Handout zur DSGVO-Schulung

Was bedeutet die DSGVO für Unternehmen und Beschäftigte

Inhaltsverzeichnis

FOLIE 2

Was bedeutet eigentlich „Datenschutz“?

Der Begriff „Datenschutz“ weckt oft rein technische Assoziationen. Richtig ist: Datenschutz schützt mit den zu treffenden technisch-organisatorischen Maßnahmen gemäß der Anlage zu § 9 Satz 1 Bundesdatenschutzgesetz (BDSG) nicht nur technische Daten, sondern vielmehr die Privatsphäre der Menschen. Genauer gesagt das Recht jedes Einzelnen, selbst darüber zu entscheiden, wer was wann über ihn weiß. Die Umsetzung dieses „Rechts auf informationelle Selbstbestimmung“ ist das Ziel der gesetzlichen Bestimmungen des Datenschutzes – in Deutschland gilt neben den Landesdatenschutzgesetzen und beispielsweise kirchlichen Datenschutzgesetzen, insbesondere für Unternehmen das BDSG.

Experten-Know-how: *Das Recht auf informationelle Selbstbestimmung ist Teil des allgemeinen Persönlichkeitsrechts, das sich wiederum aus den Grundrechten auf freie Entfaltung der Persönlichkeit (Art. 2 Abs. 1 Grundgesetz (GG)) und der Menschenwürde (Art. 1 Abs. 1 GG) ableitet. Es wurde 1983 vom Bundesverfassungsgericht im sogenannten Volkszählungsurteil als Grundrecht anerkannt. Ihr Praxistipp: Beim Umgang mit personenbezogenen Daten ist besondere Sorgfalt geboten. Denn unsere Kunden, Geschäftspartner und Mitarbeiter vertrauen darauf, dass ihre persönlichen Daten bei uns in guten Händen und vor Missbrauch geschützt sind. Datenschutz schafft Vertrauen, sorgt für Nachhaltigkeit und fördert die Wettbewerbsfähigkeit unseres Unternehmens.*

FOLIE 3

Was genau ist die DS-GVO?

Im Mai 2018 trat eine neue europäische Datenschutzrichtlinie mit der Bezeichnung **Datenschutz-Grundverordnun**g (DSGVO) in Kraft. Diese Regulierung betrifft die Datenschutzgesetze vor Ort in allen Ländern der EU und des EWR. Sie gilt für alle Unternehmen, die Produkte an europäische Bürger verkaufen und deren personenbezogene Daten speichern, einschließlich Firmen auf anderen Kontinenten. Die neue Richtlinie gibt EU- und EWR-Bürgern mehr Kontrolle über ihre personenbezogenen Daten und stellt sicher, dass ihre Informationen europaweit geschützt sind.
Gemäß der DSGVO sind personenbezogene Daten alle Daten zu einer Person, wie Namen, Fotos, E-Mail-Adressen, Bankdaten, Beiträge in den Social Media, Angaben zum Wohnort, medizinische Daten oder IP-Adressen. Es wird nicht unterschieden zwischen personenbezogenen Daten im privaten, öffentlichen oder arbeitsbezogenen Umfeld einer Person – es geht immer um die Person selbst. Auch im B2B-Bereich geht es immer um Einzelpersonen, die Informationen mit- und übereinander austauschen. Kunden in B2B-Märkten sind natürlich Unternehmen, doch die Geschäftsbeziehungen werden von einzelnen Personen gepflegt.

FOLIE 4

Was genau sind personenbezogene Daten?

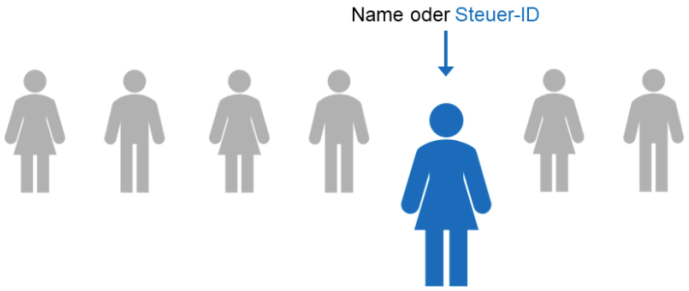
Gemäß der DSGVO sind personenbezogene Daten alle Daten zu einer Person, wie Namen, Fotos, E-Mail-Adressen, Bankdaten, Beiträge in den Social Media, Angaben zum Wohnort, medizinische Daten oder IP-Adressen. Es wird nicht unterschieden zwischen personenbezogenen Daten im privaten, öffentlichen oder arbeitsbezogenen Umfeld einer Person – es geht immer um die Person selbst. Auch im B2B-Bereich geht es immer um Einzelpersonen, die Informationen mit- und übereinander austauschen. Kunden in B2B-Märkten sind natürlich Unternehmen, doch die Geschäftsbeziehungen werden von einzelnen Personen gepflegt.

Experten-Know-how: *Zu personenbezogenen Daten zählen auch personenbeziehbare Daten. Das sind Daten, die in Kombination mit zusätzlichen Informationen Rückschlüsse auf eine bestimmte Person ziehen lassen. Dazu zählen beispielsweise Daten wie E-Mail-Adressen, Kfz-Kennzeichen oder auch IP-Adressen. Ob eine IP-Adresse wirklich den Bestimmungen des BDSG unterliegt, ist umstritten. Teilweise wird angenommen, dass statische IP-Adressen immer als personenbezogene Daten zu werten sind, dynamische hingegen nicht. Das Gegenlager geht davon aus, dass auch dynamische IP-Adressen personenbeziehbar sind, da zumindest der Access-Provider nachvollziehen kann, wem eine bestimmte IP-Adresse zu einem bestimmten Zeitpunkt zugeordnet ist.*

FOLIE 5

Was sind Personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen.



Beispiele:

Allgemeine Personendaten
Name, Geburtsdatum und Alter, Geburtsort, E-Mail-Adresse, Telefonnummer, Anschrift, Foto, Gesundheitsdaten, Ausbildung, Beruf, Familienstand, Staatsangehörigkeit, religiöse oder politische Einstellung, Sexualität, Urlaubsplanung, Vorstrafen, usf.

Kennnummern
Personalnummer, Sozialversicherungsnummer, Steueridentifikationsnummer, Kranseeversicherungsnummer, Personalausweisnummer, Matrikelnummer, usf.

Bankdaten
Kontonummer, Kreditinformation, Kontostände, Vermögen, usf.

Onlinedaten (IP-Adresse, Standort)
Benutzerkennung, Gewohnheiten, Standortdaten, usf.

Physische Merkmale
Geschlecht, Haut-, Haar- und Augenfarbe, Statur, Kleidergröße, usf.

Benutzermerkmale
Fahrzeug- und Immobilieneigentum, Grundbucheintragungen, Kfz-Kennzeichen, Zulassungsdaten, usf.

Kundendaten, Mitarbeiterdaten
Bestellungen, Adressdaten, Kontodaten, Arbeitsleistung, Verhalten in der Organisation, usf.

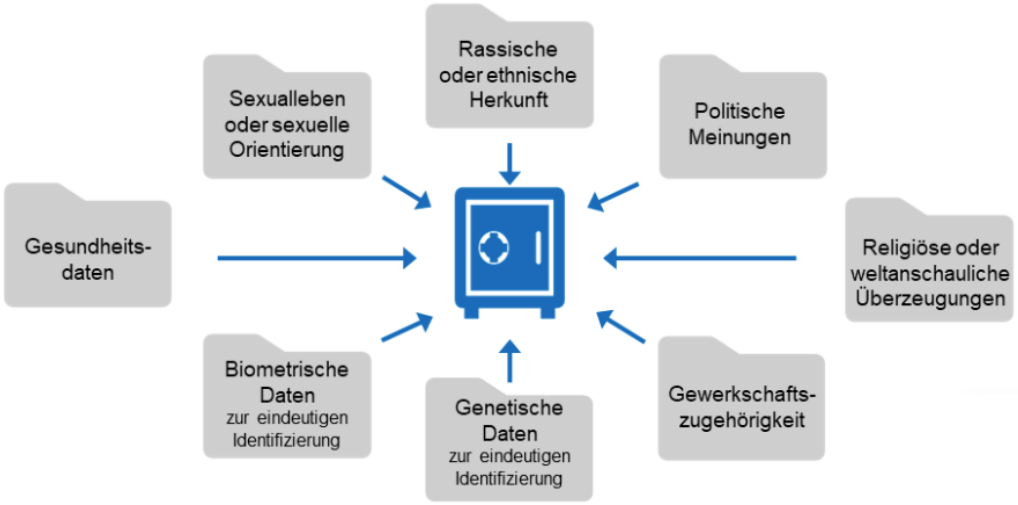
Werturteile
Schul- und Arbeitszeugnisse, usf.

Bestimmbare Daten (d.h. erst mit weiteren Informationen kann man auf eine Person rückschließen)
Personalnummer, IP-Adresse, Kfz-Nummer

FOLIE 6

Was sind Besondere Kategorien personenbezogener Daten?

Besondere Kategorien personenbezogener Daten sind (gemäß Art. 9 Abs. 1 DSGVO) Datenkategorien, die durch das Gesetz einen besonderen Schutz erfahren (sowohl juristisch als auch technisch/organisatorisch.



Die Datenschutz-Grundverordnung betrachtet personenbezogene Daten als solche besonderer Kategorien, wenn sie besonders sensibel sind und eines besonderen Schutzes bedürfen, weil ihre Verarbeitung erhebliche Risiken für die betroffenen Personen mit sich bringen kann.

Artikel 9 DSGVO (Verarbeitung besonderer Kategorien personenbezogener Daten) nennt als entsprechende personenbezogene Daten solche, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder
die Gewerkschaftszugehörigkeit hervorgehen, sowie genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder
Daten zum Sexualleben oder der sexuellen Orientierung.

Verantwortliche dürfen personenbezogene Daten besonderer Kategorien nicht verarbeiten. Es sei denn, die Verarbeitung ist in den besonderen Fällen, die Artikel 9 DSGVO nennt, zulässig.

FOLIE 7

Grundsätze der DSGVO

Der Grundsatz der DSGVO bedeutet, dass das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten grundsätzlich verboten ist.

1. Es ist für eine DSGVO-konforme Verarbeitung von personenbezogenen Daten notwendig, dass entweder eine schriftliche Einwilligung der betroffenen Person vorliegt, oder es eine Rechtsgrundlage für die Verarbeitung gibt. Bereits bei Erhebung der Daten sind Betroffene gem. Art. 13 DSGVO zu informieren.
2. Aus diesem Grund muss jede verantwortliche Stelle eine schriftliche Dokumentation, ein Verarbeitungsverzeichnis(Art. 30 DSGVO) zu führen. Diese Dokumentation zeigt schriftlich auf, wann, zu welchem Zweck und wann die Daten verarbeitet werden.
3. Auf Internetseiten muss in der vorgeschriebenen Datenschutzerklärung ebenfalls exakt dargestellt werden, wann, zu welchem Zweck und wann die Daten verarbeitet werden und stellt die Betroffenenrechte (Art. 30 DSGVO) dar.
4. Zu jeder Zeit kann ein Betroffener gem. Art. 12 Abs. 3 der DSGVO Auskunft über seine Daten mittels einer „Betroffenenanfrage“ verlangen. Diese Anfrage ist zwingend innerhalb eines Monats zu beantworten.
5. In der Dokumentation „TOM“, den technisch organisatorischen Maßnahmen, muss dargestellt werden, wie ein Unternehmen den Schutz der Daten vor Missbrauch und dem Zugriff unbefugter Dritter sicherstellt.
6. Die Datenschutzfolgeabschätzung, die DSFA, muss dann erstellt werden (Art. 35 DSGVO), wenn die Verarbeitung ein hohes Risiko für die Rechte der betroffenen Personen darstellen könnte. Ein klassisches Beispiel ist hierfür eine Videoüberwachung.

Worauf ist beim Umgang mit personenbezogenen Daten zu achten?

Grundsätzlich sind das Erheben, Verarbeiten und Nutzen von personenbezogenen Daten verboten.

Personenbezogene Daten dürfen nur dann verwendet werden, es sei denn eine von zwei Ausnahmen, greift ein.

1. eine Rechtsvorschrift dies vorsieht oder zwingend voraussetzt
2. der Betroffene freiwillig eingewilligt hat

Personenbezogene Daten dürfen nur dann verwendet werden, wenn dies ausdrücklich erlaubt ist, d. h., eine entsprechende Rechtsgrundlage vorliegt. Sollen personenbezogene Daten erhoben oder verwendet werden, muss man sich dabei auf eine Regelung aus dem Bundesdatenschutz oder aus einer anderen Rechtsvorschrift stützen können. **Natürlich kann der Betroffene auch einwilligen.**

FOLIE 8

Nach der DSGVO Art. 15 DSGVO haben Einzelpersonen folgende Rechte:

1. **Zustimmung muss erteilt werden**
   Unternehmen dürfen personenbezogene Daten nur dann verarbeiten, wenn die betreffende Person freiwillig eine spezifische, wissentliche und eindeutige Zustimmung entweder durch eine Erklärung oder aktive Bestätigung erteilt hat.

2. **Das Recht auf Zugang**
   Einzelpersonen haben das Recht, auf ihre personenbezogenen Daten zuzugreifen und zu erfahren, wie ihre Daten von dem Unternehmen, das diese Daten erfasst hat, verwendet werden. Das Unternehmen muss eine Kopie der personenbezogenen Daten kostenlos und im elektronischen Format bereitstellen, wenn die Person dies wünscht.

3. **Das Recht auf „Vergessenwerden“**
   Wenn Kunden keine Kunden mehr sind, oder wenn sie einem Unternehmen die Zustimmung zur Verwendung ihrer personenbezogenen Daten entziehen, so haben sie das Recht darauf, dass ihre Daten gelöscht werden.

4. **Das Recht auf Datenübertragbarkeit**
   Einzelpersonen haben das Recht, ihre Daten von einem Serviceanbieter auf den anderen zu übertragen. Die Übertragung muss in einem gängigen und maschinenlesbaren Format erfolgen.

5. **Das Informationsrecht**
   Dies gilt für jede Erfassung von Daten durch Unternehmen. Einzelpersonen müssen informiert werden, bevor Daten gesammelt werden. Verbraucher müssen der Erfassung ihrer Daten zustimmen und die Zustimmung muss ausdrücklich und nicht stillschweigend erteilt werden.

6. **Das Recht auf Berichtigung**
   Einzelpersonen können ihre Daten berichtigen lassen, wenn diese veraltet, unvollständig oder falsch sind.

7. **Das Recht auf Einschränkung**
   Einzelpersonen können verlangen, dass ihre Daten nicht weiterverarbeitet werden. Der Datensatz bleibt bestehen, wird aber nicht verwendet.

8. **Das Recht auf Einspruch**
   Einzelpersonen haben das Recht, gegen die Verwendung von Daten für direktes Marketing Einspruch einzulegen. Diese Regelung gilt ausnahmslos. Sobald der Antrag vorliegt, dürfen die Daten nicht mehr verwendet werden. Ebenso muss dieses Recht Einzelpersonen von vornherein mitgeteilt werden.

9. **Das Recht auf Benachrichtigung**
   Wenn es zu einer Verletzung der Datensicherheit kommt, die die personenbezogenen Daten betreffen, hat die betroffene Person das Recht, innerhalb von 72 Stunden, nachdem die Verletzung bekannt wurde, informiert zu werden.

10. **Das Recht auf Beschwerde bei der Aufsichtsbehörde**
    Jede betroffene Person das Recht auf Beschwerde bei einer Aufsichtsbehörde, insbesondere in dem Mitgliedstaat ihres gewöhnlichen Aufenthaltsorts, ihres Arbeitsplatzes oder des Orts des mutmaßlichen Verstoßes, wenn die betroffene Person der Ansicht ist, dass die Verarbeitung der sie betreffenden personenbezogenen Daten gegen diese Verordnung verstößt.

11. **Das Auskunftsrecht**
    Die betroffene Person hat das Recht, von dem Verantwortlichen eine Bestätigung darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden; ist dies der Fall, so hat sie ein Recht auf Auskunft über diese personenbezogenen Daten.

12. **Das Recht auf Löschung**
    Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende personenbezogene Daten unverzüglich gelöscht werden, und der Verantwortliche ist verpflichtet, personenbezogene Daten unverzüglich zu löschen.

13. **Das Recht auf Widerruf einer Einwilligung**
    Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmäßigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt. Die betroffene Person wird vor Abgabe der Einwilligung hiervon in Kenntnis gesetzt. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

14. **Das Recht auf Mitteilung von Berichtigungen, Löschun- gen, Einschränkungen an Empfänger**
    Der Verantwortliche teilt allen Empfängern, denen personenbezogenen Daten offengelegt wurden, jede Berichtigung oder Löschung der personenbezogenen Daten oder eine Einschränkung der Verarbeitung nach Artikel 16, Artikel 17 Absatz 1 und Artikel 18 mit, es sei denn, dies erweist sich als unmöglich oder ist mit einem unverhältnismäßigen Aufwand verbunden. Der Verantwortliche unterrichtet die betroffene Person über diese Empfänger, wenn die betroffene Person dies verlangt.

Mit der DSGVO gibt die EU Einzelpersonen, Interessenten, Kunden, Lieferanten und Mitarbeitern mehr Kontrolle über ihre Daten. Die Kontrolle der Unternehmen, die diese Daten zu kommerziellen Zwecken erfassen und verwenden, wird damit geringer. Es ist nicht das Ziel der Verordnung, Geschäfte zu unterbinden oder zu erschweren. Vielmehr sollen die Aufbewahrung und Verwendung personenbezogener Daten transparenter werden.

FOLIE 9

Wer ist für den Datenschutz im Unternehmen verantwortlich?

Die Gesamtverantwortung zum Datenschutz liegt bei der Unternehmensleitung. Aber auch jeder einzelne Mitarbeiter ist verantwortlich dafür, mit personenbezogenen Daten sorgfältig umzugehen und die Regelungen und Bestimmungen des Datenschutzes bei seiner täglichen Arbeit umzusetzen. Unter anderem hat sich jeder Mitarbeiter zur Wahrung des Datengeheimnisses (§ 5 BDSG) verpflichtet. Die Umsetzung des Datenschutzes im Unternehmen zu fördern, liegt in der Verantwortung des Datenschutzbeauftragten.

FOLIE 10

Datenschutz praktisch durch alle Beschäftigten:

Mehr Datenschutz durch …

1. **Trennung von Arbeit und Privatleben**
   Eine strikte Trennung von Arbeit und Privatleben. Weder eine private Nutzung von E-Mail und Internet, noch das Verwenden von privaten Daten oder Software im Büro sind erlaubt. Auch dürfen private Datenträger oder Geräte nicht angeschlossen werden!

2. **richtiges Entsorgen**
   a. Papierdokumente oder elektronische Datenträger, die personenbezogene oder sonstige schutzbedürftige Informationen enthalten, sind keinesfalls im normalen Hausmüll zu entsorgen. Für die Entsorgung gilt Folgendes:
      - Papierdokumente wie Akten, Ausdrucke etc. sind im Schredder (mind. Sicherheitsstufe P4) zu entsorgen.
      - Digitale Datenträger wie USB-Sticks. CD-ROMs etc. kommen in den dafür vorgesehenen, verschließbaren Behälter, dessen Inhalt regelmäßig von einem Dienstleister fachgerecht entsorgt wird.

3. **Ordnung**
   a. Chaos und Unordnung am Arbeitsplatz erschweren nicht nur die Arbeit: Es besteht auch die Gefahr, dass Dokumente mit schützenswerten Informationen verloren gehen oder in die falschen Hände geraten. Achten Sie also auf Folgendes:
   b. Dokumente/Aktenordner/Ausdrucke nicht auf dem Tisch deponieren, sondern direkt nach Gebrauch wegräumen.
   c. Keine Handys/Smartphones oder mobile Datenträger wie USB-Sticks offen liegen lassen.

4. **Wegschließen**
   a. Dokumente, Ordner und Datenträger, die schützenswerte Informationen, wie vertrauliche Inhalte und personenbezogene Daten enthalten, müssen angemessen vor dem Zugriff Unbefugter geschützt werden. Deshalb gilt:
   b. Nutzen Sie zum Verstauen von vertraulichen Unterlagen nur Schränke, die mit einem entsprechenden Sicherheitsschloss ausgestattet sind.
   c. Verschließen Sie – zumindest in Bereichen, in denen besondere Sicherheitsvorkehrungen zu treffen sind (z. B. Geschäftsleitung, Personalwesen, IT-Abteilung)

d. die Tür Ihres Büroraums bei Ihrer Abwesenheit.

5. **Vertraulichkeit bei Gesprächen**
   a. Im Bundesdatenschutzgesetz ist geregelt, dass Mitarbeiter nur Zugriff auf Daten haben dürfen, die für ihre Arbeit unbedingt erforderlich sind. Das bedeutet auch:
   b. Führen Sie keine (Telefon-)Gespräche mit vertraulichem, schutzbedürftigem Inhalt an öffentlichen Orten.
   c. Sorgen Sie im Vorfeld jedes vertraulichen Gesprächs dafür, dass kein Unbefugter Ihr Gespräch mithören kann, und ziehen Sie sich dafür an einen geeigneten Ort zurück.

6. **Besuchermanagement**
   a. Möchten Sie Besuch von externen Gästen auf dem Unternehmensgelände empfangen, gehen Sie folgendermaßen vor:
   b. Melden Sie Besucher beim Empfang mit Namen und Termin an und lassen Sie Besucherausweise erstellen.
   c. Achten Sie darauf, dass Ihr Besucher das Unternehmen nicht im Alleingang erkundet, und begleiten Sie Ihren Besucher während seines gesamten Aufenthalts auf dem Unternehmensgelände.

7. **richtigen Umgang mit dem Computer**
   a. Ihr Computer ist eines Ihrer wichtigsten Arbeitsgeräte. Sorgen Sie dafür, dass sich kein Unbefugter Zugriff auf Ihren Computer verschaffen kann:
   b. Sperren Sie beim Verlassen Ihres Arbeitsplatzes immer den Bildschirm Ihres Computers – auch bei vermeintlich kurzen Abwesenheiten.
   c. Fahren Sie den Computer nach Feierabend komplett herunter und entfernen Sie zuvor USB-Sticks oder andere Datenträger.
   d. Lassen Sie Ihren Computer auf Geschäftsreisen niemals unbeaufsichtigt.

8. **sicheres Drucken**
   a. Um zu gewährleisten, dass Dokumente, die Sie ausdrucken möchten, nicht in die Hände unbefugter Personen geraten, nutzen Sie die Option „Sicheres Drucken“. Diese richten Sie folgendermaßen ein:
   b. Wählen Sie unter „Drucker“ die Option „Eigenschaften“ aus.
   c. Dort vergeben Sie Ihrem Druckauftrag ein Kennwort.
   d. Am Druckergerät geben Sie dann zur Aktivierung Ihres Druckauftrags Ihr Kennwort ein.

9. **sichere Passwörter**
   a. Passwörter sind der Schlüssel zu sämtlichen personenbezogenen Daten und schutzbedürftigen Informationen. Um den Zugriff Unbefugter zu verhindern, beachten Sie Folgendes:
   b. Nutzen Sie ausschließlich sichere, idealerweise mindestens 10-stellige Passwörter mit einer Kombination aus Groß- und Kleinbuchstaben, Ziffern und Sonderzeichen.
   c. Verwenden Sie für jede Anwendung ein anderes Passwort. Geben Sie Ihre Passwörter an niemanden weiter. Im Datenschutzordner finden Sie einen „Password-Guide“ zur Einsicht!

DSGVO Begriffe

1) Betroffene Person
Eine betroffene Person ist eine natürliche Person. Beispiele für eine betroffene Person können eine Person, ein Kunde, ein Interessent, ein Mitarbeiter, eine Kontaktperson usw. sein.

2) Personenbezogene Daten
Alle Informationen in Bezug auf eine identifizierte / identifizierbare Person, unabhängig davon, ob sie sich auf ihr oder sein privates, berufliches oder öffentliches Leben beziehen. Kann ein Name, ein Foto, eine E-Mail-Adresse, Bankdaten, Posts auf sozialen Netzwerken, medizinische Informationen, IP-Adressen oder eine Kombination der Daten sein, die die Person direkt oder indirekt identifizieren.

3) Besondere Kategorien personenbezogener Daten
Die DSGVO bezieht sich auf Besondere Kategorien personenbezogener Daten als „spezielle Kategorien personenbezogener Daten". Zu den besonderen Datenkategorien gehören rassische oder ethnische Herkunft, politische Meinungen, religiöse oder philosophische Ansichten, Gewerkschaftszugehörigkeit, sexuelle Orientierung sowie Gesundheitsdaten, genetische und biometrische Daten, die verarbeitet wurden, um eine Person eindeutig zu identifizieren. Personenbezogene Daten in Bezug auf strafrechtliche Verurteilungen und Straftaten sind nicht enthalten, aber für ihre Verarbeitung gelten ähnliche zusätzliche Schutzmaßnahmen.

4) (Daten)Verantwortlicher
Jede Organisation, Person oder Stelle, die Zwecke und Mittel zur Verarbeitung personenbezogener Daten bestimmt, kontrolliert die Daten und ist allein oder gemeinsam für diese verantwortlich. Beispiele für den Datenverantwortlichen sind Allgemeinmediziner, Apotheker und Politiker, die personenbezogene Informationen über ihre Patienten, Kunden, Mitgliedsgruppen usw. aufbewahren. Beispiele für Organisationen können Datenverantwortliche sein, die entweder zur Gewinnerzielung oder als nicht kommerzielle Organisation, privat oder staatlich, Groß- oder Kleinunternehmen, personenbezogene Informationen über ihre Mitarbeiter, Kunden usw. führen.

5) Datenauftragsverarbeiter
Ein Datenauftragsverarbeiter verarbeitet die Daten im Namen des Datenverantwortlichen. Beispiele sind Lohn- und Gehaltsabrechnungsunternehmen, Buchhalter und Marktforschungsunternehmen.

6) DSB
Die Ernennung eines Datenschutzbeauftragten ist obligatorisch, wenn: (1) die Verarbeitung durch eine Behörde erfolgt; oder (2) die „Kerntätigkeiten" eines Datenverantwortlichen / Datenauftragsverarbeiters entweder „die regelmäßige und systematische Überwachung der betroffenen Personen in großem Umfang" erfordern oder aus der Verarbeitung besonderer Kategorien von Daten oder Daten über strafrechtliche Verurteilungen „in großem Umfang" bestehen. Wenn der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vornehmen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DSGVO unterliegen.

7) Rechenschaftspflicht
Rechenschaftspflicht ist die Fähigkeit, die Einhaltung der DSGVO nachzuweisen. In der Verordnung heißt es ausdrücklich, dass dies die Verantwortung der Organisation ist. Um die Einhaltung nachzuweisen, müssen geeignete technische und organisatorische Maßnahmen umgesetzt werden. Best-Practice-Tools wie Datenschutz-Folgeabschätzungen und eingebauter Datenschutz sind nun unter bestimmten Umständen gesetzlich vorgeschrieben.

8) Einwilligung
Einwilligung ist jede „frei gegebene, spezifische, informierte und eindeutige“ Angabe der Wünsche des Einzelnen, durch die die betroffene Person entweder durch eine Erklärung oder durch eine eindeutige bestätigende Handlung eine Einwilligung in die Verarbeitung der ihr zugehörigen personenbezogenen Daten zu einem oder mehreren Zwecke/n gibt.
Die zustimmende Maßnahme oder ein positives Opt-in bedeutet, dass die Zustimmung nicht aus Stillschweigen, vorangekreuzten Feldern oder Inaktivität abgeleitet werden kann. Es sollte von den Geschäftsbedingungen getrennt sein und auf einfache Art zu widerrufen sein. Behörden und Arbeitgeber müssen besonders darauf achten, dass die Zustimmung freiwillig gegeben wird.
Die bestehenden Zustimmungen müssen nicht automatisch in der Vorbereitung auf die DSGVO aktualisiert werden, aber sie müssen den DSGVO Standard erfüllen und spezifisch, detailliert, klar, eindeutig und ordnungsgemäß dokumentiert sein und einfach zu widerrufen sein. Wenn dies nicht der Fall ist, ändern Sie Ihre Einwilligungsmechanismen und bitten Sie um eine neue, der DSGVO entsprechende Einwilligung oder finden Sie eine Alternative zur Einwilligung.

9) Datenschutz-Folgenabschätzung (DSFA)
Die DSGVO schreibt für Datenverantwortliche und Datenauftragsverarbeiter eine neue Verpflichtung zur Durchführung einer Datenschutz-Folgenabschätzung (auch als Datenschutz-Verträglichkeitsprüfung, oder DSFA bekannt) vor, bevor sie eine Verarbeitung vornimmt, die aufgrund ihrer Art, ihres Umfangs oder Zweckes ein Risiko für die Privatsphäre darstellt.

10) Verarbeitung
Verarbeitung ist jede Tätigkeit, die an personenbezogenen Daten (Sets) durchgeführt wird, wie z. B. Erstellung, Sammlung, Speicherung, Ansicht, Transport, Verwendung, Änderung, Übertragung, Löschung usw., unabhängig davon, ob dies automatisiert erfolgt oder nicht.

11) Profiling
Profiling ist jede Form der automatisierten Verarbeitung personenbezogener Daten, die bestimmte personenbezogene Aspekte des Einzelnen bewerten oder die Leistung dieser Person bei der Arbeit, die wirtschaftliche Situation, den Standort, die Gesundheit, persönliche Vorlieben, Zuverlässigkeit oder Verhalten analysieren oder vorhersagen sollen.

12) Subjektzugriff
Das Recht der betroffenen Person, vom Datenverantwortlichen auf Anfrage bestimmte Informationen bezüglich der Verarbeitung ihrer personenbezogenen Daten einzuholen.

13) Räumlicher Anwendungsbereich
Der räumliche Anwendungsbereich der DSGVO umfasst den Europäischen Wirtschaftsraum (EWR – alle 27 EU-Mitgliedstaaten), Island, Liechtenstein und Norwegen, aber nicht die Schweiz. Durch einen Angemessenheitsbeschluss gehört die Großbritannien zu einem sicheren Drittland.

14) Dritter
Ein Dritter ist jede natürliche oder juristische Person, öffentliche 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 Daten zu verarbeiten.

15) Übermittlung
Die Übermittlung personenbezogener Daten an Länder außerhalb des EWR oder an internationale Organisationen unterliegt Beschränkungen. Wie bei der Datenschutzrichtlinie müssen Daten nicht physisch transportiert werden, um übertragen zu werden. Die Anzeige von Daten, die an einem anderen Ort gehostet werden, würde eine Übermittlung für Zwecke der DSGVO bedeuten.

16) Privacy by Default
Privacy by Default heißt übersetzt „Datenschutz durch datenschutzfreundliche Voreinstellungen“ und bedeutet, dass die Werkeinstellungen datenschutzfreundlich auszugestalten sind. Nach dem Grundgedanken sollen insbesondere die Nutzer geschützt werden, die weniger technikaffin sind und z.B. dadurch nicht geneigt sind, die datenschutzrechtlichen Einstellungen ihren Wünschen entsprechend anzupassen. Dieser Gedanke steht hinter dem Begriff „Privacy Paradox“, wonach Nutzer grundsätzlich den Schutz ihrer Privatsphäre befürworten, aber nicht aktiv entsprechende Einstellungen vornehmen.

17) Privacy by Design
Übersetzt heißt Privacy by Design „Datenschutz durch Technikgestaltung“ und greift den Grundgedanken auf, dass sich der Datenschutz am besten einhalten lässt, wenn er bereits bei Erarbeitung eines Datenverarbeitungsvorgangs technisch integriert ist. In anderen Worten: der Schutz personenbezogener Daten im Sinne der DSGVO erfolgt durch das frühzeitige Ergreifen technischer und organisatorischer Maßnahmen (TOMs) im Entwicklungsstadium.

18) Dateisystem
Ein „Dateisystem“ ist jede strukturierte Sammlung personenbezogener Daten, die nach bestimmen, Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird. Das Dateisystem kann automatisiert oder manuell geführt werden (Technologie-neutral). Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind, fallen nicht in den Anwendungsbereich der DSGVO.

19) ToM – technisch organisatorische Maßnahmen
Unter **technischen Maßnahmen** sind alle Schutzversuche zu verstehen, die im weitesten Sinne physisch umsetzbar sind, wie etwa

1) Umzäunung des Geländes
2) Sicherung von Türen und Fenstern
3) bauliche Maßnahmen allgemein
4) Alarmanlagen jeglicher Art

oder Maßnahmen, die in Soft- und Hardware umgesetzt werden, wie etwa
Benutzerkonto

1) Passworterzwingung
2) Logging (Protokolldateien)
3) biometrische Benutzeridentifikation

Als **organisatorische Maßnahmen** sind solche Schutzversuche zu verstehen, die durch Handlungsanweisung, Verfahrens- und Vorgehensweisen umgesetzt werden. Beispiele hierfür sind

1) Besucheranmeldung
2) Arbeitsanweisung zum Umgang mit fehlerhaften Druckerzeugnissen
3) Vier-Augen-Prinzip
4) festgelegte Intervalle zur Stichprobenprüfungen

20) Meldepflicht

Sollte der Schutz personenbezogener Daten verletzt worden sein, z.B. durch eine Datenpanne, muss das Unternehmen dies innerhalb von 72 Stunden der Aufsichtsbehörde melden. Allerdings besteht diese Pflicht nicht, wenn diese „Datenpanne“ voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

FOLIE 13

Einsicht in den Datenschutz Dokumentation

In Ihrem Unternehmen wird eine Datenschutzmanagementsoftware eingesetzt “PRO-DSGVO guide” in dieser Software finden Sie alle wichtigen Informationen und Dokumentation zum „Datenschutz“. Sie können jederzeit in die Software einsehen. Der Zugang wird Ihnen auf Wunsch von der Geschäftsführung zur Verfügung gestellt.

FOLIE 14

Vielen Dank für Ihre Aufmerksamkeit.

Die Inhalte der Präsentation erhalten Sie noch als Handout. In diesem Handout finden Sie noch weitere und ausführliche Informationen zu einzelnen Punkten.

Bitte unterschreiben Sie unbedingt noch die Bestätigung über Ihre Teilnahme an dieser Datenschutz-Schulung.