Handout zur DSGVO-Schulung

Was bedeutet die DSGVO für Unternehmen und Beschäftigte

Inhaltsverzeichnis

FOLIE 3

Überblick zur Datenschutz-Grundverordnung (DSGVO)

In den Jahren vor Einführung der DSGVO (2018) wurde die Forderung nach einer Neuordnung des europäischen Datenschutzrechts immer lauter. Dies hatte vielseitige Gründe. Zum einen konnten die Vorschriften der (zuvor gültigen) Datenschutzrichtlinie den rasanten technologischen Entwicklungen, dem Internet und der Globalisierung nicht mehr gerecht werden. Zum anderen legte die Datenschutzrichtlinie für die nationalen Gesetzgeber nur einen datenschutzrechtlichen Mindeststandard fest, der als Orientierung diente. Das Ergebnis war, trotz angestrebter Harmonisierung, ein uneinheitliches Datenschutzniveau in Europa mit einem Flickenteppich verschiedener mitgliedstaatlicher Regelungen. Infolgedessen herrschte eine zunehmende Rechtsunsicherheit, welche als Hemmnis für einen freien Waren – und Dienstleistungsverkehr innerhalb Europas angesehen wurde. Daher einigte sich die Europäische Union auf eine umfassende Reform ihres Datenschutz-Rechtsrahmens und verabschiedete am 24. Mai 2016 die sogenannte Datenschutz-Grundverordnung. Diese gilt allerdings erst seit dem 25. Mai 2018 verbindlich, um den Mitgliedstaaten sowie den Unternehmen eine gewisse Umsetzungszeit einzuräumen. Zum gleichen Zeitpunkt trat die Datenschutzrichtlinie außer Kraft.

FOLIE 4

Zweck und Ziele der DSGVO

Die Datenschutz-Grundverordnung hat zwei wesentliche Ziele. Wie aus Artikel 1 Abs. 2 der DS-GVO hervorgeht, ist das erste wesentliche Ziel, *„...die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf den Schutz ihrer personenbezogenen Daten“* sicherzustellen. Dieses Persönlichkeitsrecht wird dabei auch als „Recht auf informationelle Selbstbestimmung“ bezeichnet. Damit ist gemeint, dass jede natürliche Person das Recht besitzt, selbst über die Preisgabe und Verwendung ihrer persönlichen Daten zu entscheiden und wie sie sich in der Öffentlichkeit darstellen möchte. Bereits in Artikel 2 Abs. 1 GG steht: *„Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer verletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.“* In Verbindung mit Artikel 1 Abs. 1 GG „Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlicher Gewalt“, hat das Bundesverfassungsgericht bereits im Volkszählungsurteil dieses Recht etabliert. Mit dem Urteil dieser Rechtsprechung bekommt der Schutz personenbezogener Daten die Qualität eines Grundrechts. Trotz des hohen Schutzziels der Verordnung, ist der Schutz der pbD kein uneingeschränktes Recht, sondern muss gegen andere Grundrechte abgewogen werden.
Das zweite wesentliche Ziel ergibt sich aus Artikel 1 Abs. 3 DS-GVO. Darin ist festgehalten, dass die Vorschriften der Verordnung den freien Verkehr personenbezogener Daten innerhalb der EU schützen und gewährleisten sollen. Dies ist besonders für die Vollendung des digitalen Binnenmarktes und für gleiche Wettbewerbsbedingungen eine wichtige Voraussetzung. Somit verfolgt die Datenschutz-Grundverordnung den Zweck bzw. das übergeordnete Ziel, innerhalb der EU und unter Wahrung der Verhältnismäßigkeit, zwischen dem Schutz und dem freien Verkehr der personenbezogenen Daten abzuwägen.

Mit der DSGVO gibt die EU Einzelpersonen, Interessenten, Kunden, Lieferanten und Mitarbeitern mehr Kontrolle über ihre Daten. Es ist nicht das Ziel der Verordnung, Geschäfte zu unterbinden oder zu erschweren. Vielmehr sollen die Aufbewahrung und Verwendung personenbezogener Daten transparenter werden.

FOLIE 5

Wann findet die DSGVO Anwendung?

Ob und in welchem Umfang die Datenschutz-Grundverordnung überhaupt Anwendung findet, lässt sich in der Praxis nicht abstrakt und generell beantworten. Vielmehr ist der spezifische Kontext der Verarbeitung entscheidend. Diesbezüglich wird in der DS-GVO zwischen dem sachlichen und räumlichen Anwendungsbereich unterschieden. Sofern beide Anwendungsbereiche geöffnet sind, müssen die Regelungen der DS-GVO in der betrieblichen Praxis angewandt werden. Im Folgenden wird genauer auf die jeweiligen Anwendungsbereiche eingegangen und in diesem Zusammenhang zentrale Begriffe des Datenschutzes erläutert.

FOLIE 6

Sachlicher Anwendungsbereich

Nach Artikel 2 Abs. 1 DSGVO gilt die Datenschutz-Grundverordnung *„...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.“*
Der Begriff „Verarbeitung“ bezeichnet in der DS-GVO dabei jeden Vorgang oder jede Vorgangsreihe, die mit oder ohne Hilfe automatisierter Verfahren und in Zusammenhang mit personenbezogenen Daten erfolgt. Dazu gehört *„...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)
Darüber hinaus spielen weder die Dauer noch die Intensität der Verarbeitung eine Rolle, sprich selbst eine kurzzeitige und scheinbar unbedeutende Verwendung personenbezogener Daten fällt in den Anwendungsbereich der DS-GVO.
In einem nächsten Schritt muss überprüft werden, ob die Daten zur Speicherung in einem „Dateisystem“ bestimmt sind, damit der sachliche Anwendungsbereich erfasst wird. Dieses definiert Artikel 4 Nr. 6 DS-GVO als „...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.“ Nach Erwägungsgrund 15 DS-GVO sind lediglich unstrukturierte Akten oder Aktensammlungen sowie ihre Deckblätter vom Anwendungsbereich der Verordnung ausgenommen. Da in der Praxis allerdings nur in den seltensten Fällen ungeordnete Datensammlungen vorzufinden sind, dürfte diese Ausnahme eine eher untergeordnete Rolle spielen.

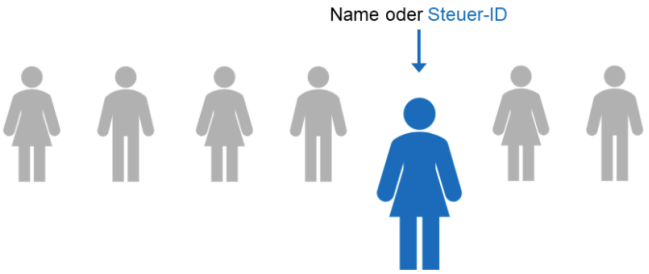
FOLIE 7

Der wichtigste Regelungsgegenstand der Datenschutz-Grundverordnung ist schließlich die Verarbeitung personenbezogener Daten. Dabei handelt es sich gemäß Artikel 4 Nr. 1 DS-GVO um *„alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen“.* Die Identifizierbarkeit wird dann angesehen, wenn eine natürliche Person „direkt oder indirekt“ identifiziert werden kann. Der europäische Gesetzgeber stellt außerdem klar, dass die Identifizierbarkeit grundsätzlich von der Berücksichtigung aller Mittel abhängt, die *„...nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren.“* In diesem Zusammenhang sollten alle objektiven Faktoren wie Kosten, erforderlicher Zeitaufwand, zum Zeitpunkt der Verarbeitung verfügbare Technologien und technologische Entwicklungen einbezogen werden.

Experten-Know-how: Im Rahmen der Identifizierbarkeit wird in der DS-GVO zwischen anonymen, anonymisierten und pseudonymisierten Daten unterschieden. Dieser Unterscheidung kommt mit Hinblick auf die Erfassung des sachlichen Anwendungsbereichs ebenfalls eine Bedeutung zu. Unter anonymen Daten werden im Allgemeinen Einzelangaben über eine Person angesehen, die dieser von niemandem mehr zugeordnet werden können. In Ergänzung dazu gelten personenbezogene Daten als anonymisiert, wenn sie derart verändert wurden, dass die Einzelangaben nicht mehr oder nur mit unverhältnismäßig großem Aufwand einer natürlichen Person zugeordnet werden können. Nach Erwägungsgrund 26 DS-GVO findet die Verordnung bei personenbezogenen Daten in anonymer/anonymisierter Art sodann keine Anwendung. In der Praxis kann, aufgrund der heute zur Verfügung stehenden Informationstechnologien, die Abgrenzung von anonymen/anonymisierten zu identifizierbaren Daten im Einzelfall jedoch durchaus Schwierigkeiten bereiten. Daher ist regelmäßig zu überprüfen, ob im Laufe der Zeit erworbenes Zusatzwissen und bessere Verknüpfungsmöglichkeiten, eine Identifizierbarkeit der anonymen Daten weiterhin ausschließen. Andernfalls greifen ab diesem Zeitpunkt wieder die Vorschriften der Datenschutz-Grundverordnung und es besteht die Gefahr einer rechtswidrigen Verarbeitung.
Von einer Pseudonymisierung hingegen wird gesprochen, wenn „die Verarbeitung personenbezogener Daten in einer Weise“ erfolgt, „...dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können.“ Im Zuge dessen erfolgt die Pseudonymisierung der Daten i.d.R dadurch, dass in einem Datenbestand das Identifizierungsmerkmal einer Person (z.B. Name) durch ein Kennzeichen („Pseudonym“) ersetzt wird. Gemäß Art. 4 Nr. 5 DS-GVO ist es darüber hinaus zwingend erforderlich, dass solche zusätzlichen Informationen, beispielsweise eine Pseudonymliste, in jedem Fall gesondert aufbewahrt werden und den technischen und organisatorischen Maßnahmen unterliegen, die eine Zuordnung verhindern. Ist dies nicht gewährleistet, fällt die Pseudonymisierung der personenbezogenen Daten in den Anwendungsbereich der Verordnung.

FOLIE 7

Beispiele für personenbezogene Daten: (Art. 4 Nr.1 DSGVO)



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, Steuer-Identifikationsnummer, Krankenversicherungsnummer, Personalausweisnummer, Matrikelnummer, usw.

Bankdaten
Kontonummer, Kreditinformation, Kontostände, Vermögen, usw.

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

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

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

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

Werturteile
Schul- und Arbeitszeugnisse, usw.

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

Wichtig! Es wird nicht unterschieden zwischen den 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 8

Räumlicher Anwendungsbereich

Ob und inwieweit eine Verarbeitung auch vom räumlichen Anwendungsbereich der Datenschutz-Grundverordnung erfasst ist, wird in Art. 3 DS-GVO festgesetzt. Demnach findet die Verordnung Anwendung auf die Verarbeitung personenbezogener Daten, soweit:

- die Verarbeitung im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder Auftragverarbeiters in der EU erfolgt. Die Verarbeitung selbst muss jedoch nicht in der EU stattfinden
- die Verarbeitung durch nicht in der EU niedergelassene Verantwortliche/Auftragsverarbeiter erfolgt, aber
    - den betroffenen Personen in der EU Waren oder Dienstleistungen (auch unentgeltlich) angeboten werden
    - das Verhalten betroffener Personen beobachtet wird, wenn dieses in der EU erfolgt (z.B. Tracking über eine Smartwatch/Handy von einem amerikanischen Unternehmen) ⟶ sogenanntes Marktortprinzip
- wenn der Standort außerhalb der EU liegt, aber dem Recht eines Mitgliedstaats unterliegt (z.B. Botschaften, Konsulate).

FOLIE 9

Rechtmäßigkeit der Verarbeitung

Für die Verarbeitung personenbezogener Daten gilt in erster Linie das Verbot mit Erlaubnisvorbehalt. Dieses besagt, dass jede Erhebung oder Verarbeitung von personenbezogenen Daten grundsätzlich verboten ist. Art. 6 Abs. 1 DS-GVO regelt jedoch einige Bedingungen, unter denen eine Verarbeitung trotzdem rechtmäßig ist. Bei der Verarbeitung personenbezogener Daten werden zwei Kategorien unterschieden:

a) allgemeine Kategorien personenbezogener Daten
b) besondere Kategorien personenbezogener Daten

FOLIE 10

Allgemeine Kategorien personenbezogener Daten

Auf Basis einer der folgenden Rechtsgrundlagen ist eine Verarbeitung rechtmäßig:

- Einwilligung der betroffenen Person
    - Es liegt eine vorherige Zustimmung der betroffenen Person vor. Diese muss zwingend vor der Datenverarbeitung eingeholt werden
    - **Wichtig!** Wenn Einwilligungen nicht den gesetzlichen Regelungen entsprechend eingeholt werden, sind sie unwirksam. Hier gilt: Schriftform, konkrete Angabe des Zwecks und Freiwilligkeit des Betroffenen.
- Vertrag bzw. vorvertragliche Maßnahme zwischen betroffener Person und Datenverarbeiter

- Beispielhaft für eine vorvertragliche Maßnahme ist die Bitte eines Kunden um Zusendung eines Angebotes. Dies geschieht auf Antrag der betroffenen Person und somit ist eine Verarbeitung der Daten zulässig

- Interessenabwägungsklausel
  - meint das berechtigte Interesse des Verantwortlichen für die Datenverarbeitung, z.B. für Verwaltungszwecke oder zur Übertragung an Teile der Unternehmensgruppe
    → Interessen des Verantwortlichen dürfen nicht den Rechten und Freiheiten der betroffenen Person überwiegen
- rechtliche Verpflichtung
  - z.B. Aufbewahrungspflichten des Handel- und Steuerrrechts
- lebenswichtige Interessen der betroffenen oder einer anderen natürlichen Person
- Verarbeitung ist für die Aufgabe öffentlicher Interessen oder zur Ausübung öffentlicher Gewalt erforderlich

FOLIE 11

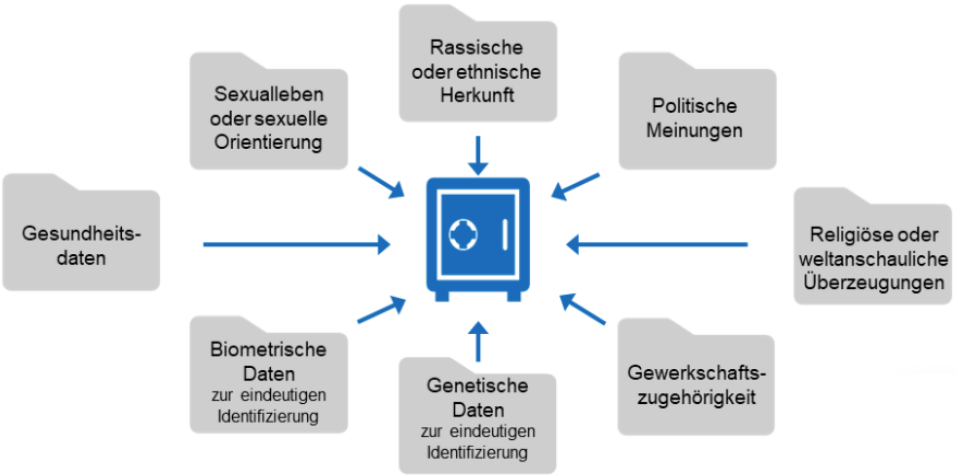
Besondere Kategorien personenbezogener Daten

Neben den allgemeinen personenbezogenen Daten, regelt die Datenschutz-Grundverordnung auch die Verarbeitung besonderer Kategorien personenbezogener Daten. Dabei handelt es sich um personenbezogene Daten, die besonders sensibel und schützenswert sind, da ihre Verarbeitung erhebliche Risiken für die betroffene Person mit sich bringen kann. Datenschutzrechtlich ist der Umgang mit solchen Daten strengen Restriktionen unterworfen, insbesondere bei der Zulässigkeit der Verarbeitung, werden teils sehr strikte Anforderungen gestellt. Wenngleich bei den besonderen Kategorien personenbezogener Daten ebenfalls das Verbotsprinzip gilt, listet Art. 9 Abs. 2 lit. a bis j DS-GVO einige Fallkonstellationen auf, in denen dieses Verbot keine Geltung hat. Nichtsdestotrotz erfahren solche Datenkategorien im Gesetz sowohl juristisch als auch technisch/organisatorisch einen besonderen Schutz. So stellt die DS-GVO bei der Verarbeitung von besonders schützenswerten Kategorien beispielsweise folgende Verpflichtungen an den Verantwortlichen:

- Erstellung eines Verarbeitungsverzeichnisses (Art. 30 Abs. 5)
- Erforderlichkeit einer Datenschutzfolgenabschätzung (Art. 35 Abs. 3 lit. b)
- Benennung eines Datenschutzbeauftragten (Art. 37 Abs. 1 lit. c)

FOLIE 12

Beispiele für besondere Kategorien personenbezogener Daten



FOLIE 13

Verantwortlichkeit

Bei der Frage nach der datenschutzrechtlichen Verantwortlichkeit sieht die DSGVO den „Verantwortlichen“ in der gesetzlichen Pflicht. Dabei handelt es sich nach Art. 4 Nr. 7 DS-GVO um diejenige *„natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.“* Demzufolge ist der Verantwortliche derjenige, der die personenbezogenen Daten verarbeitet, der entscheidet, was mit der Verarbeitung erreicht werden soll und welche Komponenten bei der Verarbeitung genutzt werden. Dies können beispielsweise Prozesse, Soft-/Hardware, Personen und Dienstleister sein. Somit ist bei der Verarbeitung personenbezogener Daten **der Verantwortliche der entscheidende Träger von Rechten und Pflichten** und erfährt in der Praxis eine entscheidende Bedeutung.
Wichtig! Im Unternehmen ist der Verantwortliche das Unternehmen und damit im Speziellen die Geschäftsführung. Dabei kann der Geschäftsführer bei Datenschutzverstößen persönlich haften!

Neben dem Verantwortlichen wird in der Datenschutz-Grundverordnung in unterschiedlichen Zusammenhängen auch der Auftragsverarbeiter als Adressat datenschutzrechtlicher Pflichten benannt. Nach Art. 4 Nr. 8 DS-GVO bezeichnet der „Auftragsverarbeiter“ *„eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.“* Trotz eigener datenschutzrechtlicher Pflichten unterliegt der Auftragsverarbeiter jedoch der Entscheidungshoheit des ihn beauftragenden Verantwortlichen und ist diesem weisungsgebunden. Damit bleibt der Verantwortliche der Auftraggeber.

Nach § 53 BDSG (Wahrung des Datengeheimnisses) sind Mitarbeiter verpflichtet, mit personenbezogenen Daten sorgfältig umzugehen sowie die Regelungen und Bestimmungen des Datenschutzes bei ihrer täglichen Arbeit umzusetzen. Dabei ist jedoch entscheidend, dass Mitarbeiter lediglich bei grober Fahrlässigkeit haften können. Bei geringer Fahrlässigkeit (die trotzdem schwere Auswirkungen haben kann) haftet der Verantwortliche. Aus diesem Grund sind Mitarbeiterschulungen und eine damit einhergehende Sensibilisierung der Mitarbeiter bezüglich des Datenschutzes elementar.

FOLIE 14

Grundsätze der DSGVO

Die in Art. 5 Abs. 1 DS-GVO aufgeführten Grundsätze können als eine Art „Grundregeln“ für die Verarbeitung personenbezogener Daten angesehen werden und helfen insbesondere bei der Auslegung der Verordnung.

1. **Rechtmäßigkeit der Verarbeitung**
   Mit dem Gebot der Rechtmäßigkeit wird darauf abgezielt, dass jede Datenverarbeitung einer entsprechenden Rechtsgrundlage bedarf, beispielsweise einer Einwilligung der betroffenen Person (vgl. Art. 6 Abs. 1 DS-GVO).
2. **Verarbeitung nach Treu und Glauben**
   Die Vorgabe nach Treu und Glauben ist als Auffangtatbestand zu verstehen. Dieser greift, sobald die Verarbeitung, trotz Einhaltung aller datenschutzrechtlichen Vorgaben im Einzelfall für die betroffene Person unverhältnismäßig ist.

3. **Transparenz**
   Das Gebot der Transparenz soll die heimliche Datenverarbeitung ausschließen und darüber hinaus gewährleisten, dass die betroffene Person umfassend über die Verarbeitung ihrer personenbezogenen Daten informiert wird.
4. **Zweckbindung**
   Gemäß des Grundsatzes der Zweckbindung dürfen personenbezogene Daten grundsätzlich nur *„...für festgelegte, eindeutige und legitime Zwecke erhoben“* und verarbeitet werden.
   Datenminimierung
   Seit jeher hat das Datenschutzrecht die Zielvorgabe, keine (Datenvermeidung) oder möglichst wenige (Datensparsamkeit) personenbezogene Daten zu verarbeiten. Dem entspricht der in der DS-GVO festgelegte Grundsatz der Datenminimierung, wonach personenbezogene Daten *„...dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt“* sein müssen. Dazu zählt auch, dass der Verantwortliche durch technische Voreinstellungen dafür sorgen muss, dass ausschließlich für die Verarbeitung essenzielle Daten erhoben werden.
5. **Richtigkeit der Datenverarbeitung**
   Personenbezogene Daten müssen *„...sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein.“* Die Einschränkung des „erforderlichenfalls“ bei der Aktualität der Daten meint, dass die Informationen überwiegend den Zustand zu einem bestimmten Zeitpunkt dokumentieren sollen. Weiterhin muss der Verantwortliche nach dem Grundsatz der Richtigkeit *„...alle angemessenen Maßnahmen“* treffen, damit unrichtige Daten unverzüglich gelöscht oder berichtigt werden.
6. **Speicherbegrenzung**
   Der Grundsatz der Speicherbegrenzung normiert eine zeitliche Grenze für die Datenverarbeitung. Demnach müssen personenbezogene Daten *„...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.“* Sobald die Kenntnis der pbD nicht mehr erforderlich ist, muss die Speicherung der Daten beendet werden.
7. **Integrität und Vertraulichkeit**
   Die Vorgaben der Integrität und Vertraulichkeit zielen auf die sog. Datensicherheit ab. Demnach sollen personenbezogene Daten so verarbeitet werden, dass *„...eine angemessene Sicherheit der personenbezogenen Daten gewährleistet“* ist. Während es beim Datenschutz allgemein um den Schutz des Persönlichkeitsrechts des Einzelnen im Umgang mit seinen personenbezogenen Daten geht, handelt es sich bei Datensicherheit speziell um den technischen Datenschutz. So soll durch technische und organisatorische Maßnahmen der *„Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung“* der Daten gewährleistet werden.

Wichtig! Der Verantwortliche ist gemäß Art. 5 Abs. 2 DS-GVO für die Einhaltung der aufgeführten Grundsätze verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“). Andernfalls können empfindliche Strafen drohen.

FOLIE 15

Rechte der betroffenen Person

Die Rechte der betroffenen Person dienen als Absicherung der Grundsätze für die Verarbeitung personenbezogener Daten aus Artikel 5 DS-GVO und räumen den Betroffenen zahlreiche Rechte gegenüber den verantwortlichen Stellen ein. Wichtig ist hierbei, dass die betroffene Person ihre Rechte ausschließlich gegenüber dem Verantwortlichen bzw. den gemeinsam Verantwortlichen geltend machen kann und nicht beispielsweise gegenüber eines Auftragverarbeiters.

1. **Recht auf Auskunft** (Art. 15 DS-GVO)
   Das Auskunftsrecht ist ein zentraler Bestandteil zum Schutz der personenbezogenen Daten. Nur wenn die betroffene Person tatsächlich Kenntnis davon hat, wer welche Daten und zu welchem Zweck von ihr besitzt, kann sie ihr Recht auf informationelle Selbstbestimmung vollumfänglich ausüben und sich ggf. schützen.

2. **Recht auf Berichtigung** (Art. 16 DS-GVO) Personenbezogene Daten, die fehlerhaft sind, muss der Verantwortliche korrigieren, sofern der Betroffene dies verlangt. Des Weiteren sind unvollständige personenbezogene Daten zu komplementieren.

3. **Recht auf Löschung bzw. „Recht auf Vergessenwerden“** (Art. 17 DS-GVO)
   Der Betroffene kann verlangen, dass sowohl der Verantwortliche als auch weitere Datenempfänger, seine personenbezogenen Daten löschen. Ein solcher Anspruch muss jedoch nur unter gewissen Voraussetzungen umgesetzt werden, beispielsweise, wenn die Daten für die Zwecke der Verarbeitung nicht mehr erforderlich sind oder die Verarbeitung unrechtmäßig erfolgt. Sind die Daten allerdings weiterhin erforderlich, z.B. aufgrund steuerrechtlicher Aufbewahrungsfristen, gilt der Anspruch auf Löschung nicht.

4. **Recht auf Einschränkung der Verarbeitung** (Art. 18 DS-GVO)
   Unter bestimmten Voraussetzungen kann die betroffene Person die Einschränkung der Verarbeitung ihrer personenbezogenen Daten verlangen. Dies gilt etwa, wenn die Richtigkeit der Daten bestritten wird. Folglich muss der Verantwortliche für die Dauer einer Überprüfung die Datenverarbeitung einschränken.

5. **Recht auf Datenübertragbarkeit** (Art. 20 DS-GVO)
   Mit diesem Artikel räumt der Gesetzgeber der betroffenen Person das Recht ein, die sie betreffenden personenbezogenen Daten, von einem Verantwortlichen zu einem anderen Verantwortlichen zu übertragen. Dieses Recht soll einen einfachen und unkomplizierten Anbieterwechsel ermöglichen und sogenannte „Lock-In-Effekte“ verhindern.

6. **Recht auf Widerspruch (Art. 21 DS-GVO)**
   Gemäß Artikel 21 steht den betroffenen Personen das Recht zu, gegen die Verarbeitung ihrer personenbezogenen Daten „...aus Gründen, die sich aus ihrer besonderen Situation ergeben“, jederzeit Widerspruch einzulegen. Dabei besteht das Widerspruchsrecht allerdings nur bei Verarbeitungen, die zur Erfüllung einer Aufgabe im öffentlichen Interesse oder zur Ausübung öffentlicher Gewalt vorgenommen werden, sowie gegen Verarbeitungen im berechtigten Interesse des Verantwortlichen oder eines Dritten. Eine weitere Verarbeitung trotz Widerspruchs ist nur zulässig bei Rechtsansprüchen oder schutzwürdigen Gründen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen. Somit sind im Rahmen

eines Widerspruchs die Gründe der betroffenen Person anzugeben und bei der Entscheidung hat eine spezifische Interessenabwägung zu erfolgen.

FOLIE 16

Datenschutzbeauftragter

Der betriebliche Datenschutzbeauftragte (DSB) nimmt heutzutage im Rahmen der Datenschutz-Grundverordnung eine wichtige und verantwortungsvolle Rolle im Unternehmen ein. Er fungiert als Schnittstelle zwischen Unternehmen, den Aufsichtsbehörden und den betroffenen Personen, wenn diese Fragen zur Verarbeitung sie betreffender personenbezogener Daten haben. Darüber hinaus tritt er im Zusammenhang mit der Verarbeitung von personenbezogen Daten als Berater des Verantwortlichen oder Auftragverarbeiters auf und ist diesbezüglich auch das Kontrollorgan innerhalb der Organisation. Sofern ein Datenschutzbeauftragter bestellt wird, ist dieser vom Verantwortlichen bzw. vom Auftragsverarbeiter an die Datenschutz-Aufsichtsbehörde zu melden.

Wichtig! Bei der Stellung des Datenschutzbeauftragten ist zu beachten, dass der DSB selbst keine Weisungsbefugnisse hat und für die Umsetzung des Datenschutzes nicht verantwortlich ist. Er besitzt lediglich eine beratende und unterstützende Funktion. Verantwortlicher für den Datenschutz bleibt das Unternehmen.

FOLIE 17

Elementare Datenschutz-Anforderungen an Unternehmen

Die DSGVO verfolgt den sogenannten risikobasierten Ansatz, d.h. für viele Aspekte des Datenschutzes muss das Risiko Beachtung finden. Hierbei ist jedoch nicht das unternehmerische Risiko, sondern das Risiko für die Rechte und Freiheiten der betroffenen Person gemeint. Aus diesem Grund hält die Datenschutz-Grundverordnung für das Unternehmen bzw. den Verantwortlichen einen breiten Pflichtenkatalog bereit, welcher eingehalten werden muss, um datenschutzkonform zu handeln. Da bei Verletzung der Anforderungen enorme Bußgelder drohen, sind dahingehende Kenntnisse für den Verantwortlichen elementar. Nachfolgend werden daher die wichtigsten Anforderungen zum Schutz der personenbezogenen Daten erläutert.

1. Verzeichnis von Verarbeitungstätigkeiten
2. Technische und organisatorische Maßnahmen
3. Datenschutz-Folgenabschätzung
4. Auftragsverarbeitungsvertrag
5. Datenübermittlung in Drittländer
6. Risikoanalyse
7. Datenschutzkonzept
8. Informationspflicht
9. Schulung von Mitarbeitern
10. Meldepflicht bei Datenpannen

FOLIE 18

Verzeichnis von Verarbeitungstätigkeiten

Im Verzeichnis von Verarbeitungstätigkeiten (VvV) werden alle Tätigkeiten beschrieben, bei denen personenbezogene Daten erfasst und verarbeitet werden. Damit dient das Verzeichnis als wesentliche Grundlage für eine strukturierte Datenschutzdokumentation und soll den Nachweis für eine verordnungskonforme Datenverarbeitung liefern. Das Unternehmen kommt mithilfe des VvV der allgemeinen Rechenschaftspflicht sowie der Erfüllung der Dokumentationspflichten nach. Gleichzeitig soll das Verzeichnis die Transparenz in Bezug auf die Verarbeitungstätigkeiten erhöhen. Art. 30 Abs. 1 und 2 DS-GVO verpflichtet sowohl den Verantwortlichen als auch den Auftragsverarbeiter zur Erstellung und Führung eines solchen Verzeichnisses.

FOLIE 19

Technische und organisatorische Maßnahmen

Um sicherzustellen und den Nachweis erbringen zu können, dass Verarbeitungen DSGVO konform erfolgen, verpflichtet Art. 24 DS-GVO den Verantwortlichen und Auftragsverarbeiter dazu, technische und organisatorische Maßnahmen (TOMs) im Unternehmen umzusetzen. Dabei muss sich die Auswahl und Umsetzung der Maßnahmen an der jeweiligen Verarbeitung (Art, Umfang, Umstände, Zwecke) und den damit einhergehenden Risiken für die Rechte und Freiheiten natürlicher Personen orientieren.
Die technischen Maßnahmen beziehen sich dabei regelmäßig auf Hard-, Software- und Netzwerkkomponenten, welche zur Datenverarbeitung herangezogen werden. In diesem Zusammenhang sieht Art. 25 DS-GVO konkrete Datenschutzinstrumente vor und Unternehmen sind angehalten, davon Gebrauch zu machen:

- **Datenschutz durch Technikgestaltung** („Privacy by Design“)
  Durch dieses Schutzkonzept soll der Datenschutz von Beginn an berücksichtigt werden, sobald eine Soft- oder Hardware eingesetzt wird, die personenbezogene Daten verarbeiten kann. Der Aspekt der Technikgestaltung soll Organisationen somit bereits im Entwicklungsstadium dazu verpflichten, auf Datenminimierung ausgerichtete IT-Systeme einzusetzen.
- **Datenschutz durch datenschutzfreundliche Voreinstellungen** („Privacy by Default“)
  Mit diesem Element soll der Datenschutz als Standardeinstellung implementiert werden und dafür sorgen, dass lediglich die zur Erreichung des Verarbeitungszwecks erforderlichen personenbezogenen Daten verarbeitet werden. Konkret ist die Idee dahinter, dass Dienst-, System- oder Gerätevoreinstellungen (Werkseinstellungen) möglichst datenschutzfreundlich umgesetzt werden und die Voreinstellungen ein Maximum an Privatsphäre sichern. So sollen auch Nutzer geschützt werden, die technisch nicht versiert sind und Datenschutzeinstellungen nicht selbst verändern können.

Die organisatorischen Maßnahmen hingegen richten sich insbesondere an Ablaufprozesse und die durchführenden Personen der Verarbeitung. Hierbei soll der Datenschutz beispielsweise durch das Aufstellen von Berechtigungskonzepten oder durch Schulungen und Vertraulichkeitsverpflichtungen der Mitarbeiter gewährleistet werden.

Weitere Beispiele für technisch organisatorische Maßnahmen sind etwa:

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

FOLIE 20

Datenschutz-Folgenabschätzung

Sofern die Verarbeitungsvorgänge *„...aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Person zur Folge“* haben, ist nach Art. 35 Abs. 1 DS-GVO vorab eine Abschätzung der Folgen durchzuführen. Damit beabsichtigt die Datenschutz- Folgenabschätzung (DSFA) den Zweck, das mit einer Verarbeitung einhergehende Risiko für die Rechte und Freiheiten natürlicher Personen zu senken. Gleichzeitig soll mit Hilfe der DSFA die Minimierung des Risikos dokumentiert und nachgewiesen werden, dass durch die im Rahmen der DSFA ermittelten und getroffenen Maßnahmen kein hohes Risiko mehr für die betroffene Person besteht. Entsprechend ist die DSFA vor Inbetriebnahme der Verarbeitung vom Verantwortlichen durchzuführen.
Zwar ist der DSGVO nicht genau zu entnehmen, unter welchen Bedingungen ein „hohes Risiko“ besteht, Anhaltspunkte für typische Konstellationen finden sich jedoch in den Erwägungsgründen 75, 83 und 85 DS-GVO. Sofern die Verarbeitung demnach zu physischen, materiellen oder immateriellen Schäden führen kann, ist eine DSFA durchzuführen. Dies ist im Einzelfall zu prüfen. Weiterhin ist eine DSFA nach Art. 35 Abs. 3 DS-GVO insbesondere in folgenden Fällen erforderlich:

1. Systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen auf Basis einer automatisierten Entscheidungsfindung, einschließlich Profiling als Grundlage einer Rechtswirkung oder ähnlich erheblichen Beeinträchtigung
2. Umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten oder pbD über strafrechtliche Verurteilungen und Straftaten
3. Systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

FOLIE 21

Auftragsverarbeitungsvertrag

Als Auftragsverarbeitung wird das Verarbeiten personenbezogener Daten durch einen Dienstleister, den Auftragsverarbeiter, im Auftrag eines Verantwortlichen bezeichnet. Wichtig ist an dieser Stelle, dass eine Auftragsverarbeitung nur dann zulässig ist, wenn die Zusammenarbeit auf einem abgeschlossenen Vertrag beruht. Durch diesen Auftragsverarbeitungsvertrag (AV-Vertrag) soll sowohl für den Auftraggeber als auch den Auftragnehmer, Klarheit über entsprechende Befugnisse, Weisungen, Zwecke der Verarbeitung sowie Rechte und Pflichten festgehalten werden. Außerdem dient der AV-Vertrag als Nachweis für den Verantwortlichen, sofern es seitens des Auftragverarbeiters zu Datenschutzverstößen kommt. Denn auch bei Auftragsverarbeitungen bleibt der Auftraggeber der Verantwortliche im Sinne der DSGVO und damit die haftende Person!
Wann genau ein AV-Vertrag abgeschlossen werden muss, kann nicht allgemein beantwortet werden. Einige Beispiele haben wir jedoch in einer Checkliste zusammengestellt.

FOLIE 22

Datenübermittlung in Drittländer

Bei der Verarbeitung von personenbezogenen Daten findet häufig eine Übermittlung von Daten in sogenannte „Drittländer“ statt. Dabei handelt es sich um alle Länder, die nicht Mitgliedstaat der EU und des Europäischen Wirtschaftsraums sind. Die Datenschutz-Grundverordnung erfordert sodann das Ergreifen von Schutzmaßnahmen, um in dem entsprechenden Drittland ein mit der DSGVO vergleichbares Datenschutzniveau sicherzustellen. Damit die Datenübermittlung in Drittländer rechtmäßig ist, bedarf es einer der folgenden Rechtsgrundlagen:

- Angemessenheitsbeschluss der EU
  - Die EU-Kommission bescheinigt dem jeweiligen Drittland ein der EU vergleichbares Datenschutzniveau. Diese Beschlüsse werden von der EU-Kommission veröffentlicht
- geeignete Garantien
  - Es wird auf verbindliche interne Datenschutzvorschriften oder spezielle Verträge zurückgegriffen, die von der EU-Kommission oder der Aufsichtsbehörde genehmigt sind (z.B. Standardvertragsklauseln)
- Ausnahmen für bestimmte Fälle
  - vom Gesetz explizit genannt, z.B. ausdrückliche Einwilligung der betroffenen Person oder eine strikte Erforderlichkeit zur Erfüllung eines Vertrags

Wichtig! Kann keine der Voraussetzungen erfüllt werden, ist die Datenübermittlung in Drittländer dringend zu unterbleiben.
Achtung! Der EU-US Privacy Shield, der zu Beginn als Rechtsgrundlage (Angemessenheitsbeschluss) zur Datenübermittlung in die USA gültig war, wurde von den Gerichten gekippt und ist nicht mehr datenschutzkonform. Damit bedarf es einer anderen gültigen Rechtsgrundlage, sofern personenbezogene Daten in die USA übermittelt werden sollen. In der Praxis geschieht dies nur in den meisten Fällen aufgrund von Standardvertragsklauseln.

Informationspflicht

Wenn Verantwortliche personenbezogene Daten erheben und verarbeiten wollen, müssen sie die Betroffenen darüber informieren. Diese sogenannten Informationspflichten ergeben sich direkt aus der Datenschutz-Grundverordnung. Auf Grundlage dieser Informationen soll dem Betroffenen ermöglicht werden, in Kenntnis aller Umstände eine selbstbestimmte Entscheidung über die Preisgabe seiner Daten zu treffen.

Umfang der Informationspflichten
Die DSGVO bestimmt in Art. 13 und 14 DSGVO, dass der Verantwortliche die betroffene Person über Folgendes unterrichten muss:

- Name und Kontaktdaten des Verantwortlichen und ggf. seines Vertreters, sowie (falls vorhanden) die Kontaktdaten des Datenschutzbeauftragten
- geeignete Rechtsgrundlage, auf der die Datenerhebung basiert und eine vollständige, detaillierte Beschreibung des Verarbeitungszwecks.

- dient als Rechtsgrundlage ein berechtigtes Interesse (Art. 6 Abs. 1 lit. f DSGVO), müssen sämtliche Interessen des Verantwortlichen einzeln aufgeführt werden. Dabei dürfen die Interessen der betroffenen Person jedoch nicht überwiegen.
- Die Empfänger der personenbezogenen Daten, d.h. jede weitere Stelle, der die personenbezogenen Daten offengelegt werden, müssen ohne Einschränkung mitgeteilt werden.
- Bei der Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist die betroffene Person darüber zu informieren: Darüber hinaus ist darzustellen, auf welcher Rechtsgrundlage die Übermittlung gestützt wird (z.B. Angemesseneheitsbeschluss, Standardvertragsklauseln)
- Angabe zur Speicherdauer der Daten
- Aufklärung der Betroffenen über ihre Rechte (Art. 15 ff. DSGVO)
- Bei Direkterhebung der Daten bei der betroffenen Person ist diese darüber zu unterrichten, ob die Daten aufgrund gesetzlicher oder vertraglicher Umstände erforderlich sind
- Angabe der Quelle, sofern die Erhebung nicht direkt beim Betroffenen erfolgte

Schulung von Mitarbeitern

Laut DSGVO besteht zwar keine explizite Pflicht innerhalb des Unternehmens eine Datenschutz-Schulung von Mitarbeitern durchzuführen. Allerdings ergibt sich eine Notwendigkeit zur Sensibilisierung und Schulung der Mitarbeiter durch deren Aufgabengebiete, die sie verantworten. So hat das Unternehmen als verantwortliche Stelle nach Art. 24 DSGVO sicherzustellen, dass personenbezogene Daten in einer Weise verarbeitet werden, die ein angemessenes Sicherheitsniveau gewährleistet. Dies beinhaltet auch den Schutz gegen unberechtigte oder unrechtmäßige Verarbeitung. Darüber hinaus sollen angemessene technische und organisatorische Maßnahmen getroffen werden, die gegen Verlust, Zerstörung oder Schäden an den Daten schützen sollen.
Wir empfehlen daher dringend, Mitarbeiterschulungen durchzuführen und zusätzlich eine Verpflichtungserklärung der Mitarbeiter zur Einhaltung des Datenschutzes einzuholen.
Es kann festgehalten werden:

- Mitarbeiter sind diejenigen, die personenbezogene Daten verarbeiten und sind damit ebenfalls Ziel der DSGVO. Daher muss das Unternehmen sicherstellen, dass der Mitarbeiter die Daten nicht unberechtigt oder gegen geltendes Recht verarbeitet.
- Unternehmen haben im Rahmen eines „angemessenen Schutzniveaus“ für personenbezogene Daten dafür Sorge zu tragen, dass Mitarbeiter erkennen können, wann sie ggf. mit der Datenverarbeitung gegen Gesetze verstoßen bzw. unberechtigt Daten verarbeiten.
- Schulungen bieten die beste Möglichkeit, Mitarbeiter für die DSGVO zu sensibilisieren und aufzuklären. Entsprechende Teilnehmerlisten dokumentieren, dass Maßnahmen zum „angemessenen Schutzniveau" getroffen wurden.
- Nach Art. 39 DSGVO ist es die Aufgabe des Datenschutzbeauftragten, Mitarbeiter zu schulen. Hierin erweist es sich von Vorteil einen Datenschutzbeauftragten zu haben, der auch solche Maßnahmen koordiniert und durchführt.
- Eine konkrete Strafandrohung gibt es bei Verletzung des Art. 24 DSGVO für die Unternehmen nicht. Allerdings lässt die DSGVO in Art. 58 der Aufsichtsbehörde die Möglichkeit, Unternehmen entsprechend anzuweisen, Mängel in den technischen und organisatorischen Maßnahmen zu beheben. Befolgt das Unternehmen dies nicht, kann ein Bußgeld nach Art. 83 Abs. 5 (e) DSGVO verhängt werden.

Meldepflicht bei Datenpannen

Mit Einführung der DSGVO ist der Verantwortliche dazu verpflichtet, jede Datenschutzverletzung zu dokumentieren. Dies gilt unabhängig des zu erwartenden Risikos für die persönlichen Rechte und Freiheiten des Betroffenen. (Art. 33 Abs. 5 DSGVO). Der Aufwand der Dokumentation ist dabei nicht zu unterschätzen, da alle zusammenhängenden Fakten, Auswirkungen und ergriffenen Maßnahmen zu erfassen sind.

Wichtig! Sofern eine Datenpanne mehr als ein geringes Risiko für die Rechte und Freiheiten der betroffenen Person zur Folge hat, muss dieser Vorfall vom Verantwortlichen innerhalb von 72 Stunden an die Aufsichtsbehörde gemeldet werden!

Für den Verantwortlichen ergeben sich zusammenfassend folgende Pflichten:

Risiko/ Pflichten	Interne Dokumentationspflicht	Meldepflicht an zuständige Aufsichtsbehörde	Benachrichtigungs-pflicht an betroffene Person
Voraussichtlich kein bzw. nur geringes Risiko	ja	nein	nein
Risiko	ja	ja	nein
Hohes Risiko	ja	ja	ja

FOLIE 23

Datenschutzmanagementsystem

Der Aufbau eines Datenschutzmanagementsystems erfährt in der datenschutzrechtlichen Praxis eine zentrale Bedeutung. Durch dessen Einsatz soll die Einhaltung des Datenschutzes und der DSGVO über die gesamte Organisation hinweg gesichert, dokumentiert und fortlaufend verbessert werden. Insbesondere die Pflicht zur Erfüllung der Dokumentations-, Nachweis- und Rechenschaftspflichten machen den Einsatz eines DSMS nahezu unvermeidbar. Im Kern besteht ein Datenschutzmanagementsystem dabei aus Dokumentationen, Arbeitsanweisungen und Prüfprozessen. So soll eine lückenlose Nachvollziehbarkeit sowie eine klare und effiziente Verteilung der Verantwortlichkeiten gewährleistet werden. Die ständige Überprüfung hat einen kontinuierlichen Verbesserungsprozess zum Schutz der personenbezogenen Daten zur Absicht.

FOLIE 24

Konsequenzen aus Verstößen

Nach Art. 82 Abs. 1 DS-GVO hat *„...jede Person, der wegen eines Verstoßes gegen diese Verordnung ein materieller oder immaterieller Schaden entstanden ist, [...] Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter.“*
Artikel 83 thematisiert die Verhängung von Bußgeldern und sieht zwei mögliche Kategorien bei Verstößen vor:

1. Formeller Verstoß (Art. 83 Abs. 4 DS-GVO)
   → bis zu 10 Millionen Euro oder im Falle von Unternehmen bis zu 2 % des gesamten weltweit erzielten Vorjahresumsatzes
   (z.B. bei fehlerhaften oder unvollständigen Verzeichnis von Verarbeitungstätigkeiten, nicht ausreichend umgesetzte technische und organisatorische Maßnahmen)

2. Materieller Verstoß (Art. 83 Abs. 5 DS-GVO)
   → bis zu 20 Millionen Euro oder im Falle von Unternehmen bis zu 4 % des gesamten weltweit erzielten Vorjahresumsatzes
   (z.B. bei Nichtbeachtung der Grundsätze der Verarbeitung oder der Rechte betroffener Personen)

Die Höhe der potenziellen Bußgelder verdeutlicht, dass diese einen großen Abschreckungseffekt erzielen sollen und Verstöße gegen die Datenschutz-Grundverordnung erhebliche Konsequenzen für Unternehmen zur Folge haben können!

Vielen Dank für eure Aufmerksamkeit!

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, schutzbedürftigen 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. **richtiger 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!