Schulung zum Datenschutz
bei der Rechtsanwaltskammer Köln

Inhaltsübersicht

- Einführung
- Anwendungsbereich des Datenschutzrechts
- Grundprinzipien des Datenschutzes
- Rechte der Betroffenen
- Welche Folgen können bei Datenschutzverstößen eintreten
- Regelungen zum Datenschutz und zur Informationssicherheit in Ihrem Unternehmen
- Wohin kann ich mich bei Fragen wenden?

Was ist Datenschutz?

Datenschutz ist Grundrechtsschutz

- Das Grundgesetz garantiert jedem das Recht, über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen (Grundrecht auf informationelle Selbstbestimmung).
- Jeder soll frei entscheiden können, welche seiner personenbezogenen Daten er wann, wem und zu welchem Zweck zugänglich macht.
- Schutz des Einzelnen vor dem Missbrauch seiner personenbezogenen Daten.

Wo ist der Datenschutz gesetzlich geregelt?

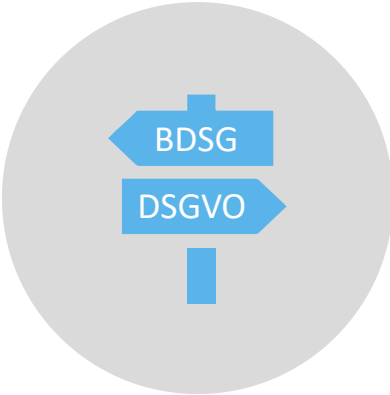
- Europaweit in der DSGVO geregelt
- BDSG ergänzt die DSGVO
- Bereichsspezifische Vorschriften
  - Strafgesetzbuch: § 201 Vertraulichkeit des Wortes, § 202 Briefgeheimnis
  - Kunsturhebergesetz: §§ 22 ff Recht am eigenen Bild
  - Sozialgesetzbücher
  - Arzneimittelgesetz: § 40 Abs. 2a, §40b Abs. 6

- Abgeschlossene Datenvereinbarungen vorrangig, soweit sie den Anforderungen der DSGVO gerecht werden

Wo ist der Datenschutz gesetzlich geregelt?

Die Datenschutzgrundverordnung (DSGVO)

- Einheitliches Datenschutzniveau innerhalb der EU
- Gilt sachlich für ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten
- Sowie für die nichtautomatisierte Verarbeitung von Daten die gespeichert sind, oder gespeichert werden sollen
- Gilt räumlich für Verarbeitung durch Verantwortlichen oder Auftragsverarbeiter mit Niederlassung innerhalb der EU; unabhängig davon ob die Verarbeitung innerhalb der EU stattfindet
- Gilt räumlich auch für Verarbeitung personenbezogener Daten, sofern das jeweilige Angebot auf den europäischen Markt („Marktort“) gerichtet ist



Wer muss Datenschutz beachten?

- Öffentliche Stellen
- Unternehmen
- Vereine
- Verbände
- Privatpersonen
  - soweit sich der Umgang mit den personenbezogenen Daten nicht ausschließlich auf persönliche oder familiäre Zwecke beschränkt (z. B. für den privaten Terminkalender)

An wen richtet sich die Datenschutzgrundverordnung (DSGVO)?

Verantwortlicher
ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Sie ist für die Einhaltung der gesetzlichen Bestimmungen zum Datenschutz verantwortlich.

Dritter
ist jede Person oder Stelle außerhalb der verantwortlichen Stelle. Der Austausch von Daten zwischen der verantwortlichen Stelle und dem Dritten bedarf einer Rechtsgrundlage

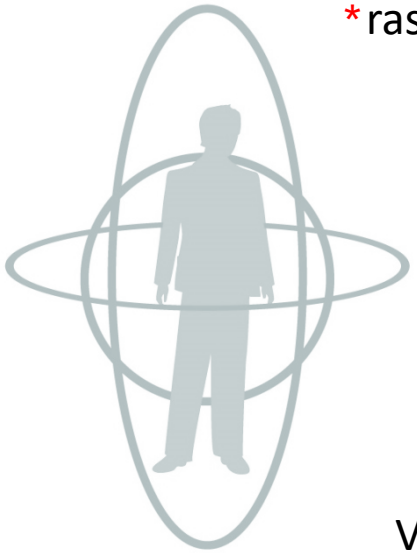
Kein Konzernprivileg
Konzerngesellschaften sind in der Regel untereinander Dritte. Sie dürfen nur bei Vorliegen einer entsprechenden Rechtsgrundlage Daten austauschen.
In Ihrem Unternehmen gilt dies in der Regel auch für den Datenaustausch zwischen zwei Gesellschaften

Welche Daten werden geschützt?

- Die Datenschutzgrundverordnung gilt, wenn es um „personenbezogene Daten“ geht.
- Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen
- Der Datenschutz umfasst ausschließlich natürliche Personen, das heißt Menschen aus Fleisch und Blut. Juristische Personen werden nicht geschützt.
- Die natürliche Person (Betroffener) muss bestimmt oder bestimmbar sein, das heißt die Informationen sind unmittelbar oder mit verfügbarem Zusatzwissen der Person zuzuordnen.
- Geschützt werden alle Informationen, die etwas über die Bezugsperson aussagen.

Welche Daten werden geschützt? Beispiele für personenbezogene Daten

Name
Foto
Einkommen
Vermögen
*rassische/ethnische Herkunft
*politische Meinung
Geburtsdatum
E-Mail-Adresse
Anschrift
Ausbildung/Beruf
IP-Adresse
Telefonnummer
Bankverbindung
Familienstand
*Sexualleben
*Religion
*Gesundheitsdaten
Personalnummer
Versicherungen



* Genetische Daten
*Gewerkschaftszugehörigkeit
* Biometrische Daten

* Besondere Kategorien personenbezogener Daten, die aufgrund ihrer Sensibilität besonders schützenswert sind.

Welche Datenarten gibt es?

Häufig treffen Sie folgende Datenarten an:

- Mitarbeiterdaten: z. B. Adresse, Sozialdaten, Arbeits-zeiten, Ausbildung, Fähigkeiten, Arbeitszeugnisse
- Kundendaten: z. B. Adresse, Bankverbindung, Bonität, Vertragsverhältnisse, Zahlungsverhalten
- Lieferantendaten: z. B. Adresse, Bankverbindung

In welcher Form kommen personenbezogene Daten vor?

- Papier, Akte
- Gesprochenes Wort,
- Bildliche Darstellung (z. B. Video, Fotos)
- Digitale Form (z. B. Word-/Excel-Dokumente)

Welcher Datenumgang wird vom Datenschutzrecht erfasst?

- Die EU-Datenschutzgrundverordnung und das Bundesdatenschutzgesetz gelten, wenn personenbezogene Daten erhoben, verarbeitet werden, oder genutzt werden - unabhängig davon, ob dies elektronisch oder in anderer Form erfolgt.

- Verarbeitung meint 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;

Welcher Datenumgang wird vom Datenschutzrecht erfasst?

- Erheben ist das Beschaffen von Daten des Betroffenen
- Speichern ist jedes Fixieren von Daten auf Datenträger, z. B. auch das Schreiben auf ein Stück Papier.
- Verändern meint, dass Daten einen neuen Informations-/Aussagegehalt erhalten.
- Übermitteln bedeutet, dass die Daten einem Dritten bekanntgegeben werden.
- Sperren heißt, dass die Daten gekennzeichnet werden, um die weitere Verarbeitung einzuschränken.
- Löschen bedeutet die Unkenntlichmachung der Daten dergestalt, dass der Informations-/ Aussagegehalt nicht mehr vorhanden/ unlesbar ist, z. B. physische Vernichtung, Überschreiben, Durchstreichen.“

Grundprinzipien der Datenverarbeitung (1)

- Jede Verarbeitung von personenbezogenen Daten bedarf einer gesetzlichen Rechtfertigung. Bei der Erhebung der Daten ist außerdem der Zweck, für den die Daten verarbeitet werden sollen, konkret festzulegen.

- Erlaubnisse zur Verarbeitung personenbezogener Daten nach **DSGVO** sind:
  - Die Einwilligung des Betroffenen, welche freiwillig und nachweisbar sein muss. Ein Vertrag darf nicht von einer Einwilligung abhängig gemacht werden (Kopplungsverbot).
  - Zur Erfüllung eines Vertrages oder einer vorvertraglichen Maßnahme
  - Zur Erfüllung einer rechtlichen Verpflichtung
  - Zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht die Interessen der betroffenen Person überwiegen
  - Bei Datenverarbeitung zu neuen Zwecken, wenn diese mit dem ursprünglichen Zweck kompatibel sind

Grundprinzipien der Datenverarbeitung (2)

- Das **BDSG** ergänzt die Erlaubnistatbestände der EU.DSGVO zur:
  - Verarbeitung im Beschäftigungskontext
  - Videoüberwachung
  - Datenübermittlung an Auskunfteien
  - Zum Scoring
  - Verarbeitung bes. persönlicher Daten für Forschungszwecke
  - Verarbeitung zu anderen Zwecken

- Andere Rechtsvorschriften
  - Auch außerhalb dieser beiden gibt es Rechtsvorschriften, welche dazu berechtigen oder sogar dazu verpflichten können, Daten zu verarbeiten. Von hoher Relevanz in diesem Zusammenhang sind beispielsweise das Steuer- und Sozialversicherungsrecht für die Entgeltabrechnung.
  - Abgeschlossene Betriebs- oder Dienstvereinbarungen können ebenfalls einen Erlaubnistatbestand beinhalten und sind immer vorrangig, soweit sie den Grundsätzen der EU-DSGVO entsprechen “

Die Einwilligungserklärung

- Die Einwilligung ist nur wirksam, wenn …
  - sie auf der freien Entscheidung des Betroffenen beruht
  - sie widerrufbar ist (Widerruf muss genauso simpel wie Einwilligung selbst sein)
  - Ferner muss sie jede Phase der beabsichtigten Datenverarbeitung umfassen.
  - Der Betroffene ist auf den vorgesehenen Zweck der Erhebung, Verarbeitung oder Nutzung hinzuweisen.
  - Die Einwilligung bedarf grundsätzlich der Schriftform, in manchen Fällen kann sie auch in anderer Form, z.B. elektronisch, erfolgen.
  - Darüber hinaus ist die Einwilligung gegenüber anderen Textpassagen besonders optisch hervorzuheben.

- Liegt keine wirksame Einwilligung vor, ist die auf die Einwilligung gestützte Datenverarbeitung unzulässig. Bereits gespeicherte Daten müssen gelöscht werden

Direkterhebung beim Betroffenen

- Grundsätzlich sind die Daten direkt beim Betroffenen zu erheben. Der Betroffene ist darüber zu informieren:
  - wer die verantwortliche Stelle ist,
  - zu welchem Zweck die Daten erhoben, verarbeitet oder genutzt werden und
  - an wen die Daten weitergegeben werden.
- Ohne Mitwirkung des Betroffenen dürfen Daten nur in den gesetzlich geregelten Fällen erhoben werden. Der Betroffene ist in der Regel hierüber zu informieren.

Zweckbindung

- Personenbezogene Daten müssen:
- 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“);
- 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 Artikel 89 Absatz 1 DSGVO nicht als unvereinbar mit den ursprünglichen Zwecken
- dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein
- 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

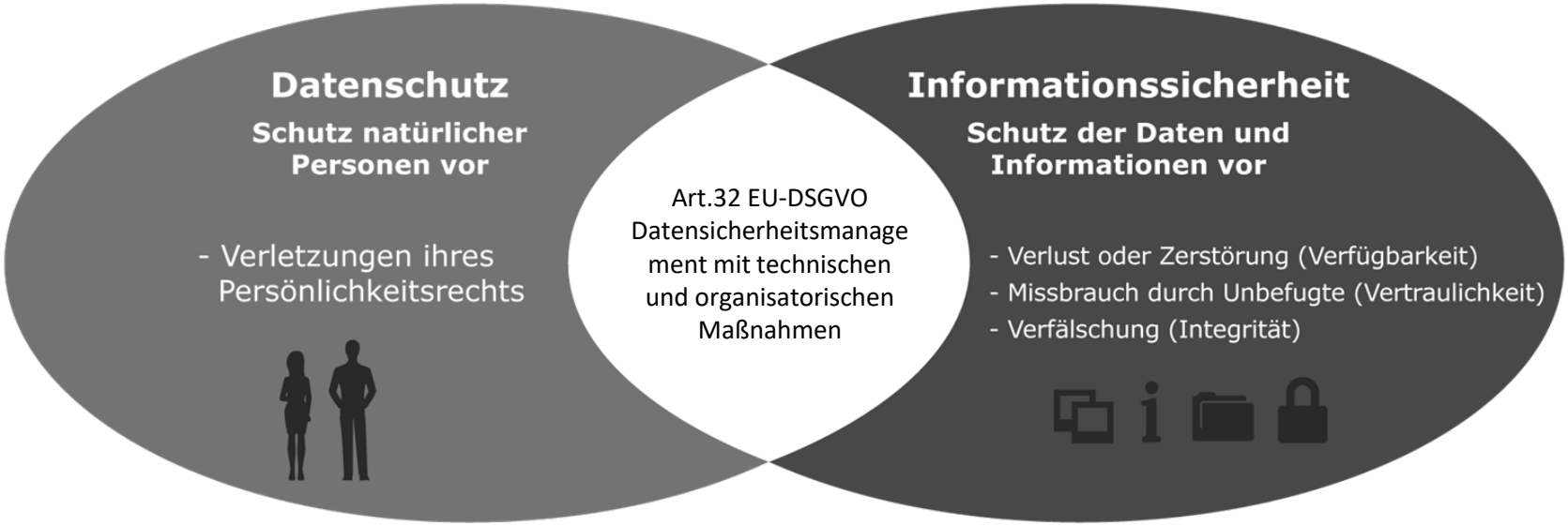
Zweckbindung

- 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; 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 Artikel 89 Absatz 1 DSGVO verarbeitet werden
- 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

Datenvermeidung und Datensparsamkeit

- Datenverarbeitungen sind an dem Ziel auszurichten:
  - keine oder so wenig wie möglich personenbezogene Daten zu erheben, zu verarbeiten oder zu nutzen. Soweit möglich, sind personenbezogene Daten zu
  - anonymisieren, das heißt die Daten können nicht oder nur mit einem unverhältnismäßig großen Aufwand einer Person zugeordnet werden, oder zu
  - pseudonymisieren, das heißt das Identifikationsmerkmal (z. B. Name) wird durch ein anderes Kennzeichen ersetzt.

Technische und organisatorische Maßnahmen



Welche Rechte hat der Betroffene?

- Jeder, dessen personenbezogene Daten erhoben, verarbeitet oder genutzt werden hat folgende Rechte:
  - Recht auf Benachrichtigung
  - Recht auf Auskunft
  - Recht auf Berichtigung
  - Recht auf Löschung
  - Recht auf Vergessen werden
  - Recht auf Einschränkung der Verarbeitung
  - Recht auf Widerspruch
  - Recht auf Datenübertragung

Welche Folgen können bei Datenschutzverstößen eintreten?

- Meldepflicht des Verantwortlichen gegenüber Betroffenen und der Aufsichtsbehörde bei unrechtmäßiger Kenntniserlangung von „Risiko“-Daten (z. B. Daten zu Bank- und Kreditkartenkonten, besondere Arten personenbezogener Daten)
- Vertrauensverlust bei Kunden, Geschäftspartnern, Mitarbeitern und Behörden

- Daneben können Datenschutzverstöße
  - Bußgelder (Geldbußen bis zu 20.000.000 Euro oder 4% des Umsatzes aus dem Vorjahr)
  - Geldstrafen, Freiheitsstrafen
  - eine Schadensersatzpflicht gegenüber den Betroffenen sowie
  - arbeitsrechtliche Sanktionen (Von der Abmahnung bis zur Kündigung)
- nach sich ziehen

Datenschutzschulung | Regelungen zum Datenschutz und zur Informationssicherheit

Wer ist in Ihrem Unternehmen für die Einhaltung des Datenschutzes und der Informationssicherheit verantwortlich?

- Die Geschäftsführung regelt die Grundlagen für die Einhaltung des Datenschutzes und der Informationssicherheit.
- Die Führungskräfte tragen die Verantwortung für die Einhaltung des Datenschutzes und der Informationssicherheit innerhalb der Organisationseinheit und deren Geschäftsprozesse.
- Alle Mitarbeiter sind wiederum für die Einhaltung des Datenschutzes und der Informationssicherheit bei der Erfüllung ihrer Aufgaben verantwortlich.
- Hierbei haben sie die Verpflichtung auf Vertraulichkeit zu wahren.
  - *Dies besagt, dass es allen Mitarbeitern, die Zugang zu personenbezogenen Daten haben, untersagt ist, personenbezogene Daten unbefugt zu erheben, zu verarbeiten oder zu nutzen. Dies gilt auch nach Beendigung ihrer Tätigkeit fort.*
  - Nur solche Personen dürfen auf die vorhandenen personenbezogenen Daten zugreifen, die dies für die Erfüllung ihrer Aufgaben benötigen.
- Grundsätzlich ist festzuhalten, dass jeder Einzelne dafür verantwortlich ist den Datenschutz zu wahren und einzuhalten.

Datenschutzschulung | Regelungen zum Datenschutz und zur Informationssicherheit

Allgemeine Anweisungen um den täglichen Datenschutz zu wahren

- Papiere mit vertraulichem Inhalt oder personenbezogenen Daten sind mit Hilfe des Aktenvernichters zu vernichten oder alternativ in dem dafür bereitgestellten Datenentsorgungsbehälter / Daten-schutztonne in der Garage zu entsorgen.
- Beim Verlassen des Arbeitsplatzes, auch kurzzeitig, ist der PC zu sperren („Windows-Taste + L“). Unbeaufsichtigte, nicht gesperrte Computer sind ein hohes Sicherheitsrisiko.
- Es ist darauf zu achten, dass Datenträger, Ausdrucke, Kopien oder auch Dokumente mit sensiblen Informationen und personen-bezogenen Daten nicht frei zugänglich für Unbefugte herumliegen, z.B. neben dem Drucker, im Kopierer oder auf dem Schreibtisch. Solche Dokumente müssen sicher verwahrt werden.

Datenschutzschulung | Regelungen zum Datenschutz und zur Informationssicherheit

Allgemeine Anweisungen um den täglichen Datenschutz zu wahren

- Am Abend, vor Verlassen des Büros, ist der Arbeitsplatz frei zu räumen. Schriftstücke oder Datenträger mit vertraulichen Inhalten sind an einem sicheren Ort (Schreibtisch oder Schrank) aufzubewahren; am besten verschlossen.
- Achten Sie auf betriebsfremde und Ihnen nicht bekannte Personen. Zögern Sie bitte nicht nach dem Beweggrund zu fragen oder ob Sie der Person behilflich sein können.

- Unternehmensrichtlinie Datenschutz
  - Diese Unternehmensrichtlinie ist die verbindliche Basis für einen rechtskonformen und nachhaltigen Schutz personenbezogener Daten im Unternehmen.
  - Mit dieser Richtlinie sollen die Persönlichkeitsrechte von Betroffenen gewahrt und geschützt werden.
  - Die Unternehmensrichtlinie Datenschutz ist für alle Beschäftigten und leitenden Angestellten jederzeit leicht zugänglich: [Pfad angeben]

Aufgaben des Datenschutzbeauftragten

- Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten hinsichtlich ihrer Pflichten nach DSGVO
- Überwachung der Einhaltung der DSGVO
- Beratung im Zusammenhang mit der Datenschutzfolgeabschätzung
- Zusammenarbeit mit der Aufsichtsbehörde
- Tätigkeit als Anlaufstelle für die Aufsichtsbehörde

Datenschutzschulung | Ihr Datenschutzbeauftragter

Ansprechpartner bei Fragen des Datenschutzes

Sebastian Feik, Dipl.-WJur. (FH)
(Datenschutzbeauftragte)

Datenschutz BackOffice der legitimis
Tel: +49 2202 28 941 - 0
Fax: +49 2202 28 941 - 47
dataprivacy-helpdesk@legitimis.com

Der Datenschutzbeauftragte ist insbesondere in folgenden Fällen einzubinden:

- Beschwerden von Betroffenen (Mitarbeitern, Kunden)
- Einführung eines neuen Systems/Tools/Verfahrens
- Einsatz eines neuen Dienstleisters (z.B. ADV-Vertrag)
- Werbemaßnahmen (z.B. Versand von Newsletter)
- Onlinemarketing-Maßnahmen (Google AdWords, Conversion Tracking, etc.)
- Auftragsverarbeitungsverhältnissen

*** Der Vollständigkeit halber sei darauf hingewiesen, dass der Datenschutzbeauftragte in seiner Funktion der Verschwiegenheit verpflichtet ist und sich so vertrauensvoll auch Ihrer persönlichen Anfragen zu Datenschutzfragen annimmt. ***

Vielen Dank für Ihre Aufmerksamkeit!