentlich oder** es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Art 9 Abs. 1 (dazu im Anhang) bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Art. 10.

-> Die Verarbeitung ist m.E. schon dann nur gelegentlich, wenn z.B. auf die gespeicherten Kundendaten nur zugegriffen wird, wenn eine neue Bestellung eingeht oder einmal im Jahr eine Weihnachtskarte versandt wird. Denn nur bei einer weiten Interpretation der Vorschrift bleibt für die Ausnahmeregel überhaupt noch ein sinnvoller Anwendungsbereich im wirklichen Leben. Dann kommt es nur noch auf die Mitarbeiterzahl an. Aber auch bei regelmäßiger Verarbeitung ist das Verarbeitungsverzeichnis nur auf Verlangen der Aufsichtsbehörde vorzulegen. Zur Not kann das Verzeichnis dann immer noch erstellt werden.

-> Ich empfehle allerdings nachdrücklich, dieses Verarbeitungsverzeichnis zumindest in groben Zügen zeitnah zu erstellen, jedenfalls dann, wenn Kundendaten regelmäßig verarbeitet werden. Jeder Unternehmer sollte sich im Klaren darüber sein, welche Daten er zu welchen Zwecken verarbeitet oder verarbeiten lässt und insbesondere ob er oder sein Dienstleister den hohen Sicherheitsanforderungen, die m.E. berechtigter Weise an Datenverarbeitungsprozesse gestellt werden, wirklich in allen Punkten gerecht werden.

10) In welchen Fällen ist in einem Betrieb ein Datenschutzbeauftragter erforderlich?

-> Nach § 38 BDSG n. F. ist ein Datenschutzbeauftragter zu benennen, wenn

- im Unternehmen i. d. R. mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind,
- im Unternehmen (unabhängig von der Personenzahl) personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet werden,
- die Hauptaufgabe des Unternehmens in einer umfangreichen Verarbeitung besonderer Datenkategorien oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.

Anhang: Auszüge aus der DSGVO

Art. 5 DSGVO Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Art. 89 Abs. 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

e) 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; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Art. 89 Abs. 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 9 Abs. 1 DSGVO

(1) Die Verarbeitung personenbezogener 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 ist untersagt.

Art. 30 Abs. 1 bis 4 DSGVO Verzeichnis von Verarbeitungstätigkeiten

(1) Jeder Verantwortliche und gegebenenfalls sein Vertreter führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. 2Dieses Verzeichnis enthält sämtliche folgenden Angaben:

- den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;
- die Zwecke der Verarbeitung;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1.

(2) Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1.

(3) Das in den Absätzen 1 und 2 genannte Verzeichnis ist schriftlich zu führen, was auch in einem elektronischen Format erfolgen kann.

(4) Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.