EU-Datenschutz-GVO

-

Was kommt da auf uns zu ?

Karsten Witt

Datenschutz

Ihr Ansprechpartner: **Karsten Witt**

Externer Datenschutzberater

aktives Mitglied im Bundesverband der Datenschutzbeauftragten Deutschlands BvD (e.V.)

Datenschutz-Auditor (TÜV)

Datenschutz ?

Datenschutz
ist ein
modernes Grundrecht !

- **Grundgesetz – Art. 1+2 - Recht auf informelle Selbstbestimmung**
- **RL 95/46/EG des europ. Parlaments u. des Rates zum Schutz natürlicher Personen bei der Verarbeitung pers.-bezogener Daten u. zum freien Datenverkehr)**
- **Ca. 400 v.Cr. – Eid des Hippocrates – ärztliche Schweigepflicht**
- **Informationsfreiheitsgesetze – 1766 Schweden, 1888 Kolumbien, 1946 UNO, 1966 USA**
- **1990 bis 2018 Bundesdatenschutzgesetz**
- **ab 25. Mai 2018: Europ. Datenschutz-Grundverordnung (DS-GVO)**

Wussten Sie, dass derzeit:

- ab 10 Mitarbeitern, welche mit EDV auf personenbezogene Daten zugreifen können ein Datenschutzbeauftragter bestellt sein muss;

- regelmäßige Datenschutzunterweisungen der MA verpflichtend sind;

- bei einer Auftragsdatenverarbeitung umfangreiche Dokumentations- und Kontrollpflichten bestehen und in den entsprechenden Aufträgen dies zwingend schriftlich zu regeln ist;

- Wirtschaftsprüfer die IT + TK-Dokumentation bei Bilanz-Testaten prüfen müssen; (Quelle : 8. EU-Vorgabe „Euro-SOX“ v. 07.06.2008)

Häufige Praxisprobleme

- Mitarbeiter auf Datenschutz + Geheimhaltung verpflichtet?
- E-Mail-Archivierung
- Unverschlüsselte Datentransporte
- Fotos von Arbeitnehmern veröffentlichen
- Privatnutzung von Internet und E-Mail geregelt
- Datenschutzerklärung auf der Website
- Umgang mit erfassten Daten (Zugangskontrollen, Arbeitszeit, Tracking…..)
- Videoüberwachung
- Heimarbeit ?
- IT-Richtlinie vorhanden ?
- Recovery-Konzept getestet ?
- Entsorgungskonzept (Papier, Datenträger, moderne Technik mit Speichern)

Ab 25.Mai 2018: EU-DSGVO

<u>Änderungen durch Datenschutz-Grundverordnung:</u>

u.a.: - europ. Angleichung zum Datenschutz (rechtliche Basis)

- Meldepflicht zur Person des Datenschutzbeauftragten

- Pflicht zur Führung eines Verarbeitungsverzeichnisses

- Risiko-/Folgenabschätzung bei jeder Verarbeitung von personenbezogenen Daten incl. deren Dokumentation

- gemeinsame Haftung von AG + AN bei Auftragsdatenverarbeitung

- weitreichendere Belehrung zur Datenspeicherung / Einwilligung

- Anforderungen ans EDV-Design

- Meldepflicht bei Datenschutz-Pannen an Aufsicht und Betroffene

……u.a.m.

Motivation zum Datenschutz?

- Die gesetzliche Verpflichtung
- Vermeiden von Beanstandungen und Bußgelder
- Wettbewerbsvorteile
- Persönliche unbegrenzte Haftung des Unternehmers / Geschäftsführers

Nachtrag zur Motivation

Sanktionen bei Verstößen (ab 2018)

- Bußgeld bis 20.000.000 € oder 4% des Konzern-Vorjahresumsatzes
- Schadenersatz
- Anordnungen zur Beendigung des Verstoßes, z.B. Rüge; Anweisung, die Datenverarbeitung den gesetzlichen Vorgaben anzupassen; zeitlich begrenzte oder endgültiges Verbot der Datenverarbeitung

Tipp:

Neu sind der Direktanspruch des Betroffenen auf gegen den Auftragsverarbeiter und die Beweislastumkehr für Datenschutzverletzungen. Dies könnte zur vermehrten Klagen führen. Unternehmen sollten sich darauf einstellen, indem Sie ihre Prozesse zur Verarbeitung personenbezogener Daten und ihre Datenschutz-Organisation gut dokumentieren, um sich jedenfalls gegen unbegründete Ansprüche angemessen verteidigen zu können.

DSGVO – was kommt da auf Unternehmen zu ?

EU-Datenschutz-Grundverordnung

99 Artikel

173 Erwägungsgrunde

… und dann auch noch das neugefasste BDSG

Struktur der DSGVO

Konzentration ! → **…das sieht doch schon besser aus**

Kapitel 2
Grundsätze
(Artikel 5 - 11)

Artikel 5 - Grundsätze für die Verarbeitung personenbezogener Daten

Artikel 6 – Rechtmäßigkeit der Verarbeitung

Artikel 7 – Bedingungen für die Einwilligung

Artikel 8 – Einwilligung eines Kindes

Artikel 9 – Verarb. Besonderer Kat. personenbezogener Daten

Artikel 10 – Verarb. pers.-bez. Daten über strafr. Verurteilungen + Straftaten

Artikel 11 – Verarb. für die eine Identifiz. der betroffenen Person nicht erforderlich ist

Kapitel 3
Rechte der betroffenen Person
(Artikel 12 - 23)

Abschnitt 1 - Transparenz und Modalitäten

Artikel 12 – Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person

Abschnitt 2 - Informationspflicht und Recht auf Auskunft zu personenbezogenen Daten

Artikel 13 – Info-Pflicht bei Erhebung von personenbez. Daten bei der betroff. Person

Artikel 14 – Informationspflicht, wenn die personenbez. Daten nicht bei der betroff. Person erhoben wurden

Artikel 15 – Auskunftsrecht der betroffenen Person

Abschnitt 3 - Berichtigung und Löschung

Artikel 16 – Recht auf Berichtigung

Artikel 17 – Recht auf Löschung („Vergessenwerden")

Artikel 18 – Recht auf Einschränkung d. Verarbeitung

Artikel 19 – Mitteilungspflicht im ZH mit der Berichtigung o. Löschung personenbez. Daten oder der Einschränkung der Verarb.

Artikel 20 – Recht auf Datenübertragbarkeit

Abschnitt 4 - Widerspruchsrecht und autom. Entscheidung im Einzelfall

Artikel 21 - Widerspruchsrecht

Artikel 22 – Autom. Entscheidungen im Einzelfall einschl. Prüfung

Abschnitt 5 - Beschränkungen

Artikel 23 - Beschränkungen

… *die* **Arbeit** *steckt hier :*

Kapitel 4

Verantwortlicher

und Auftragsverarbeiter

(Artikel 24 – 43)

... *die* Arbeit *steckt hier :*

Kapitel 4
Verantwortlicher
und Auftragsverarbeiter
(Artikel 24 – 43)

Abschnitt 1 - Allgemeine Pflichten

Artikel 24 – Verantwortung des für die Verarbeitung Verantwortlichen

Artikel 25 – Datenschutz durch Technik-Gestaltung + durch DS-freundl. Voreinstellungen

Artikel 26 – Gemeinsam für die Verarbeitung Verantwortliche

Artikel 27 – (außerhalb EU ansässige...)

Artikel 28 – Auftragsverarbeiter

Artikel 29 – Verarbeitung unter der Aufsicht des Verantwortlichen o. des Auftragsverarbeiters

Artikel 30 – Verzeichnis von Verarbeitungstätigkeiten

Artikel 31 – ZA mit der Aufsichtsbehörde

Abschnitt 2 - Sicherheit personenbez. Daten

Artikel 32 – Sicherheit der Verarbeitung

Artikel 33 – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

Artikel 34 – Benachrichtigung der von einer Verletzung des Schutzes pers.-bezog. Daten betroffene Person

Abschnitt 3 - Datenschutz-Folgenabschätzung

Artikel 35 – Datenschutz-Folgenabschätzung

Artikel 36 – Vorherige Konsultationen

Abschnitt 4 - Datenschutzbeauftragter

Artikel 37 - 39 Benennung, Stellung und Aufgaben des DSB

Abschnitt 5 - Verhaltensregeln und Zertifizierung

Artikel 40 - Verhaltensregeln

Artikel 41 – Überwachung der genehmigten Verhaltensregeln

Artikel 42 - Zertifizierung

Artikel 43 - Zertifizierungsstellen

Was müssen Sie können bzw. regeln?

Sie müssen sich auskennen mit …

1

den DSGVO –

Prinzipien

Art. 5 DSGVO - Grundsätze für die Verarbeitung personenbezogener Daten

(1) Personenbezogene Daten müssen

a) auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz“);

b) für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken („Zweckbindung“);

c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“);

d) sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („Richtigkeit“);

Art. 5 DSGVO - Grundsätze für die Verarbeitung personenbezogener Daten

e) in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („Speicherbegrenzung“);

f) in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“);

(2) Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).

Art. 4 DSGVO - Begriffsbestimmungen

(1) „personenbezogene Daten“ alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

Vor jeder neuen Verarbeitung zwingend zu prüfen:

Privacy by Design

Privacy by Default

Sie müssen sich auskennen mit …

2

den DSGVO –

Zulässigkeitstatbeständen

Rechtmäßigkeit der Verarbeitung (Art.6)

Die Verarbeitung ist nur rechtmäßig, wenn mindestens eine der nachstehenden Bedingungen erfüllt wurde:

a) Die betroffene Person hat ihre Einwilligung zu der Verarbeitung der sie betreffenden pers.-bezog. Daten für einen o. mehrere bestimmte Zwecke gegeben;

b) die Verarbeitung ist für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich, die auf Anfrage der betroffenen Person erfolgen;

c) die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt;

d) die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen;

e) die Verarbeitung ist für die Wahrnehmung einer Aufgabe erforderlich, die im öffentlichen Interesse liegt o. in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde;

f) die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz pers.-bezog. Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.

Sie müssen sich auskennen mit …

3

der DSGVO –

Einwilligung

Bedingungen für die Einwilligung (Art.7)

1. Nachweisbarkeit der Einwilligung
2. Wenn schriftliche Erklärung → zwingend in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen.
3. Recht, jederzeit zu widerrufen (dies muss auch belehrt werden).
   Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.
4. Freiwilligkeit,
   d.h. wenn die Einwilligung für die für die Erfüllung des Vertrags nicht erforderlich ist gilt ein Kopplungsverbot.

Sie müssen sich auskennen mit …

4

den neuen DSGVO –

Informationspflichten

Informationspflichten

Zum **Zeitpunkt der Erhebung** personenbezogener Daten ist zu informieren über:

1. Name + Kontaktdaten des Verantwortlichen + ggf. seines Vertreters;
2. ggf. die Kontaktdaten des Datenschutzbeauftragten;
3. die Zwecke, für die die pers.-bezog. Daten verarbeitet werden sollen, sowie die Rechtsgrundlage;
4. ggf. die berechtigten Interessen, die von dem Verantwortlichen o. einem Dritten verfolgt werden;
5. ggf. die Empfänger oder Kategorien von Empfängern der personenbezogenen Daten und
6. evtl. Absicht, die pers.-bezog. Daten an ein Drittland o. eine int. Organisation zu übermitteln,

Zusätzlich folgende Infos, um eine faire und transparente Verarbeitung zu gewährleisten:

1. die Speicherdauer bzw. die Kriterien für die Festlegung dieser Dauer;
2. das Auskunftsrecht über die betreffenden pers.-bezog. Daten sowie auf Berichtigung, Löschung oder auf Einschränkung der Verarbeitung o. eines Widerspruchsrechts gegen die Verarbeitung sowie des Rechts auf Datenübertragbarkeit;
3. das Widerrufsrecht für die Zukunft
4. das Bestehen eines Beschwerderechts bei einer Aufsichtsbehörde;
5. ob die Bereitstellung der pers.-bezog. Daten gesetzlich o. vertraglich vorgeschrieben oder für einen Vertragsabschluss erforderlich ist, ob die betroffene Person verpflichtet ist, die pers.-bezog. Daten bereitzustellen, und welche mögliche Folge die Nichtbereitstellung hätte
6. Info bei automatisierter Entscheidungsfindung einschließlich Profiling sowie ggf. aussagekräftige Informationen über die involvierte Logik sowie die Tragweite einer derartigen Verarbeitung.

Sie müssen sich auskennen mit …

5

den neuen DSGVO –

Betroffenenrechten

Betroffenenrechte

Die betroffene Person kann von dem Verantwortlichen eine Bestätigung darüber verlangen, ob dort sie betreffende personenbezogene verarbeitet werden, und wenn dies der Fall ist, welche Daten dies genau sind. (*Art. 15 Abs. 1 DS-GVO*)

Darüber hinaus sind vom Verantwortlichen mitzuteilen:

- die Verarbeitungszwecke,
- die Kategorien personenbezogener Daten, die verarbeitet werden (**neu!**),
- die gegebenen oder möglichen Datenempfänger bzw. Kategorien von Empfängern,
- soweit möglich über die geplante Speicherdauer (**neu!**),
- Informationen über die Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung sowie über ein Widerspruchsrecht nach Art. 21 DS-GVO (**neu!**),
- das Beschwerderecht bei der Aufsichtsbehörde (**neu!**),
- die Herkunft der Daten, soweit diese nicht von der/dem Betroffenen selbst erhoben wurden,
- soweit zutreffend über das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling (**neu!**).

Sie müssen sich auskennen mit …

6

der neuen DSGVO –

Auftragsverarbeitung

Verarbeitung ?

Der Begriff der „Verarbeitung“ erfasst als Oberbegriff alle Arten des „Datenumgangs“.

- *das Erheben,*
- *das Erfassen,*
- *die Organisation,*
- *das Ordnen,*
- *die Speicherung,*
- *die Anpassung oder Veränderung,*
- *das Auslesen,*
- *das Abfragen,*
- *die Verwendung,*
- *die Offenlegung durch Übermittlung,*
- *die Verbreitung oder eine andere Form der Bereitstellung,*
- *den Abgleich oder die Verknüpfung,*
- *die Einschränkung* (in Deutschland auch bekannt als „Sperrung“),
- *das Löschen oder etwa die Vernichtung*.

Auftragsverarbeitung

- Auftragsverarbeiter haben künftig mehr Verantwortung und mehr Pflichten;
- Es dürfen nur Auftragsverarbeiter eingesetzt werden, die hinreichend Garantien dafür bieten, dass sie geeignete technische und organisatorische Maßnahmen für einen ausreichenden Datenschutz haben;
- Schriftlicher oder elektronischer Vertrag erforderlich;
- Subunternehmer bedürfen vorheriger Genehmigung und müssen benannt werden
- Meldepflicht bei Datenpannen an Auftraggeber und Haftungsthematik für Auftragsverarbeiter gegenüber Betroffenen

Sie müssen sich auskennen mit …

7

den neuen DSGVO –

Datensicherheitsvorgaben

Sicherheit der Verarbeitung (Art.32)

Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte + Freiheiten natürl. Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete techn. + org. Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;
diese Maßnahmen schließen unter anderem Folgendes ein:

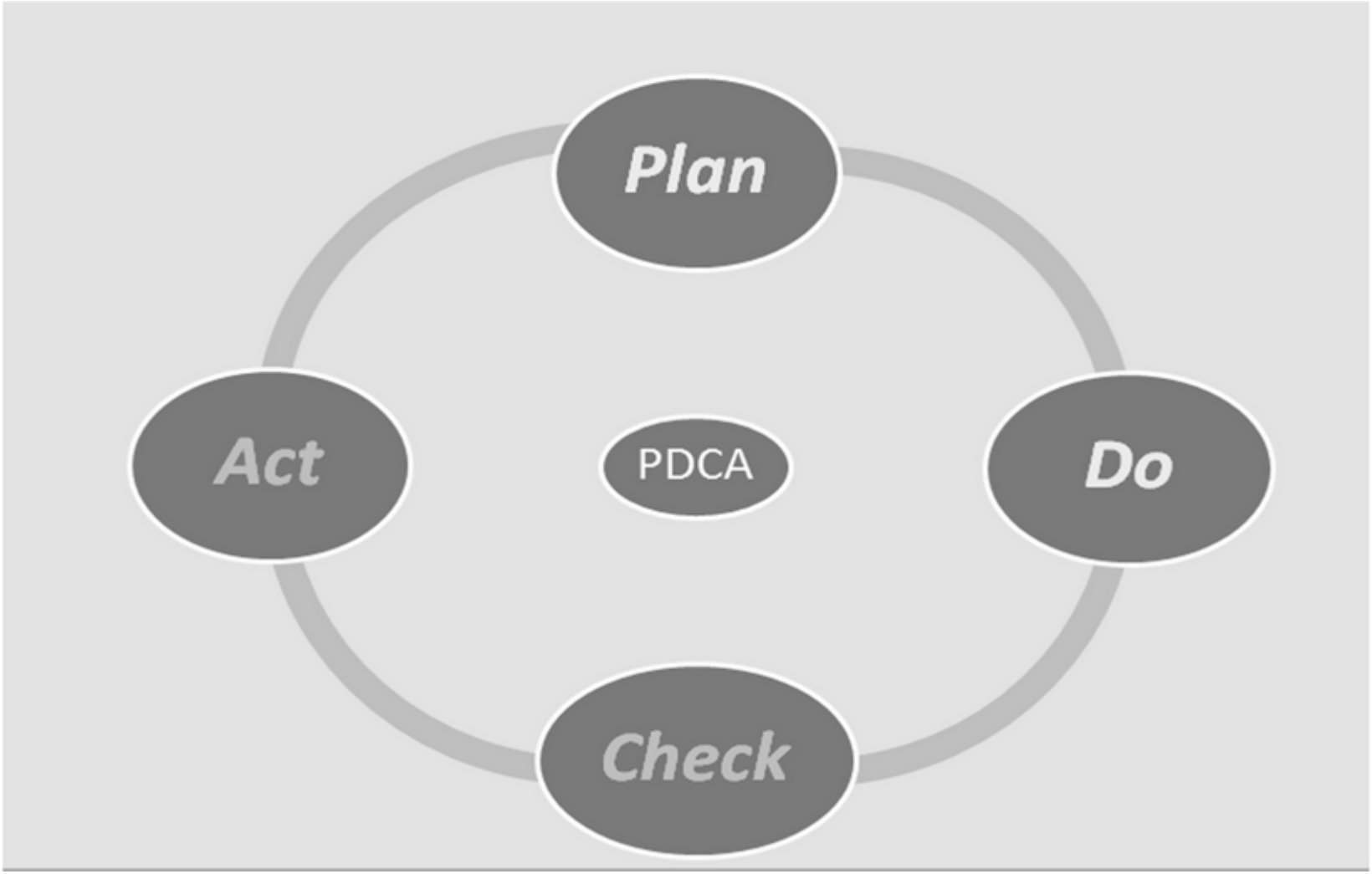
a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten;

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der pers.-bezog. Daten und den Zugang zu ihnen bei einem physischen oder techn. Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der techn. + org. Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Laufender Prozess !



Empfehlung ISMS/DMS

- Richtlinien und deren Anwendungsbereiche definieren
  (IT-Benutzer-Richtlinie, Leitlinien für Informationssicherheit,
  Mobile-Device-Policies, Notfallplan,
  Kennwort-RL, Datensicherung/Backupplanung,
  RL zur Entsorgung/Vernichtung ....)

- Risiko-/Schwachstellenanalyse

- Klassifizierung von Informationen (incl. DSB-Einbindung)

- Dokumentenlenkung & Versionierung

Empfehlung ISMS/DMS

Außerdem !

Aufzeichnungen zu Training, Fertigkeiten, Erfahrung und Qualifikationen, Überwachung, internes Audi-Programm, Resultate interner Audits, Resultate von Korrekturmaßnahmen, Protokolle über Anwenderaktivitäten, Ausnahmefälle und Sicherheitsereignisse.....

Sie müssen sich auskennen mit …

8

der neuen DSGVO –

Datenschutzfolgenabschätzung

Datenschutzfolgenabschätzung (Art. 35)

Wann? **Wenn eine Form der Verarbeitung, d. h. eine konkret durchgeführte Verarbeitungstätigkeit ein hohes Risiko für die Rechte und Freiheiten der Betroffenen mit sich bringt.**

Wie ? Das Risiko soll nach objektiven Kriterien ermittelt werden und Faktoren wie **Eintrittswahrscheinlichkeit**, **Schaden** bei der Art, Umfang, Umstände und Zweck einer konkreten Verarbeitung berücksichtigen (ErwGr. 76).

Wichtig! → Bei der Risiko-Analyse steht der Betroffene im Mittelpunkt der Betrachtung (Datenschutz-Risiko).

Was ist unter ein Schaden bezüglich Rechte und Freiheiten" zu verstehen?
ErwGr. 75 gibt hierzu Hilfestellung: Eine Verarbeitung kann demnach zu physischen, materiellen und immateriellen Schäden führen. Darunter wird beispielsweise verstanden:

- *Diskriminierung*
- *Identitätsdiebstahl*
- *Finanzieller Verlust*
- *Rufschädigung*
- *Hinderung der Kontrolle über eigene Daten*
- *Profilbildung mit Standortdaten*

Datenschutzfolgenabschätzung (Art. 35)

Risikoreduktion durch geeignete Maßnahmen

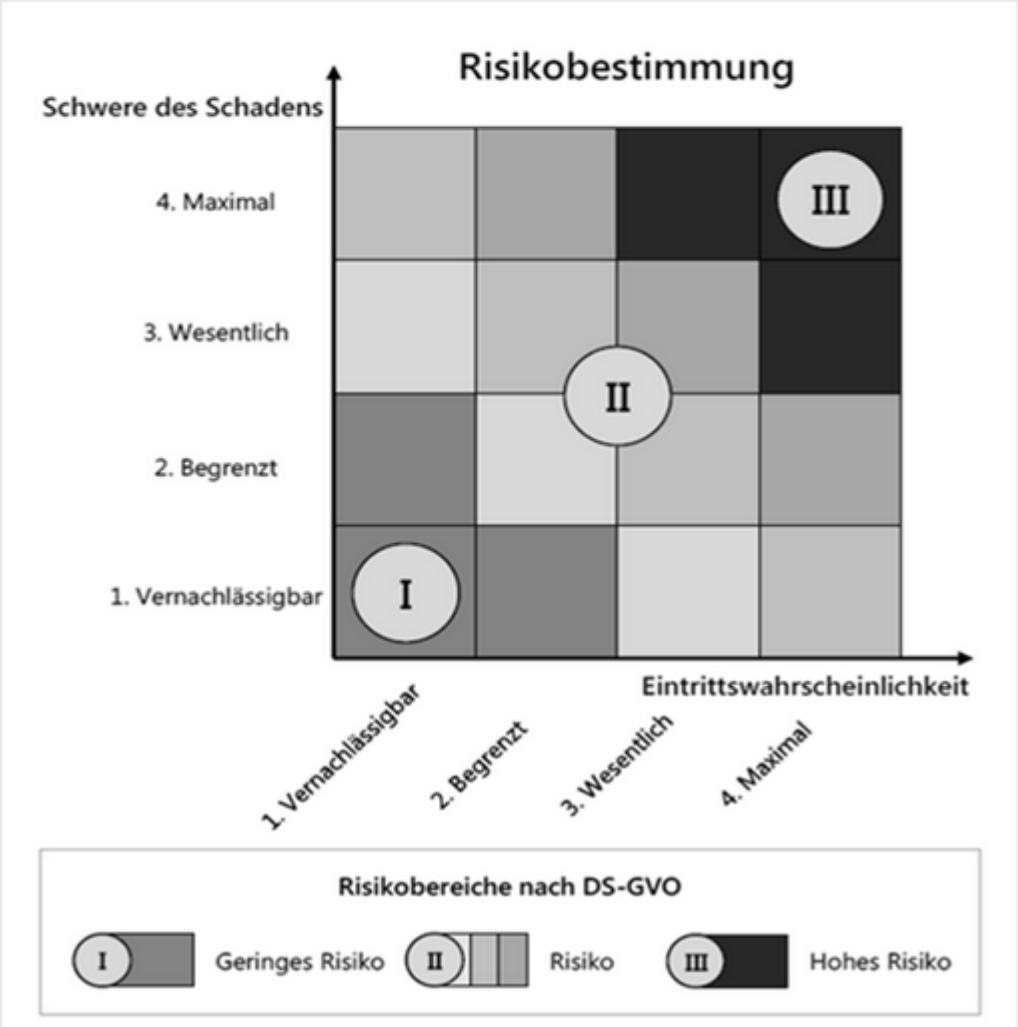
*Das Risiko einer Verarbeitung **muss** durch techn., organisat. und ggf. rechtl. Maßnahmen Reduziert werden. Dabei muss ebenfalls das Risiko und primär fahrlässiges und unrechtmäßiges Handeln interner wie externer Risikoquellen berücksichtigen.*

Inhalt einer DSFA

Eine Datenschutz-Folgenabschätzung muss eine systematische Beschreibung der Verarbeitungs-vorgänge und die Zwecke der Verarbeitung enthalten. Dazu sind (technische) Prozesse, IT-Systeme und Produkte sowie Datenflüsse und Systemgrenzen im Detail zu bewerten.

Die berechtigten Interessen des Verantwortlichen, z. B. Sicherheit durch neuartige Video-überwachung oder Erkenntnisse durch Big-Data-Analysen, sind zu beschreiben sowie die Verhältnismäßigkeit und Notwendigkeit der Verarbeitung festzulegen.
Zusätzlich ist eine systematische Risikobeurteilung (Risk-assessment) durchzuführen.
Durch geeignete Maßnahmen wird das Risiko minimiert – ist das Restrisiko dann immer noch hoch, ist die zuständige Aufsichtsbehörde zu konsultieren (Art. 36 DS-GVO).

Datenschutzfolgenabschätzung (Art. 35)



Wichtig!

→ *Bei der Risiko-Analyse steht der Betroffene im Mittelpunkt der Betrachtung.*

*Sie müssen sich **vor allem** auskennen mit …*

9

den **Datenverarbeitungsprozessen**

in Ihrem Unternehmen

Worauf konzentrieren?

- **Datenklassifizierung –** prüfen, wo im System personenbezogene Daten gespeichert sind insbesondere in unstrukturierten Formaten wie in Dokumenten, Präsentationen und Kalkulationstabellen. Das ist wichtig, um die Daten schützen und Anforderungen zum Korrigieren und Löschen von Daten nachkommen zu können.

- **Metadaten –** man muss wissen, wann, weshalb und für welchen Zweck Daten erfasst wurden. Bei personenbezogenen Daten, die in IT-Systemen gespeichert sind, sollte regelmäßig geprüft werden, ob sie weiterhin aufbewahrt werden müssen (Löschpflicht).

Worauf konzentrieren?

- **Governance –** Datenschutz durch Technik ist gesetzlich festgeschrieben. Für unstrukturierte Daten sollten Klarheit herrschen, wer personen-bezogene Daten verwendet und wer zugriffsberechtigt sein sollte. Tipp: → rollenbasierte Zugriffskontrolle einführen. Dabei erhält jeder Mitarbeiter genau die Rechte, die er braucht, um seinen Job zu machen.

- **Überwachung –** Die Meldepflicht für Sicherheitsvorfälle bedeutet : Firmen sollten in der Lage sein, ungewöhnliche Zugriffsmuster bei der Verwendung personenbezogener Daten zu erkennen und Datenschutzverletzungen unverzüglich ihrer Datenschutzbehörde zu melden. Wird das unterlassen, drohen empfindliche Geldbußen.

Verfahrensverzeichnis

Pflicht zur Führung für

- nach Art. 30 Abs. 5 DS-GVO Verantwortliche mit mehr als 250 Mitarbeitern,
- Oder wenn Verarbeitungen personenbezogener Daten durchgeführt werden,
    - die ein Risiko für die Rechte und Freiheiten der betroffenen Personen bergen (z. B. Scoring),
    - die nicht nur gelegentlich erfolgen oder
    - die besondere Datenkategorien gemäß Art. 9 Abs. 1 DS-GVO (Religionsdaten, Gesundheitsdaten, usw.) oder über strafrechtliche Verurteilungen und Straftaten betreffen.
- Auftragsverarbeiter (für die durchgeführten Verarbeitungen der Kunden)

ABER, wie wollen Sie eine Datenschutzfolgenabschätzung vornehmen,
wenn Sie nicht wissen, welche Verarbeitungen in Ihrem Unternehmen stattfinden?
Nur wer die eigenen Verarbeitungsprozesse kennt, kann gezielt Maßnahmen ergreifen, um eine rechtmäßige Verarbeitung personenbezogener Daten sicherstellen zu können.

Verfahrensverzeichnis

Inhalt des Verzeichnisses für Verantwortliche *(Art. 30 Abs. 1)*

1. den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;

2. die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden;

3. gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

4. wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Artikel 32 Absatz 1.

AUFGABE !

ZIEL

Bis zum Herbst 2017 kennen Sie sich mit den Kernregelungen der DSGVO aus und haben eine GAP-Analyse fertiggestellt. Auf deren Basis sollten Sie bestehende Lücken im Hinblick auf ihr Risiko bewerten und Maßnahmen treffen, die eine Compliance von mind. 80% bis **25.05.2018** *gewährleistet*

Datenschutzberater

Fragen?

Karsten Witt

Tel.: 0151 – 1260 1154

Witt @ BC-Datenschutz.de

www.BC-Datenschutz.de