



# Datenschutz

- Bisher Datenschutzgesetz auf Grundlage einer EU-Richtlinie
- Ab 28. Mai 2018 Anwendung der EU-Datenschutz-Grundverordnung (EU-DSGVO)
- Verordnung lässt den einzelnen Mitgliedsstaaten gewisse Spielräume in der nationalen Umsetzung (untypisch für Verordnungen)
- Sehr strenges Reglement, allerdings bestehen viele offene Fragen in der Umsetzung, bzw der Interpretation von Begriffen die ggf wohl von den nationalen Gerichten und dem EuGH vorzunehmen sein werden



Republik Österreich  
Datenschutz  
behörde

[Leitfaden der DSB](#)

<https://www.privacyofficers.at/>

## Was wird geregelt?



- Dt Bundesverfassungsgericht 1983: Grundrecht auf informationelle Selbstbestimmung
- Grundrecht auf Datenschutz
- Grundrecht auf Achtung des Privat- und Familienlebens
- EU-Datenschutz-Grundverordnung (EU-DSGVO)

Musterdokumente

Aufwendige Umsetzung

Die Verwendung von Daten greift in  
viele Grundrechte ein

Stehen im Stufenbau der  
Rechtsordnung ganz oben ->  
Fundament des Staates!



➤ Jede Art der Verarbeitung von personenbezogenen Daten natürlicher Personen ist betroffen

- Online, zB durch Software
- Offline, in jeder Art der Verwaltung von Daten
- Sogar manuell geführte Karteien wenn Du für die Geburtstagsfeier der Oma eine Sammlung von Karteikärtchen mit Name und Adresse der Verwandten anlegst

Alles was mit Daten gemacht wird ist Verarbeitung, zB auch die Löschung

Nicht betroffen sind Daten juristischer Personen und von Personengesellschaften, sehr wohl aber von deren Gesellschaftern und Einzelunternehmern!

## Wo gilt die DSGVO?



- Räumlicher Anwendungsbereich
  - Anwendung auf jede Datenverarbeitung einer Niederlassung in der EU
  - Marktortprinzip -> Daten von Personen die in der EU aufhältig sind werden außerhalb der EU verarbeitet, um
    - Waren oder Dienstleistungen anzubieten (zB Bücher über das Internet aus Russland anbieten)
    - Verhalten von Personen in der EU beobachten (zB Onlineanalyse von außerhalb der EU)
  - Die DSGVO ist anzuwenden!

# Begriffe



- Personenbezogene Daten
  - Personenbezogene Daten sind alle Daten, die sich direkt oder indirekt auf eine identifizierbare oder identifizierte natürliche Person beziehen
    - Name einer Person -> identifiziert die Person direkt
    - Geburtsdatum -> macht für sich alleine ein Person noch nicht identifizierbar, aber gemeinsam mit einem oder mehreren anderen Kriterien schon, zB Name + Geburtsdatum, oder Geburtsdatum + Geburtsort -> indirekt identifizierbar
    - IBAN -> für die Bank jedenfalls identifizierbar, für andere Personen / Institutionen gemeinsam mit Kontobewegungen -> indirekt identifizierbar

Beispiele



## ➤ Anonymisierte Daten

- Anonymisierte Daten sind Daten, die nicht auf eine identifizierte oder identifizierbare Person bezogen werden können
- Anonymisierte Daten unterliegen nicht der DSGVO
- Anzahl der Krankheitsfälle einer Grippewelle bei der die Daten von 100.000 Personen nur nach dem Kriterium erkrankt / gesund erfasst werden
- Weitere Gruppierung dieser Daten nach Altersgruppen 0-20 Jahre, 20-40 Jahre, 40-60 Jahre, > 60 Jahre
- Eine zusätzliche Gruppierung dieser Daten nach Postleitzahlen kann schon problematisch sein, wenn in einem kleinen Ort nur eine Person der Gruppe > 60 Jahre lebt -> wäre indirekt identifizierbar

Anonymisierung ist ein sehr sensibler und komplexer Vorgang!

Beispiele

## ➤ Sensible Daten



➤ Verarbeitung

- Jeder (nicht) automatisierter Vorgang in Zusammenhang mit personenbezogenen Daten

zB Unternehmen das Daten von Mitarbeitern verarbeitet

➤ Verantwortlicher

- Natürliche oder juristische Person oder Einrichtung, Behörde, Stelle, die gemeinsam mit anderen oder alleine über die Mittel und Zwecke der Verarbeitung von personenbezogenen Daten entscheidet

zB Anbieter von Clouddienstleistungen

➤ Auftragsverarbeiter

- Natürliche oder juristische Person oder Einrichtung, Behörde, Stelle, die im Auftrag des Verantwortlichen personenbezogene Daten verarbeitet





➤ Die Einwilligung der betroffenen Person, deren Daten verarbeitet werden muss

Beweislast, dass  
eingewilligt wurde liegt  
beim Verantwortlichen

- freiwillig in informierter Weise für den bestimmten Fall erfolgen
- unmissverständlich abgegeben werden
- schriftlich, elektronisch, durch Anklicken eines Kästchens, Auswahl von Einstellungen, etc
- jederzeit widerrufen werden können und gilt ab dem Zeitpunkt des Widerrufs



- durch Erklärung oder sonstige eindeutig bestätigende Handlung erfolgen
- Stillschweigen oder die Akzeptanz von bereits gesetzten Voreinstellungen ist keine Einwilligung

Ausdrückliche, dh aktive Einwilligung ist nur bei der Verarbeitung von sensiblen Daten erforderlich!

# Grundsätze für die Verarbeitung



- Rechtmäßigkeit, Treu und Glauben, Transparenz
- Die Verarbeitung von personenbezogenen Daten braucht eine rechtliche Grundlage
- Rechtmäßigkeit durch Einwilligung, Erfüllung eines Vertrages, von rechtlichen Verpflichtungen, lebenswichtigen Interessen, Wahrnehmung von Aufgaben im öffentlichen Interesse / Ausübung öffentlicher Gewalt

Ausdrückliche Einwilligung bei  
**sensiblen Daten!**



➤ Zweckbindung

Vor Beginn der  
Verarbeitung!

- Der Zweck der Verarbeitung muss eindeutig und legitim festgelegt werden, in damit nicht vereinbarter Weise darf nicht weiterverarbeitet werde
- Für andere Zwecke als den festgelegten darf nur weiterverarbeitet werden, wenn eine Einwilligung oder eine gesetzliche Grundlage dafür vorliegt

Ist vor Beginn der  
abweichenden  
Verarbeitung einzuholen!



➤ Datenminimierung

- Nur die Daten, die unbedingt für die Verarbeitung notwendig sind dürfen verarbeitet werden, dies ist auch durch entsprechende technische Voreinstellungen sicherzustellen

Benötigt ein Versandhandel zB nur  
Name und Adresse des Kunden  
darf das Geburtsdatum nicht  
verarbeitet werden

➤ Richtigkeit

- Die Daten müssen richtig und auf dem aktuellen Stand sein; technische Maßnahmen, damit falsche Daten gelöscht oder aktualisiert werden sind einzurichten



➤ Speicherbegrenzung

- Die Identifizierung einer Person ist nur solange zulässig, als dies für den Zweck, für den die Daten verarbeitet wurden erforderlich ist

Die Maßnahmen dürfen nicht vom finanziellen Aufwand abhängig gemacht werden; dh wenn ich Daten die entsprechende Maßnahmen erfordern verarbeiten will muss ich mir das leisten

Es sind unternehmerische und gesetzliche Aufbewahrungsfristen und –verpflichtungen zu beachten

➤ Integrität und Vertraulichkeit


- Angemessene Sicherheit ist durch geeignete technische Maßnahmen zu gewährleisten; Unbefugte dürfen weder Daten erlangen, noch Geräte, auf denen diese Daten verarbeitet werden benutzen können







➤ Rechenschaftspflicht

- Der Verantwortliche ist für die Einhaltung der Grundsätze (auch durch den Auftragsverarbeiter!!!) verantwortlich und muss die Einhaltung nachweisen können
- Der Verantwortliche ist auch für die Einhaltung der Grundsätze durch den von ihm beauftragten Auftragsverarbeiter verantwortlich. Verstößt der Auftragsverarbeiter gegen die Grundsätze (auch ohne das Wissen des Auftraggebers), so haftet der Verantwortliche als Auftraggeber
- Sowohl die Entscheidungen bei der Einführung der Maßnahmen nach der DSGVO, als auch der laufende Betrieb ist zu dokumentieren

➤ Verarbeitung von sensiblen Daten

 Besprechung in „Allge... 00:48 —

Anruf läuft. Klicken Sie hier, um zum Anrufbildschirm zurückzukehren.





- Bei einem Verstoß gegen die Grundsätze für die Verarbeitung drohen
  - Geldstrafen von bis zu € 20.000.000,-- oder
  - von bis zu 4% des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres

Der jeweils höhere Betrag  
kann verhängt werden

# Rechte des von der Datenverarbeitung Betroffenen



- Der von einer Datenverarbeitung Betroffene hat verschiedene Rechte

Informationspflichten  
des Verantwortlichen

Auskunftsrecht

Recht auf Berichtigung

Recht auf Löschung



Recht auf  
Einschränkung der  
Verarbeitung

Recht auf  
Datenübertragbarkeit

Widerspruchsrecht



➤ Allgemeines zu den Rechten des Betroffenen

➤ Der Betroffene kann seine Rechte gegenüber dem Verantwortlichen geltend machen

➤ Für die Geltendmachung keine Formvorschriften, dh sie kann schriftlich, mündlich

➤ Dem Begehren des Betroffenen innerhalb eines Monats kostenlos nachzukommen

➤ Der Betroffene kann Beschwerde bei der Schutzbehörde erheben wenn er der Meinung ist, dass gegen seine Rechte verstoßen wurde

➤ Wurde gegen die Rechte des Betroffenen verstoßen können Geldstrafen iHv € 20.000.000,-- oder 4% des weltweiten letztjährigen Jahresumsatzes verhängt werden

Vgl Folie 8

Diese Punkte gelten für alle Rechte des Betroffenen



➤ Informationspflicht wenn beim Betroffenen Daten erhoben werden

➤ Der Verantwortliche hat dem Betroffenen gewisse Informationen zu erteilen wenn er Daten von ihm erhebt

➤ Name und Kontaktdaten des Verantwortlichen

➤ Kontaktdaten des Datenschutzbeauftragten wenn es einen gibt

➤ Rechtsgrundlage und Zweck der Verarbeitung

➤ Dauer der Datenspeicherung

➤ Rechte des Betroffenen

➤ Möglichkeit des Widerrufs der Zustimmung zur Verarbeitung

Die Informationen sind im Zeitpunkt der  
Datenerhebung zu erteilen

- Möglichkeit einer Beschwerde bei der Aufsichtsbehörde
- Grundlage für die Bereitstellung der Daten und Folgen bei Nichtbereitstellung
- Vorliegen von automatisierten Entscheidungsfindungen, zB Profiling



Die Informationen sind  
im Zeitpunkt der  
Datenerhebung zu  
erteilen





➤ Auskunftsrecht

- Der Betroffene hat Anspruch auf Auskunft, ob und welche Daten wie verarbeitet werden
- Negativauskunft: dem Betroffenen muss auch mitgeteilt werden, wenn keine Daten verarbeitet werden



➤ Recht auf Berichtigung

- Der Betroffene hat Anspruch darauf, dass fehlerhafte Daten berichtigt werden, zB falsche Adresse
- Der Betroffene hat Anspruch darauf, dass unvollständige Daten vervollständigt werden. Maßstab, ob die Daten vollständig sind ist der Zweck der Verarbeitung



➤ Recht auf Löschung -> „Recht auf Vergessenwerden“

Aber:  
EuGH: Google muss das  
„Recht auf Vergessen“  
nicht weltweit umsetzen

- Der Betroffene hat einen Anspruch auf Löschung der Daten, wenn
  - die Daten für den Zweck für den sie erhoben wurden nicht mehr notwendig sind
  - der Betroffene seine Zustimmung zur Verarbeitung zurückgezogen hat
  - der Betroffene Widerspruch gegen die Verarbeitung eingelegt hat (vgl Folie 35)
  - die Daten unrechtmäßig verarbeitet wurden





Vgl Folie 6

- Die Daten sind vom Verantwortlichen zu löschen
- Der Verpflichtung zur Löschung kann auch durch eine Anonymisierung erfüllt werden
- Die Löschung kann abgelehnt werden, wenn die Verarbeitung erforderlich ist
  - zur Wahrung des Rechts auf freie Meinungsäußerung
  - zur Erfüllung einer rechtlichen Verpflichtung
  - zur Erfüllung öffentlicher Interessen im Gesundheitswesen
  - Zur Geltendmachung/Verteidigung/Ausübung von Rechtsansprüchen

➤ Recht auf Einschränkung der Verarbeitung

➤ Der Betroffene hat einen Anspruch auf Einschränkung der Verarbeitung, wenn

- der Betroffene die Richtigkeit der Daten bestreitet während der Verantwortliche dies prüft
- der Betroffene Widerspruch gegen die Verarbeitung erhoben hat während der Verantwortliche die Rechtmäßigkeit des Anspruchs prüft
- der Betroffene bei unrechtmäßiger Verarbeitung die Löschung der Daten ablehnt und die Einschränkung der Verarbeitung verlangt
- der Verantwortliche die Daten nicht mehr benötigt, der Betroffene aber schon um Rechtsansprüche geltend zu machen

Er könnte sie zB noch zu Beweis Zwecken benötigen

Dh der Verantwortliche muss seinem potentielle Kläger Beweismittel „sichern“

Die Daten dürfen vom Verantwortlichen nur mehr gespeichert werden



➤ Recht auf Datenübertragbarkeit

- Der Betroffene hat einen Anspruch darauf,
  - dass ihm die personenbezogenen Daten, die er dem Verantwortlichen zur Verfügung gestellt hat übermittelt werden
  - dass die Daten in einer strukturierten, gängigen und maschinenlesbaren Form zur Verfügung gestellt werden
  - dass die Daten in einem branchenüblichen Format, oder in einem offenen Format wie XML, JSON oder CSV zur Verfügung gestellt werden



- dass die Daten sowohl die personenbezogenen Daten umfassen, die er direkt zur Verfügung gestellt hat, als auch die Daten, die sich durch die Nutzung der Dienstleistung und die Beobachtung des Betroffenen ergeben haben. Dazu zählen zB Aktivitätsprotokolle, Suchverläufe, oder Standortdaten, nicht aber Daten, die der Verantwortliche selbst generiert hat wie zB Nutzerprofile
- dass die Daten ihm oder einem von ihm benannten anderen Verantwortlichen übermittelt werden



➤ Recht auf Widerspruch

- Der Betroffene hat einen Anspruch darauf,
  - dass er gegen die Verarbeitung von Daten zu Zwecken des Direktmarketings jederzeit Widerspruch erheben kann. Die Verarbeitung ist einzustellen
  - gegen die Verarbeitung zu wissenschaftlichen, historischen und statistischen Zwecken Widerspruch zu erheben wenn sie besondere Gründe vorbringen kann
  - gegen die Verarbeitung für die Wahrnehmung einer Aufgabe die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt Widerspruch zu erheben, es sei denn, es liegen zwingende schutzwürdige Gründe für die Verarbeitung vor

# Pflichten des Verantwortlichen



- Der für die Datenverarbeitung Verantwortliche hat unterschiedliche Pflichten

Informationspflichten  
gegenüber Betroffenen

Erfüllung der Rechte  
der Betroffenen

Implementierung von  
Datensicherheitsmaßnahmen

Führung eines Verzeichnisses aller  
Datenverarbeitungstätigkeiten



Data breach  
notification

Risikoanalysen

Bestellung eines  
Datenschutzbeauftragten

➤ Informationspflichten gegenüber Betroffenen

- Der Verantwortliche hat Betroffene vor der Erhebung ihrer Daten umfassend zu informieren -> vgl Folie 20f

➤ Erfüllung der Rechte der Betroffenen

- Der Verantwortliche hat den Rechtsansprüchen von Betroffenen nachzukommen -> vgl Folie 22ff



➤ Implementierung von Datensicherheitsmaßnahmen

➤ Der Verantwortliche ist verpflichtet, Datenschutz und Datensicherheit

➤ durch Technik und

➤ datenschutzfreundliche Voreinstellungen sicherzustellen

Privacy by  
design

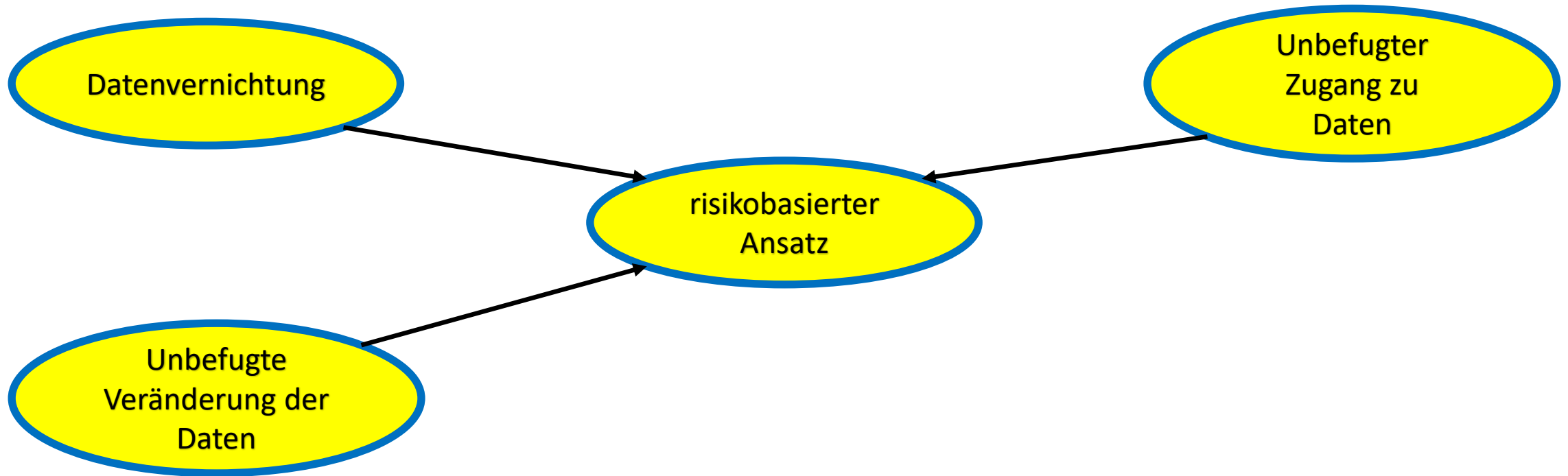
Privacy by  
default





- Datenschutz durch Technik (privacy by design) durch
  - Pseudonymisierung und Verschlüsselung
  - organisatorische, physische und it-technische Maßnahmen zur Sicherstellung der Sicherheit und Vertraulichkeit der Systeme
  - Systeme und Prozesse zur Überprüfung der Maßnahmen und Sicherstellung eines entsprechenden Schutzniveaus

➤ Welches Schutzniveau ist nötig?





- Für die Maßnahmen sind der Stand der Technik, die Kosten der Implementierung, Art und Umfang der Datenverarbeitung sowie die damit verbundenen Risiken entscheidend
- Wenn sich der Verantwortliche die Kosten „nicht leisten“ kann oder will darf er die Daten nicht verarbeiten
- Zertifizierungen oder Verhaltensregeln können ein Anhaltspunkt sein, stellen aber keine verbindliche Bestätigung der Erfüllung der notwendigen Maßnahmen dar



- Datenschutz durch datenschutzfreundliche Voreinstellungen (privacy by default)
  - Voreinstellungen sind datenschutzfreundlich zu setzen
  - Es dürfen nur die Daten erhoben und verarbeitet werden, die für den vorgesehenen Zweck erforderlich sind

zB alle Optionen für User auf „leer“ setzen und die User frei entscheiden lassen. User sind zwar „faul“, aber dadurch angehalten, sich damit auseinanderzusetzen, was sie alles nutzen wollen



- Führung eines Verzeichnisses aller Datenverarbeitungstätigkeiten
  - Der Verantwortliche hat Verzeichnisse aller Datenverarbeitungstätigkeiten in schriftlicher Form zu führen über
    - den Verantwortlichen
    - den Zweck der Datenverarbeitung
    - die Kategorien von betroffenen Personen, Daten und Empfängern (zB Behörden, Sozialversicherung, etc) von Daten
    - die Lösungsfristen der Kategorien sowie Datensicherheitsmaßnahmen

Dazu müssen in einem ersten Schritt sämtliche Datenverarbeitungsvorgänge im Unternehmen analysiert werden



- Unternehmen mit weniger als 250 Mitarbeitern müssen keine Verzeichnisse führen, wenn

- die Datenverarbeitung kein Risiko für Rechte und Freiheiten der Betroffenen darstellt

- die Verarbeitung nur gelegentlich erfolgt

- keine sensiblen Daten verarbeitet werden

Sobald ein Unternehmen zB Kundendateien hat verarbeitet es nicht mehr „gelegentlich“

Vgl Folie 7

Das Unternehmen muss überprüfen ob und beweisen, dass eine der Ausnahmen vorliegt

- Wurde gegen die Rechte des Betroffenen verstoßen können Geldstrafen iHv € 10.000.000,-- oder 2% des weltweiten letztjährigen Jahresumsatzes verhängt werden



➤ Meldung von Datenschutzverletzungen – data breach notification

➤ Der Verantwortliche ist verpflichtet, Datenschutzverletzungen zu melden, wenn

➤ den Betroffenen ein physischer, materieller oder immaterieller Schaden entstehen kann

➤ voraussichtlich ein Risiko für die Rechte und Freiheiten der Betroffenen besteht binnen 72 Stunden an die Datenschutzbehörde

➤ voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen besteht an die Betroffenen

zB Hacking von  
Bankdaten,  
Gesundheitsdaten,  
privaten Daten, etc

Wann dies gegeben ist muss  
der Verantwortliche auf  
eigenes Risiko einschätzen

Kommt es beim  
Auftragsverarbeiter zu einem  
Zwischenfall muss er dies dem  
Verantwortlichen melden

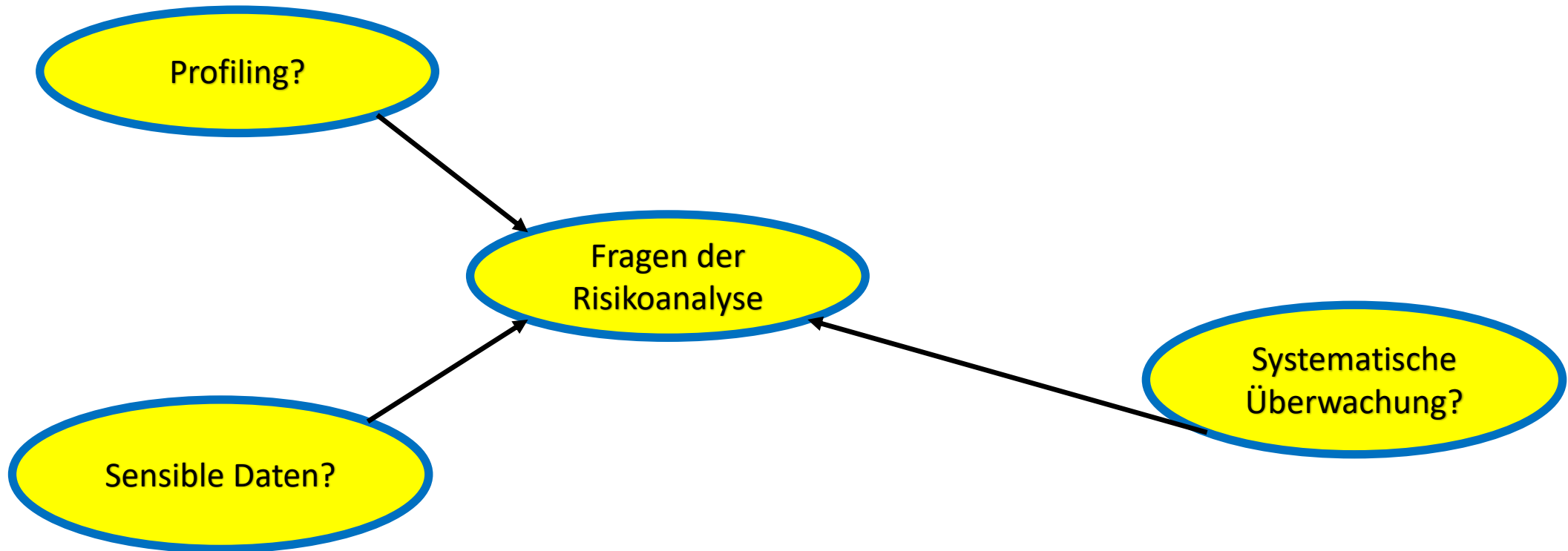
- Wurde gegen die Melde- oder Benachrichtigungspflicht verstoßen können Geldstrafen iHv € 10.000.000,-- oder 2% des weltweiten letztjährigen Jahresumsatzes verhängt werden





## ➤ Risikoanalysen

- Bis zur Einführung der DSGVO musste der Verantwortliche Meldungen an die Datenschutzbehörde machen und Vorabkontrollen seiner Anwendungen durch die Behörde durchführen lassen
- Nunmehr muss er selbst eine Risikoanalyse durchführen und haftet dafür





- Sind eine oder mehrere Kriterien erfüllt ist eine Datenschutz-Folgenabschätzung durchzuführen
- Jedenfalls muss eine Datenschutz-Folgenabschätzung durchgeführt werden, wenn die Tätigkeit auf der black list der Datenschutzbehörde erfasst ist
- Keine verpflichtende Datenschutz-Folgenabschätzung ist durchzuführen, wenn die Tätigkeit auf der white list der Datenschutzbehörde erfasst ist
- In allen anderen Fällen liegen die Entscheidung und das Risiko einer Fehlentscheidung beim Verantwortlichen. Die Entscheidung ist vor Aufnahme der Verarbeitung zu treffen.

zB Überwachung  
öffentlicher Orte, Einsatz  
neuer Technologien

zB Kundenverwaltung.  
Archivierung,  
Organisation von  
Veranstaltungen

- Wurde gegen die Vorschriften zur Risiko- und Datenschutz-Folgenabschätzung verstoßen können Geldstrafen iHv € 10.000.000,-- oder 2% des weltweiten letztjährigen Jahresumsatzes verhängt werden

## Pflichten des Auftragsverarbeiters



- Der Auftragsverarbeiter wird für den Verantwortlichen tätig der für ihn haftet
  - für die Implementierung von Datensicherheitsmaßnahmen
  - für die Führung von Verzeichnissen
  - für die Durchführung von Risikoanalysen
- Ein Auftragsverarbeiter darf ohne vorherige schriftliche Genehmigung des Verantwortlichen keinen Subauftragnehmer beauftragen. Tut er es trotzdem haftet dennoch der Verantwortliche, da er den Auftragsverarbeiter ausgewählt hat
- Der Auftragsverarbeiter hat eine Warnpflicht gegenüber dem Verantwortlichen falls eine Weisung gegen die DSGVO verstößt



## Der Datenschutzbeauftragte

- Verantwortliche müssen einen Datenschutzbeauftragten bestellen, wenn
  - es sich um eine Behörde oder öffentliche Stelle mit Ausnahme der Justiz handelt
  - in der Kerntätigkeit des Verantwortlichen eine umfangreiche und regelmäßige Überwachung von Betroffenen erfolgt (zB Kreditunternehmen)
  - in der Kerntätigkeit des Verantwortlichen eine umfangreiche Verarbeitung sensibler Daten oder Daten von strafrechtlichen Verurteilungen erfolgt
- In allen anderen Fällen kann ein Datenschutzbeauftragter bestellt werden



- Aufgaben des Datenschutzbeauftragten
  - Beratung des Verantwortlichen und der Mitarbeiter hinsichtlich datenschutzrechtlicher Pflichten
  - Überprüfung und Überwachung der Einhaltung von Vorschriften und Strategien zur Einhaltung des Datenschutzes
  - Beratung iZm der Datenschutz-Folgeabschätzung und Überwachung der Einhaltung
  - Zusammenarbeit mit der Aufsichtsbehörde



Was sind die  
jeweiligen Vor-  
und Nachteile?

- Stellung des Datenschutzbeauftragten
  - Als Datenschutzbeauftragter kann ein Mitarbeiter des Verantwortlichen oder eine externe Person benannt werden
  - Der Datenschutzbeauftragte ist in seiner Tätigkeit weisungsfrei und zur Einhaltung von Geheimhaltung und Vertraulichkeit verpflichtet
  - Dem Datenschutzbeauftragten sind vom Verantwortlichen die benötigten Ressourcen zur Verfügung zu stellen
  - Der Datenschutzbeauftragte ist der Datenschutzbehörde zu benennen
- Wurde gegen die Bestimmungen iZm dem Datenschutzbeauftragten verstoßen können Geldstrafen iHv € 10.000.000,-- oder 2% des weltweiten letztjährigen Jahresumsatzes verhängt werden



Alle Staaten die  
nicht Mitglied  
der EU oder des  
EWR sind

## Internationaler Datenverkehr

zB UNO,  
OSZE

- Innerhalb der EU ist eine Übermittlung von personenbezogenen Daten aufgrund des einheitlichen Schutzstandards jedenfalls zulässig
- Bei einer Übermittlung von personenbezogenen Daten an einen Empfänger in einem Drittstaat oder eine internationale Organisation ist die Zulässigkeit zu prüfen
- Mögliche Grundlagen für eine Übermittlung
  - Angemessenheitsbeschluss der Europäischen Kommission der bestätigt, dass ein angemessenes Schutzniveau gegeben ist; liegt derzeit vor für Andorra, Argentinien, Färöer-Inseln, Guernsey, Insel Man, Israel, Jersey, Kanada, Schweiz, Uruguay

Prüfschema





Diese Nachfolgeregelung des Safe-Harbor-Abkommens (wurde vom EuGH aufgehoben) unterliegt massiver Kritik

- EU-US-Privacy Shield: Abkommen zwischen der EU und den USA nach dem sich amerikanische Unternehmen nach einer Selbstzertifizierung auf einer vom US-Handelsministerium überwachten Liste („Privacy Shield List“) eintragen können

Unternehmen die nicht auf dieser Liste eingetragen sind unterliegen nicht der Vereinbarung! Es muss ggf auf einer anderen Rechtsgrundlage übermittelt werden!

- Geeignete Garantien
- Vorliegen einer Ausnahme für bestimmte Fälle
- Bei einem Verstoß gegen die Bestimmungen können Geldstrafen iHv € 20.000.000,-- oder 4% des weltweiten letztjährigen Jahresumsatzes verhängt werden

## Rechtsdurchsetzung



- Die Datenschutzbehörde wird nicht wie bisher im Vorhinein, sondern erst bei Verstößen, oder von sich aus aktiv
- Die Datenschutzbehörde kann Geldbußen gegen als Verwaltungsstrafen gegen Unternehmen und Einzelpersonen verhängen, dagegen kann eine Beschwerde an das Bundesverwaltungsgericht erhoben werden
- Der Verantwortliche haftet für materielle und immaterielle Schäden
- Im Falle von Datenschutzvorfällen oder Beschwerden herrscht die Beweislastumkehr, dh der Verantwortliche muss beweisen, dass er nicht für das eingetretene Problem verantwortliche ist / war

## Datenschutz als kontinuierlicher Prozess



- Der Verantwortliche muss die Einhaltung der Vorschriften der DSGVO nachweisen können
- Datenschutz ist kein „einmaliger Vorgang“, sondern ein kontinuierlicher Prozess
- Regelmäßige Prüfungen, ob die vorhandenen Maßnahmen und Dokumentationen noch aktuell sind müssen durchgeführt werden
- In jedem Fall von Neuerungen bzw Neueinführung von Datenverarbeitungsprozessen sind die Bestimmungen der DSGVO anzuwenden