Lektion 1

Begriffserklärungen

Die 25 wichtigsten Begriffe und Erklärungen der DSGVO mit Kommentar und Praxisbeispielen.

DSGVO KURSE
INFORMATIV UND FLEXIBEL

DSGVO ADVICE
E-LEARNING PLATTFORM

DSGVO oder DS-GVO?

Wenn Sie sich bereits mit dem europäischen Datenschutzgesetz, der "EU-Datenschutz-Grundverordnung", beschäftigt haben, sind Sie wahrscheinlich auf die Frage gestoßen, wie man es am besten abkürzen kann. Häufig werden die Abkürzungen "DS-GVO" und "DSGVO" verwendet - aber welche ist korrekt?

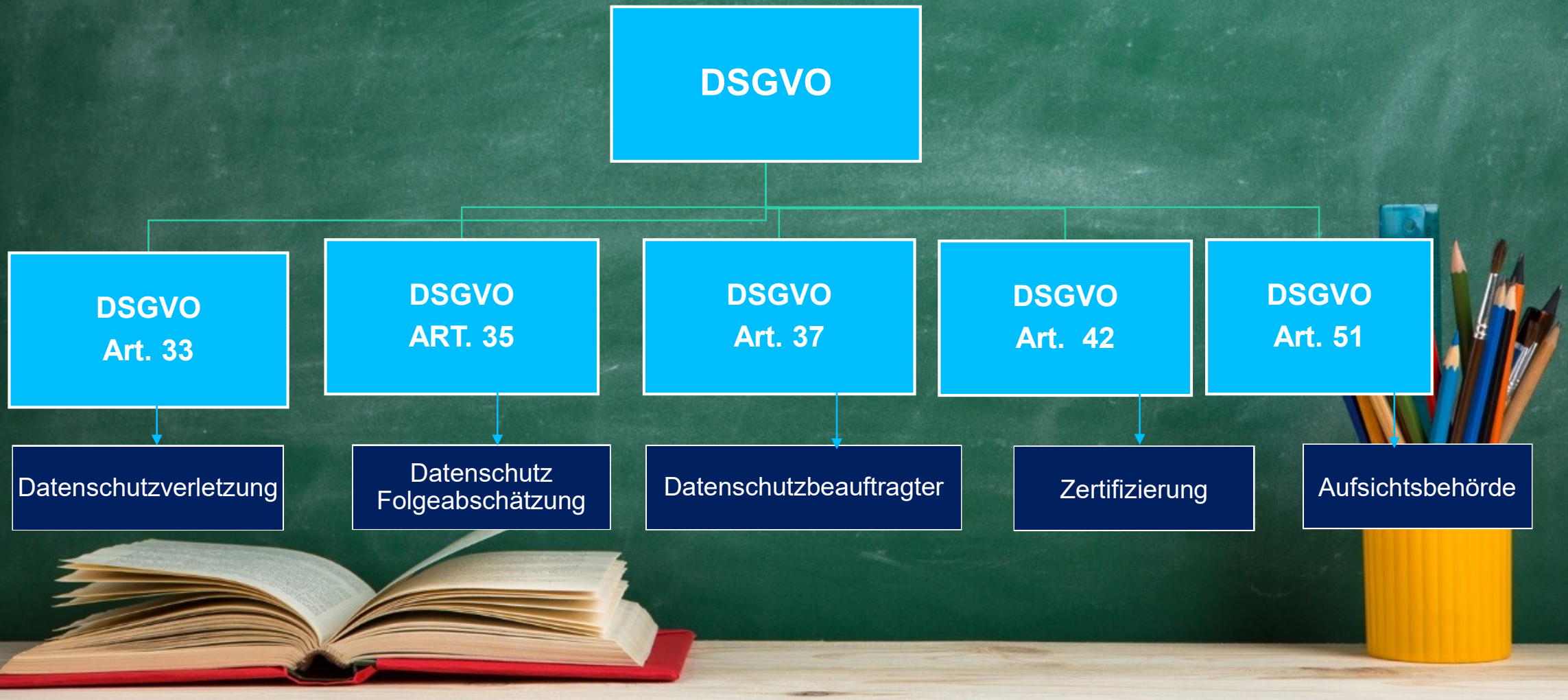
In der aktuellen Fassung der DSGVO (wir verwenden hier die Version ohne Bindestrich) gibt es keine festgelegte Abkürzung. Stattdessen wird dort von der "Datenschutz-Grundverordnung", der "Verordnung" oder der "Verordnung (EU) 2016/679" gesprochen.

Es ist anzumerken, dass im ursprünglichen Entwurf der EU-Kommission tatsächlich die Abkürzung "DS-GVO" verwendet wurde (Entwurf DS-GVO 2017-10).

DSGVO KURSE
INFORMATIV UND FLEXIBEL

DSGVO und die wichtigsten Artikel

DSGVO und die wichtigsten Artikel



1

"Betroffener" - Personenbezogene Daten

Im Gesetzestext wird das Wort Betroffener nicht verwendet. Es wird eigentlich von einer „natürlichen Person" oder einer „betroffenen Person" gesprochen. Trotzdem hat sich das Wort „Betroffener" in der Verwendung mit der DSGVO etabliert.

Somit sind die Begriffe „Betroffener", „natürliche Person", „Datensubjekt" und „betroffene Person" Synonyme. Wer es genau wissen will, kann das im **Art.4/1 DSGVO** nachlesen.

„Personenbezogene Daten" sind 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 (1)

Beispiel:
Ein Unternehmen speichert E-Mail-Adressen, Namen, usw. von Mitarbeitern (Betroffene) im Intranet. Durch das Speichern, Bereithalten und der Abrufbarkeit von Daten im internen Netzwerk des Unternehmens, ist der Tatbestand der Datenverarbeitung personenbezogener Daten im Sinne der DSGVO erfüllt.

2

Genetische Daten

„genetische Daten“ sind personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden.

Art. 4 (13)

Beispiel:

Mitarbeiter einer Arztpraxis oder eines Krankenhauses erheben für die Analyse und Bewertung möglicher Krankheitsdispositionen Informationen über erbliche Merkmale (genetische Daten) des Betroffenen.

3 Biometrische Daten

Art. 4 (14)

„personenbezogene Daten“ sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen.

Beispiel:
Der 2010 in Deutschland eingeführte neue Personalausweis verfügt über eine Biometriefunktion im Sinne der DSGVO. Damit wird es berechtigten Behörden, z. B. der Polizei, ermöglicht, das auf dem elektronischen Chip des Ausweises gespeicherte Lichtbild oder ggf. gespeicherte Fingerabdrücke des Ausweisinhabers auszulesen.

4 Gesundheitsdaten

Art. 4 (15)

Gesundheitsdaten“ sind personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen.

Beispiel:
Ein Unternehmen ergreift wegen der Corona-Krise, Maßnahmen die das Erheben von Gesundheitsdaten umfassen; z. B. durch Fiebermessungen oder Fragebögen, die an Mitarbeiter verteilt werden und in denen nach Krankheitssymptomen gefragt wird, oder zu welchen Personen ein erkrankter Mitarbeiter Kontakt hatte.

5 Profiling

Art. 4 (4)

„Profiling“ ist jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen 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.

Beispiel:
Ein Energieversorger installiert mitrechnende Stromzähler, das heißt intelligente Messsysteme in den Haushalten seiner Kunden. Diese Geräte könnten Verbrauchsprofile erstellen, z. B. ob Mitglieder eines Haushalts im Urlaub oder auf der Arbeit sind und fallen deshalb unter den Profilingbegriff gemäß Art. 4 Abs. 4 DSGVO.

6 Pseudonymisierung

Art. 4 (5)

„Pseudonymisierung“ ist die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden.

Beispiel:
In einer neuen Forschungsdatenbank der Krankenkassen sollen künftig die Daten aller gesetzlich Versicherten wie beispielsweise Alter, Geschlecht und Wohnort aber auch Diagnosen, Behandlungen und Krankschreibungen pseudonymisiert (Art. 4 Abs. 5 DSGVO) (ohne Zuordnungsmöglichkeit) gespeichert werden.

7 Datenverarbeitung

„Verarbeitung“ ist jeder 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 (2)

Beispiel:

Bei einem Unternehmen geht eine E-Mail zwecks Bestellung einer Ware ein. Die Mail enthält Angaben über den Besteller und stellt in der Regel bereits eine Erhebung personenbezogener Daten dar. Nach der Erhebung folgt in aller Regel die Datenweiterverarbeitung, zum Beispiel die Eingabe in das interne Bestellsystem der Firma. Auch die elektronische Übermittlung der Adressdaten des Bestellers an einen Paketdienst, der die Auslieferung der Waren übernimmt, ist als Verarbeitung personenbezogener Daten zu werten.

8 Dateisystem

Art. 4 (6)

Unter „Dateisystem“ versteht die DSGVO jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

Beispiel:

Ein Rechtsanwalt ordnet die Akten seiner Mandanten nach dem Namen oder alternativ nach Vorgangsnummern. Die Aktensammlung gilt als Dateisystem. Eine Sekte notiert im Rahmen der Missionierung handschriftliche Notizen auf Zettel. Da die Daten der angesprochenen Personen in der Sammlung leicht wiederzufinden und zugeordnet werden können, gelten die Zettel als Dateisystem im Sinne der DSGVO.

9

Einwilligung

“Einwilligung“ der betroffenen Person ist 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.

Art. 4 (11)

Beispiel:

Ein deutsches Unternehmen bietet spezielle Services für Jugendliche an. Um diese Services nutzen zu können, müssen diese der Verarbeitung ihrer personenbezogenen Daten zustimmen. Damit diese Einwilligung rechtswirksam ist, müssen die Jugendlichen mindestens 16 Jahre alt sein. Wenn nun in Deutschland ein 14-jähriger den Service in Anspruch nehmen will und ohne Einverständniserklärung der Erziehungsberechtigten der Verarbeitung seiner Daten zustimmt, fehlt es an einer gültigen Einwilligung und das Unternehmen darf die Daten des Jugendlichen weder erheben noch verarbeiten.

10 Verantwortlicher

Der oder die „Verantwortlicher“ ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personen-bezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verant-wortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.

Art. 4 (7)

Beispiel:
Google durchsucht das Internet automatisch, kontinuierlich und systematisch auf dort veröffentlichte Informationen und erhebt somit auch personenbezogene Daten. Diese werden ausgelesen, gespeichert und organisiert auf den Servern von Google für die Nutzer der Suchmaschine bereit. Das ist eine Datenverarbeitung im klassischen Sinn. Die Fa. Google ist daher laut der DSGVO Verantwortlicher für die Daten im Suchindex.

11 Auftragsverarbeiter

Art. 4 (8)

Ein „Auftragsverarbeiter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

Beispiel:

Eine Brauerei unterzeichnet einen Vertrag mit einem Lohnabrechnungsunternehmen, das die Gehälter der Brauereimitarbeiter bucht und überweist. Zu diesem Zweck erhielt das Lohnabrechnungsunternehmen von der Brauerei personenbezogene Daten der Mitarbeiter. Die Daten werden im betriebseigenen IT-System des Lohnabrechnungsunternehmens gespeichert und verarbeitet. Damit ist das Lohnabrechnungs-unternehmen Auftragsverarbeiter im Sinne der DSGVO.

12 Dritter

Ein „Dritter“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten.

Art. 4 (10)

Beispiel:
Das deutsche Tochterunternehmen eines weltweit tätigen Pharmaunternehmens erstellt und vertreibt Arzneimitteln. Beim Austausch von medizinischen Informationen zu ihren Produkten arbeitet die Firma mit Ärzten, Apothekern und Patienten zusammen. Dazu werden auch personenbezogene Daten erfasst und verarbeitet. Der Mutterkonzern im Ausland hat Interesse an diesen Daten. Er ist im Sinne der DSGVO als Dritter zu werten.

13 Empfänger

Ein „Empfänger“ ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung.

Art. 4 (9)

Beispiel:
Ein Kunde bestellt auf der Webseite eines Online-Shops, Waren und gibt zwecks Bearbeitung und Lieferung der Bestellung, seinen Namen und seine Adresse an. Empfänger dieser Daten ist der Verantwortliche für den Online-Shop.

14 Verzeichnis von Verarbeitungstätigkeiten

Der richtige Begriff ist „Verzeichnis der Verarbeitungstätigkeiten„. Es werden für diesen Begriff verschiedene Worte verwendet so z.B.

- **Dokumentationspflicht**
- **Verfahrensverzeichnis**
- **Verarbeitungsverzeichnis**

Diese Beschreibungen sind Synonyme für den oben genannten Begriff.

Art. 30 (1)

Beispiel:

Ein Unternehmen erfasst die Arbeitszeiten seiner Mitarbeiter und erhebt dazu bestimmte persönliche Daten derselben. Diese Verarbeitungstätigkeit, wird vom Unternehmen in das Verzeichnis von Verarbeitungstätigkeiten gemäß Art. 30 DSGVO aufgenommen. Ein anderes Unternehmen präsentiert sich online. Da im Rahmen des Webauftrittes in jedem Fall Server-Log Daten verarbeitet werden, wird dieses Verfahren von dem Unternehmen in das Verzeichnis von Verarbeitungstätigkeiten aufgenommen.

15 Unternehmen

Art. 4 (18)

Das „Unternehmen“ ist eine natürliche oder juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

16 Unternehmensgruppe

Art. 4 (19)

Die „Unternehmensgruppe“ ist eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

17 Internationale Organisation

Art. 4 (26)

„internationale Organisation“ eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

18 Hauptniederlassung

Art. 4 (16)

- im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;

- im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

19 Vertreter

Art. 4 (17)

Ein „Vertreter“ ist eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt.

20 Grenzüberschreitende Verarbeitungen

Art. 44 (1)

entweder

- eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder
- eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann.

Beispiel:
Die Internationale kriminalpolizeiliche Organisation (Interpol) erhält, speichert und übermittelt zwecks Erfüllung ihres Auftrags, personenbezogene Daten, um nationale Behörden bei der Bekämpfung internationaler Kriminalität zu unterstützen. Die Datenübermittlung aus der Union an Interpol und die Staaten, die Mitglieder zu Interpol abgestellt haben, ist eine grenzüberschreitende Verarbeitung im Sinne der DSGVO.

21 Verbindliche interne Datenschutzvorschriften

Unter „verbindliche interne Datenschutzvorschriften“ Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern

Art. 47 (2)

Beispiel:
Ein Unternehmen erlässt ein Datensicherheitskonzept mit Maßnahmen zum Schutz personenbezogener Daten, und verpflichtet sich als Verantwortliche für die Datenverarbeitung zur Einhaltung dieser Vorgaben.

22 Verletzung des Schutzes personenbezogener Daten

„Verletzung des Schutzes personenbezogener Daten“ ist eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

Art. 4 (12)

Beispiel:
Der Mitarbeiter eines Unternehmens verliert seinen Laptop mit personenbezogenen Daten.

23 Maßgeblicher und begründeter Einspruch

„Maßgeblicher und begründeter Einspruch“ einen Einspruch im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder nicht oder ob die beabsichtigte Maßnahme gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen.

Art. 4 (24)

Beispiel:
Das Unternehmen meldet den Verlust des Laptops an den niedersächsischen Datenschutzbeauftragten.

24 Aufsichtsbehörde

Art. 4 (21)

„Aufsichtsbehörde“ ist eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle.

Beispiel:

Dieser verhängt ein Bußgeld. Das Unternehmen legt gegen den Bußgeldbescheid Einspruch ein und begründet diesen damit das keine Datenschutzverletzung vorliegt, da die Daten auf dem Laptop passwortgeschützt und die Festplatte außerdem verschlüsselt ist.

25 Betroffene Aufsichtsbehörde

Art. 4 (20)

„betroffene Aufsichtsbehörde“ ist die Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

- der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,
- diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder
- eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde.

Je nachdem wo der für die Datenschutzverletzung Verantwortliche seinen Firmensitz hat, sind mit Ausnahme von Bayern die jeweiligen Landesbeauftragten für den Datenschutz die betroffene Aufsichtsbehörde. In Bayern besteht hierfür ein eigenständiges Landesamt für Datenschutzaufsicht.

Schauen Sie sich diese Geschichte an. ☺

Das Bremer Unternehmen Testtrans (**Verantwortlicher**) verkauft weltweit Speicheltests für DNA-Analysen, die der Kunde (**Betroffener**) von zuhause aus durchführt. Die vom Kunden zurückgesandten Blutproben lässt das Unternehmen in einem Labor (**Auftragsverarbeiter**) analysieren. Die Webseite des Unternehmens verfügt über einen Webshop, worüber Waren und/oder Dienstleistungen des Unternehmens gekauft werden können. Für die Abwicklung des Kaufs und den Vertragsabschluss, erhebt und speichert (**Verarbeitung**) das Unternehmen personenbezogene Daten seiner Kunden, zum Beispiel Namensdaten, Postanschrift und E-Mail-Adresse, im internen CRM-System (**Dateisystem**).

Auf einer Online-Coaching-Plattform bietet das Unternehmen außerdem eine personalisierte Ernährungsberatung an. Dazu arbeitet das Unternehmen mit selbstständigen Ernährungsberatern (**Dritter**) zusammen, die auf der Grundlage von Kundenangaben zu ihrer Gesundheit, wie z. B. Zuckerwerte, Cholesterinwerte etc. (**Gesundheitsdaten**), individuelle Ernährungsempfehlungen aussprechen. Rechtsgrundlage für die Verarbeitung dieser Daten ist die (**Einwilligung**) entsprechend Art. 6 Abs. 1 a in Verbindung mit Art. 9 Abs. 2 S. 1 DSGVO, die der Kunde bei einer Registrierung als Nutzer der Plattform abgeben musste. Die Firma verbürgt sich dafür dass alle Gesundheitsdaten ihrer Kunden ohne Hinzuziehung zusätzlicher Informationen (Algorithmus zur Berechnung der Zuordnung) nicht mehr einer spezifischen Person zugeordnet werden können (**Pseudonymisierung**) und von der Firma als einzelne Daten daher nicht einsehbar sind.

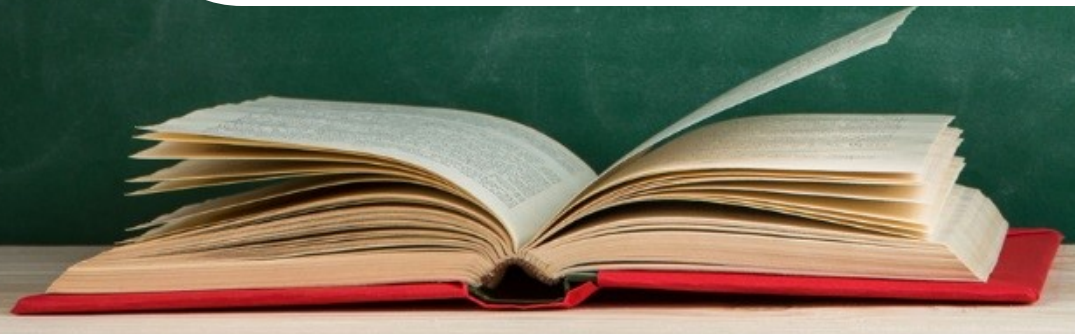
Auf der Webseite besteht für Kunden die Möglichkeit, einen kostenfreien Newsletter zu abonnieren. Um den Newsletter auf die persönlichen Interessen der Besteller zuzuschneiden, wird bei Versand des Newsletters, dass Nutzerverhalten der Empfänger automatisch ausgewertet und ein Benutzerprofil erstellt (**Profiling**). Rechtsgrundlage ist Art. 6 Abs. 1 f DSGVO (**Interessensabwägung**). Zur weiteren Optimierung der Webseite wird der Dienst Google Analytics, dessen Rechenzentren in den USA stehen, eingesetzt, wodurch ein Drittlandtransfer (**grenzüberschreitende Verarbeitung**) stattfindet.

Als die Server des Unternehmens gehakt und versucht wurde personenbezogene Daten zu entwenden, hat das Unternehmen Testtrans, um korrekt zu handeln, sofort reagiert und die Datenschutzverletzung dem Bremer Datenschutzbeauftragten (**Betroffene Aufsichtsbehörde**) gemeldet. Da aufgrund ergriffener IT-Sicherheitsstandards keine personenbezogenen Daten unbefugt entwendet werden konnten (**Verletzung des Schutzes personenbezogener Daten**) und auch kein Verstoß gegen das vom Unternehmen eingeführte Datenschutzkonzept () vorlag, hat die zuständige Aufsichtsbehörde von Maßnahmen abgesehen. Ein Einspruch (**Maßgeblicher und begründeter Einspruch**) (**Verbindliche interne Datenschutzvorschriften**) gegen eine evtl. nicht im Einklang mit der DSGVO stehende Maßnahmenanordnung der Datenschutzbehörde entfiel daher.

Artikel 4 der DSGVO definiert die wichtigsten Begriffe, die in der Verordnung verwendet werden. Ein Beispiel für einen solchen Begriff ist "personenbezogene Daten", der in Artikel 4(1) wie folgt definiert ist:

"Personenbezogene Daten" sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person ("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, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.

Ein Beispiel für personenbezogene Daten wäre der Name, die Adresse oder die E-Mail-Adresse einer Person.



Artikel 5 der DSGVO legt die Grundsätze für die Verarbeitung personenbezogener Daten fest.

Ein Beispiel für einen dieser Grundsätze ist das Prinzip der "**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben**, **Transparenz**", wie es in Artikel 5(1)(a) definiert ist. Dieser Grundsatz besagt, dass personenbezogene Daten auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden müssen.

Ein Beispiel dafür wäre, wenn ein Online-Shop die personenbezogenen Daten seiner Kunden (wie Namen, Adressen und Zahlungsinformationen) nur für den Zweck der Abwicklung von Bestellungen verwendet und die Kunden über die Verwendung ihrer Daten transparent informiert, beispielsweise durch eine Datenschutzerklärung auf der Website oder durch explizite Einwilligungserklärungen während des Bestellvorgangs.

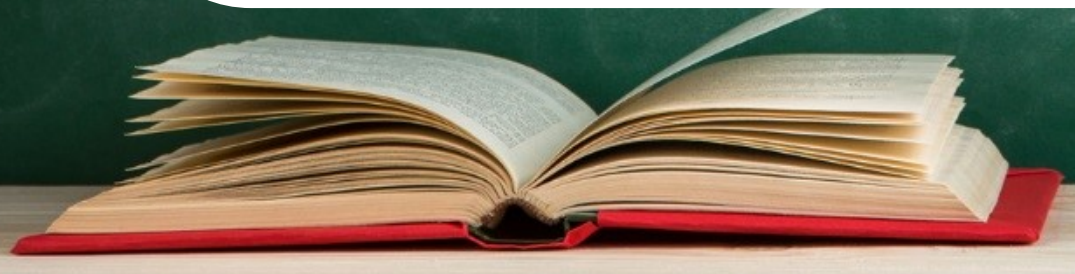
Artikel 6 der DSGVO behandelt die Rechtmäßigkeit der Verarbeitung personenbezogener Daten.

Ein Beispiel für einen Absatz dieses Artikels wäre Artikel 6(1)(a), der die Verarbeitung personenbezogener Daten aufgrund der Einwilligung der betroffenen Person regelt.

Ein Beispiel für die Anwendung dieses Artikels wäre, wenn ein Online-Marketingunternehmen personenbezogene Daten wie E-Mail-Adressen verwendet, um Newsletter an potenzielle Kunden zu senden. Gemäß Artikel 6(1)(a) der DSGVO muss das Unternehmen die ausdrückliche Einwilligung der betroffenen Personen einholen, bevor es deren Daten für diesen Zweck verarbeitet. Die betroffenen Personen müssen klar informiert werden, wie ihre Daten verwendet werden, und sie müssen aktiv der Verarbeitung zustimmen, indem sie beispielsweise ein Kontrollkästchen auf einer Website ankreuzen oder eine Bestätigungs-E-Mail senden.

Artikel 20 der DSGVO behandelt das Recht auf Datenübertragbarkeit. Gemäß diesem Artikel hat die betroffene Person das Recht, die sie betreffenden personenbezogenen Daten, die sie einem Verantwortlichen bereitgestellt hat, in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Sie hat auch das Recht, diese Daten einem anderen Verantwortlichen ohne Behinderung durch den Verantwortlichen, dem die personenbezogenen Daten bereitgestellt wurden, zu übermitteln.

Ein Beispiel für die Anwendung dieses Artikels wäre, wenn ein Social-Media-Nutzer seine persönlichen Daten, wie Profilinformationen, Fotos und Beiträge, von einem sozialen Netzwerk herunterladen möchte, um sie dann zu einem anderen sozialen Netzwerk zu übertragen. Gemäß Artikel 20 der DSGVO hat der Nutzer das Recht, eine Kopie seiner Daten in einem maschinenlesbaren Format zu erhalten und diese Daten dann an das neue soziale Netzwerk zu übertragen, ohne dabei durch das erste soziale Netzwerk behindert zu werden.



Artikel 22 der DSGVO betrifft das automatisierte individuelle Entscheidungsfindung einschließlich Profiling.

Gemäß diesem Artikel hat die betroffene Person das Recht, nicht einer ausschließlich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt.

Ein Beispiel für die Anwendung dieses Artikels wäre, wenn ein Finanzinstitut ein automatisiertes System verwendet, um Kreditanträge zu bewerten und zu entscheiden, ob ein Kredit gewährt wird oder nicht, ohne dass menschliche Entscheidungsträger eingreifen. Wenn ein Kunde aufgrund dieses automatisierten Systems abgelehnt wird und glaubt, dass die Entscheidung fehlerhaft oder diskriminierend war, hat er das Recht, nicht ausschließlich dieser automatisierten Entscheidung unterworfen zu sein. Stattdessen könnte der Kunde verlangen, dass seine Bewerbung von einem menschlichen Mitarbeiter überprüft wird, um sicherzustellen, dass alle relevanten Faktoren berücksichtigt wurden.

Artikel 28 der DSGVO regelt die Verarbeitung im Auftrag. Dieser Artikel legt die Bedingungen fest, unter denen ein Verantwortlicher (z. B. ein Unternehmen oder eine Organisation) einen Auftragsverarbeiter (z. B. einen externen Dienstleister) beauftragen kann, personenbezogene Daten im Auftrag des Verantwortlichen zu verarbeiten.

Ein Beispiel für die Anwendung dieses Artikels wäre, wenn ein Unternehmen einen Cloud-Dienstleister beauftragt, um seine Kundendaten zu speichern und zu verwalten. Gemäß Artikel 28 der DSGVO müssen zwischen dem Unternehmen (dem Verantwortlichen) und dem Cloud-Dienstleister (dem Auftragsverarbeiter) ein Vertrag geschlossen werden, der die Bedingungen für die Verarbeitung der personenbezogenen Daten festlegt. Der Vertrag sollte unter anderem die Art und Zwecke der Datenverarbeitung, die Sicherheitsmaßnahmen, die der Auftragsverarbeiter ergreifen muss, sowie die Rechte und Pflichten beider Parteien in Bezug auf den Datenschutz und die Datenverarbeitung festlegen.

Artikel 33 der DSGVO behandelt die Mitteilung einer Datenschutzverletzung an die Aufsichtsbehörde.

Gemäß diesem Artikel ist der Verantwortliche im Falle einer Verletzung des Schutzes personenbezogener Daten verpflichtet, die Aufsichtsbehörde unverzüglich und möglichst **binnen 72 Stunden**, nachdem ihm die Verletzung bekannt wurde, zu benachrichtigen, es sei denn, die Verletzung ist voraussichtlich nicht mit einem Risiko für die Rechte und Freiheiten natürlicher Personen verbunden.

Ein Beispiel für die Anwendung dieses Artikels wäre, wenn ein Unternehmen feststellt, dass aufgrund eines Hackerangriffs personenbezogene Daten seiner Kunden kompromittiert wurden. In diesem Fall ist das Unternehmen verpflichtet, die zuständige Aufsichtsbehörde innerhalb von 72 Stunden nach Entdeckung des Vorfalls über die Datenschutzverletzung zu informieren. Die Benachrichtigung sollte alle relevanten Informationen über die Art der Verletzung, die betroffenen Daten und die getroffenen oder geplanten Maßnahmen zur Eindämmung des Vorfalls enthalten.

Artikel 35 der DSGVO betrifft die Datenschutz-Folgenabschätzung.

Gemäß diesem Artikel ist der Verantwortliche verpflichtet, vor der Verarbeitung personenbezogener Daten eine Datenschutz-Folgenabschätzung durchzuführen, wenn die vorgesehene Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben würde.

Ein Beispiel für die Anwendung dieses Artikels wäre, wenn ein Unternehmen plant, ein neues System einzuführen, das eine umfangreiche Verarbeitung personenbezogener Daten beinhaltet, beispielsweise ein System zur automatisierten Profilbildung von Kunden für personalisierte Werbezwecke. Bevor dieses System implementiert wird, muss das Unternehmen eine Datenschutz-Folgenabschätzung durchführen, um die potenziellen Risiken für die Datenschutzrechte der betroffenen Personen zu bewerten. Die Folgenabschätzung könnte beinhalten, Risiken wie Datenschutzverletzungen, Diskriminierung oder Verlust der Privatsphäre zu identifizieren und geeignete Maßnahmen zu entwickeln, um diese Risiken zu minimieren oder zu verhindern.

Artikel 37 der DSGVO betrifft die Bestellung eines Datenschutzbeauftragten.

Gemäß diesem Artikel ist der Verantwortliche und der Auftragsverarbeiter verpflichtet, einen Datenschutzbeauftragten zu bestellen, wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung von personenbezogenen Daten besteht, die eine regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang erfordert oder wenn die Verarbeitung von besonderen Kategorien personenbezogener Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten umfangreich ist.

Ein Beispiel für die Anwendung dieses Artikels wäre, wenn ein Krankenhaus regelmäßig und systematisch personenbezogene Gesundheitsdaten von Patienten verarbeitet, um medizinische Behandlungen durchzuführen und medizinische Versorgung zu gewährleisten. In einem solchen Fall wäre das Krankenhaus gemäß Artikel 37 der DSGVO verpflichtet, einen Datenschutzbeauftragten zu bestellen, um sicherzustellen, dass die Verarbeitung der sensiblen Gesundheitsdaten der Patienten gemäß den Datenschutzbestimmungen erfolgt und die Rechte der betroffenen Personen gewahrt werden.

Artikel 42 der DSGVO betrifft die Zertifizierung.

Gemäß diesem Artikel können unabhängige Zertifizierungsstellen Zertifizierungsmechanismen und -verfahren für die Zertifizierung der Einhaltung der Datenschutz-Grundverordnung entwickeln. Diese Zertifizierungen können sich auf spezifische Verarbeitungstätigkeiten beziehen und sollten den betroffenen Personen und den Aufsichtsbehörden als Nachweis für die Einhaltung dienen.

Ein Beispiel für die Anwendung dieses Artikels wäre, wenn ein Cloud-Dienstleister ein Zertifizierungsverfahren gemäß Artikel 42 durchläuft, um seine Datenschutzmaßnahmen zu validieren und die Einhaltung der DSGVO zu bestätigen. Nach Abschluss des Zertifizierungsverfahrens erhält der Cloud-Dienstleister ein Datenschutzzertifikat, das von einer unabhängigen Zertifizierungsstelle ausgestellt wurde. Dieses Zertifikat dient dann als Nachweis für die Kunden des Cloud-Dienstleisters und den Aufsichtsbehörden, dass der Dienstleister die Anforderungen der DSGVO erfüllt und angemessene Datenschutzmaßnahmen implementiert hat.

Artikel 51 der DSGVO behandelt die Befugnisse der Aufsichtsbehörden.

Gemäß diesem Artikel haben die Aufsichtsbehörden verschiedene Befugnisse, um sicherzustellen, dass die Bestimmungen der Datenschutz-Grundverordnung eingehalten werden.

Ein Beispiel für die Anwendung dieses Artikels wäre, wenn eine Aufsichtsbehörde eine Untersuchung einleitet, um eine mögliche Datenschutzverletzung in einem Unternehmen zu prüfen. Die Behörde hat das Recht, von dem betreffenden Unternehmen alle erforderlichen Informationen anzufordern, um die Verarbeitung personenbezogener Daten zu überprüfen, einschließlich Zugang zu den relevanten Dokumenten und Systemen.

Darüber hinaus kann die Aufsichtsbehörde auch Vor-Ort-Inspektionen durchführen, um sicherzustellen, dass die Datenschutzbestimmungen eingehalten werden. Wenn die Untersuchung ergibt, dass das Unternehmen gegen die DSGVO verstößt, kann die Aufsichtsbehörde entsprechende Sanktionen verhängen, um die Einhaltung der Verordnung sicherzustellen.

Die Artikel 12 bis 22 der DSGVO behandeln die Rechte der betroffenen Personen:

- **Artikel 12:** Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person.
- **Artikel 13:** Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person.
- **Artikel 14:** Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden.
- **Artikel 15:** Recht auf Auskunft und Kopie der verarbeiteten personenbezogenen Daten.
- **Artikel 16:** Recht auf Berichtigung der verarbeiteten personenbezogenen Daten.
- **Artikel 17:** Recht auf Löschung ("Recht auf Vergessenwerden") der verarbeiteten personenbezogenen Daten.
- **Artikel 18:** Recht auf Einschränkung der Verarbeitung der personenbezogenen Daten.
- **Artikel 19:** Mitteilungspflicht im Zusammenhang mit der Berichtigung oder Löschung personenbezogener Daten oder der Einschränkung der Verarbeitung.
- **Artikel 20:** Recht auf Datenübertragbarkeit.
- **Artikel 21:** Widerspruchsrecht gegen die Verarbeitung personenbezogener Daten.

Ein Beispiel für die Anwendung dieser Rechte wäre, wenn ein Internetnutzer von einem Unternehmen verlangt, eine Kopie seiner gespeicherten Daten gemäß Artikel 15 zu erhalten. Das Unternehmen müsste dem Nutzer dann eine Zusammenfassung seiner gespeicherten Daten zur Verfügung stellen, einschließlich Informationen darüber, wie diese Daten verwendet wurden und an wen sie weitergegeben wurden.

Und hier eine Geschichte, in der alle Begriffe vorkommen. ☺

Inmitten der geschäftigen Altstadt Lingen, wo Fachwerkhäuser den Marktplatz säumten, befand sich die kleine Schneiderei von Frau Meier. Sie war bekannt für ihre handgefertigten Unikate, die sie mit Liebe zum Detail und viel Sorgfalt entwarf.

An einem sonnigen Tag trat ein junger Mann namens Jonas in ihr Geschäft. Er hatte von Frau Meiers Talent gehört und wünschte sich ein individuelles Hemd. Mit seinen Maßen (DSFA ist erforderlich) und Wünschen im Gepäck, willigte Jonas in die Verarbeitung seiner personenbezogenen Daten ein, damit Frau Meier sein Wunschhemd
schneidern konnte.

Um die Daten von Jonas zu schützen, hatte Frau Meier einen Datenschutzbeauftragten bestellt. Dieser kümmerte sich um die Einhaltung der Datenschutzgrundsätze und unterstützte Frau Meier bei der Erfüllung ihrer Rechenschaftspflicht.

Bevor Frau Meier mit der Verarbeitung von Jonas' Daten begann, führte sie eine Datenschutz-Folgenabschätzung durch, um mögliche Risiken für seine Privatsphäre zu identifizieren. Sie entschied sich dafür, seine Daten zu pseudonymisieren, um seine Identität zu schützen.

Mit Hilfe eines Auftragsverarbeiters, einer Schneiderei in der Nachbarschaft, fertigte Frau Meier das Hemd nach Jonas' Vorgaben. Sie versicherte sich, dass der Auftragsverarbeiter die Datenschutzbestimmungen einhielt.

Als das Hemd fertig war, war Jonas begeistert. Er bedankte sich bei Frau Meier und bat sie um eine Kopie seiner Daten, um sie bei Bedarf zu anderen Schneidern übertragen zu können. Frau Meier gewährte ihm sein Recht auf Datenübertragbarkeit und stellte ihm alle relevanten Informationen zur Verfügung.

Einige Wochen später erhielt Frau Meier eine Nachricht von der Datenschutzbehörde. Es war eine Datenschutzverletzung gemeldet worden: Jonas' Daten waren unbeabsichtigt an Dritte weitergegeben worden. Frau Meier nahm die Angelegenheit ernst und leitete sofort Schritte ein, um den Schaden zu beheben.

Sie informierte Jonas über den Vorfall und entschuldigte sich für die Unannehmlichkeiten. Jonas war verärgert, aber er wusste, dass Frau Meier alles in ihrer Macht Stehende tat, um die Situation zu beheben.

Der Vorfall sensibilisierte Frau Meier noch mehr für die Bedeutung des Datenschutzes. Sie verstärkte ihre Sicherheitsmaßnahmen und schulte ihre Mitarbeiter im Umgang mit personenbezogenen Daten.