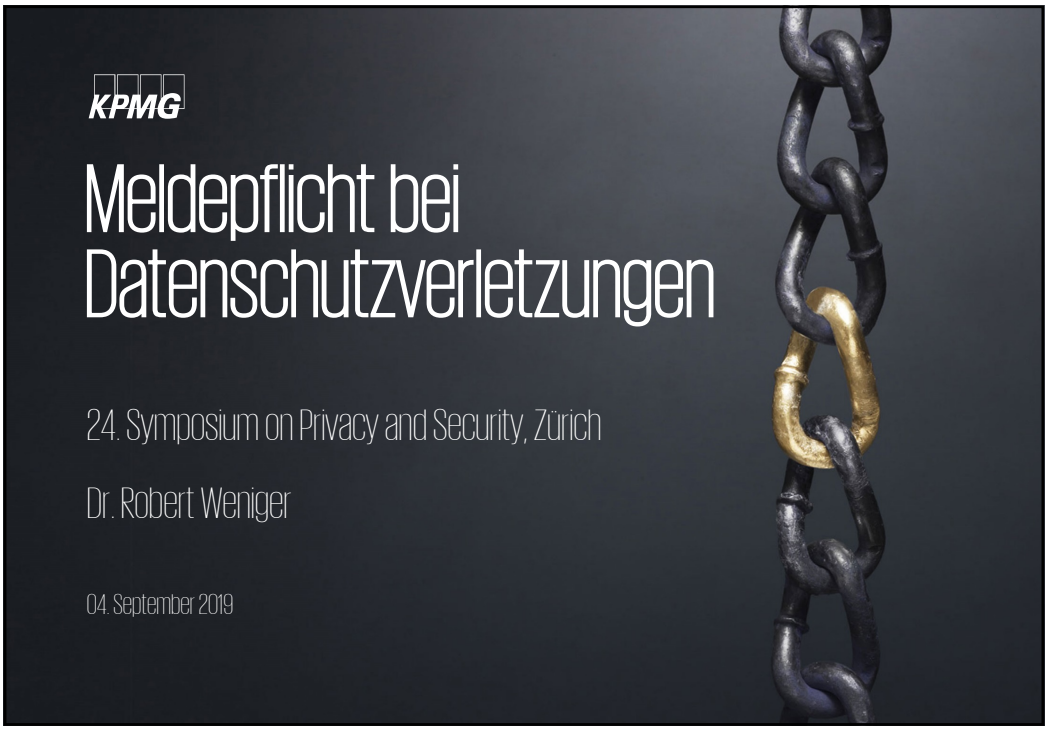


Inhalt

KPMG

Einleitung

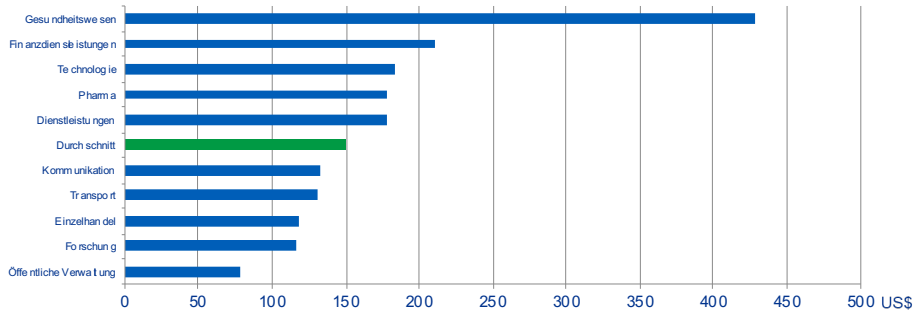
Datenschutzverletzungen

- **Datenpanne**
  - Ereignis, bei dem geheimhaltungswürde Informationen unberechtigten Dritten gegenüber mutmasslich oder erwiesenermassen bekannt geworden sind.
  - Beispiel: Person verschafft sich unbefugterweise über einen Mitarbeiter-PC Zugang zum Unternehmensnetzwerk und späht Daten aus.
- **Datenschutzverletzung**
  - Datenpanne, bei **der personenbezogene Daten** betroffen sind.
  - Beispiel: Person späht im oben genannten Beispiel Kunden- oder Mitarbeiterdaten aus.
- **Schäden**
  - Materieller oder immaterieller Nachteil sowohl für verantwortliche Stellen wie auch für betroffene Personen.

KPMG

Kosten

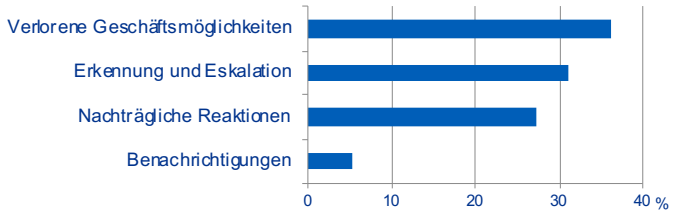
Beispielhafte Kosten einer Datenschutzverletzung pro Datensatz für unterschiedliche Wirtschaftssektoren.
Die durchschnittlichen Kosten einer Datenschutzverletzung pro Datensatz betragen 150 US $.
Eine durchschnittliche Datenschutzverletzung umfasst ca. 25.000 Datensätze.



Quelle: Cost of a Data Breach Report 2019; Conducted by Ponemon Institute; Sponsored by IBM Security

Kostenbestandteile

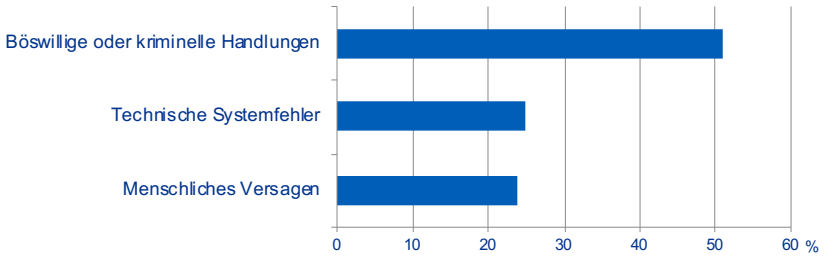
Durchschnittlicher Anteil an den Gesamtkosten einer Datenschutzverletzung bezogen auf 100%



Quelle: Cost of a Data Breach Report 2019; Conducted by Ponemon Institute; Sponsored by IBM Security

Ursachen

Durchschnittlicher Anteil aller untersuchten Ursachen von Datenschutzverletzungen bezogen auf 100%



Quelle: Cost of a Data Breach Report 2019; Conducted by Ponemon Institute; Sponsored by IBM Security

Grundlagen

Gesetzliche Grundlagen

Meldepflichten für Datenschutzverletzungen

- Art. 30 und 31 EU-Richtlinie 2016/680, Erw. 61 - 62 (EU-JI-RL)
- Art. 33 und 34 EU-Verordnung 2016/679, Erw. 85 - 88 (EU-DSGVO)
- Art. 7 Abs. 2 Datenschutzkonvention des Europarates (SEV-Nr. 108)
- Art. 15 Schengen-Datenschutzgesetz (SDSG)
- Art. 22 Entwurf Datenschutzgesetz (E-DSG)
- Art. 4 Abs. 2 DSG („Grundsatz von Treu und Glauben“)
- Weitere spezialgesetzliche Meldepflichten

Grundsätze

- **Regel:** Meldepflicht
- **Ausnahme:** Kein Risiko für die Rechte und Freiheiten der betroffenen Person
- **Differenzierung:** Meldung an Aufsichtsbehörde und an betroffene Person
- **Zeitliche Vorgaben**
- **Inhaltliche Vorgaben**
- **Dokumentationspflicht**

Zweck

- **Rechenschaftspflicht gegenüber Aufsichtsbehörde**
- **Beratung durch Aufsichtsbehörde**
- **Transparenz gegenüber betroffener Personen**
- **Begrenzung des Schadens für betroffene Person**
- **Präventivwirkung**

KPMG

Verletzung

Definitionen

- **Definitionen**
  - **Art. 4 Nr.12 EU-DSGVO:**

    „**Verletzung des Schutzes personenbezogener Daten**“: eine Verletzung der Sicherheit, die zur **Vernichtung**, zum **Verlust** oder zur **Veränderung**, ob unbeabsichtigt oder unrechtmässig, oder zur **unbefugten Offenlegung** von beziehungsweise zum **unbefugten Zugang** zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.“
  - **Art. 3 Abs. 1 lit. c SDSG:**

    „**Verletzung der Datensicherheit**“: jede Verletzung der Sicherheit, die ungeachtet der Absicht oder der Widerrechtlichkeit dazu führt, dass Personendaten **verloren** gehen, **gelöscht**, **vernichtet** oder **verändert** werden oder **Unbefugten offengelegt** oder **zugänglich** gemacht werden.“

- **Abgrenzung**
  - Im Fokus steht die Bewertung **eines Defizits der Datensicherheit** und **nicht eines Erlaubnistatbestandes.**

Formen der Verletzung

- **Verletzungshandlung**
  - Jedes Tun oder Unterlassen, ob beabsichtigt oder unbeabsichtigt.
- **Verletzungserfolg**
  - **Verletzung der Vertraulichkeit***
    Unbefugte oder unbeabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten.
  - **Verletzung der Integrität***
    Unbefugte oder unbeabsichtigte Änderung personenbezogener Daten.
  - **Verletzung der Verfügbarkeit***
    Unbefugter oder unbeabsichtigter Verlust des Zugangs zu personenbezogenen Daten oder die unbeabsichtigte oder unrechtmässige Vernichtung personenbezogener Daten.
- **Die Möglichkeit des Eintritts eines Verletzungserfolges ist bereits ausreichend.**

***Quelle**: ARTIKEL-29-DATENSCHUTZGRUPPE; WP 250rev.01; zuletzt überarbeitet und angenommen am 06.02.2018

Folgen der Verletzung

- **Physischer, materieller oder immaterieller Schaden**
- **Beispiele, vgl. Erw. 85 EU-DSGVO:**
  - Verlust der Kontrolle über die eigenen personenbezogenen Daten
  - Einschränkung der Rechte der betroffenen Personen
  - Diskriminierung
  - Identitätsdiebstahl oder -betrug
  - Finanzielle Verluste
  - Unbefugte Aufhebung der Pseudonymisierung
  - Rufschädigung
  - Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten
  - Andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile

KPMG

Reaktionsplan

Zweck und Elemente

- **Zweck**
  - **Festlegung von Verfahrensschritten**, die bei einer Datenschutzverletzung zu befolgen sind.
- **Erforderlichkeit**
  - Ohne Reaktionsplan können die **gesetzlichen Meldepflichten nur unzureichend oder überhaupt nicht erfüllt** werden.
- **Elemente**
  - **Rasche Kenntnis** von Datenschutzverletzungen.
  - **Klare Zuständigkeiten**: Wer macht was bis wann?
  - **Beurteilung der Faktenlage und des Risikos** für die betroffenen Personen.
  - **Massnahmen zur Verhinderung oder Eingrenzung des Risikos oder** gar **des** eingetretenen **Schadens.**
  - **Entscheidung, ob Meldung** gegenüber Aufsichtsbehörde und betroffenen Personen **erfolgen muss.**
  - **Durchführung der Meldung** gegenüber der Aufsichtsbehörde und den betroffenen Personen.

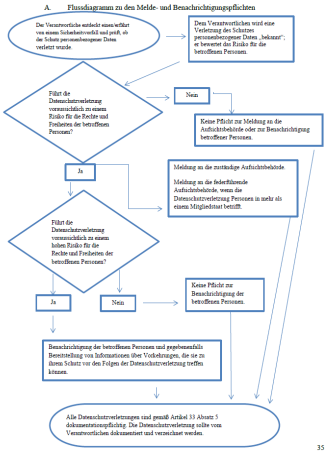
Gemeinsam Verantwortliche und Auftragsverarbeiter

- **Gemeinsam Verantwortliche**
  - Artikel 26 EU-DSGVO: Gemeinsam für die Verarbeitung Verantwortliche **legen vertraglich fest, wer von ihnen die Verpflichtungen** aus den Art. 33 und 34 EU-DSGVO **erfüllt**.
- **Auftragsverarbeiter**
  - Art. 33 Abs. 2 EU-DSGVO: **Macht dem Verantwortlichen „unverzügliche" Meldung**.
  - **Ist nicht verpflichtet, die Wahrscheinlichkeit des Risikos** für die Rechte und Freiheiten der betroffenen Personen **zu prüfen**; dies liegt in der Zuständigkeit des Verantwortlichen.
  - Art. 28 Abs. 3 lit. f EU-DSGVO: **Festlegung der Einzelheiten, nach denen die Verpflichtungen** nach Art. 33 Abs. 2 EU-DSGVO **erfüllt werden müssen**.
- **Verantwortliche und Auftragsverarbeiter ausserhalb der EU**
  - **Meldepflichten** nach Art. 33 und 34 EU-DSGVO **gelten auch für nicht in der EU niedergelassene Verantwortliche oder Auftragsverarbeiter, soweit der Anwendungsbereich der EU-DSGVO aufgrund der extraterritorialen Wirkung** nach Art. 3 Abs. 2 EU-DSGVO **eröffnet ist**.
  - **Soweit** ein **Verantwortlicher** (und Auftragsverarbeiter) **nach Art. 27 i.V.m. Art. 3 Abs. 2 EU-DSGVO einen Vertreter in der EU benannt hat**, sollen **Datenschutzverletzungen an diejenige Aufsichtsbehörde** in dem EU-Mitgliedstaat gemeldet werden, **in dem der Vertreter des Verantwortlichen niedergelassen** ist.

Schema Melde- und Benachrichtigungspflichten

VII Anhang

A. Flussdiagramm zu den Melde- und Benachrichtigungspflichten



35

Quelle: ARTIKEL-29-DATENSCHUTZGRUPPE; WP 250rev.01; zuletzt überarbeitet und angenommen am 06.02.2018

Zeitpunkt der Meldung

Wann muss gemeldet werden?

- **Zeitpunkt der Meldung gegenüber Aufsichtsbehörde**
  - Art. 33 Abs. 1 EU-DSGVO: **Unverzüglich** und möglichst **binnen 72 Stunden nach „Bekanntwerden“**.
  - Art. 15 Abs. 1 SDSG: **„So rasch wie möglich“** [nach «Bekanntwerden“].
- **Zeitpunkt der Meldung gegenüber betroffenen Personen**
  - Art. 34 Abs. 1 EU-DSGVO: Die Meldung muss **unverzüglich nach „Bekanntwerden“** erfolgen.
  - Art. 15 Abs. 4 SDSG: **Keine Konkretisierung in zeitlicher Hinsicht**; empfehlenswert **Anlehnung an Art. 15 Abs. 1 SDSG** [d.h. **„so rasch wie möglich“**]; im Übrigen „**falls der Beauftragte es verlangt**“.
- **Wann ist „bekannt“?**
  - Die Frist beginnt mit dem Zeitpunkt, ab welchem der Verantwortliche eine **hinreichende Gewissheit** darüber hat, **dass ein Sicherheitsvorfall aufgetreten ist** und die **Möglichkeit des Eintritts eines Verletzungserfolges nicht ausgeschlossen werden** kann.
  - **Unerheblich** ist, ob der **Verantwortliche** die **Datenschutzverletzung selbst festgestellt hat** oder er hierüber **durch den Auftragsverarbeiter oder durch Dritte in Kenntnis gesetzt** worden ist.

Schrittweise und verzögerte Meldung

- **Schrittweise Meldung**
  - Der **Zweck der Meldung** ist darauf ausgerichtet, **Datenschutzverletzungen und daraus resultierende Schäden umgehend zu verhindern oder einzudämmen**.
  - Das **Fehlen detaillierter Informationen**, bspw. über die genaue Anzahl der betroffenen Personen oder über das genaue Ausmass des Schadens, **stellt daher keinen Rechtfertigungsgrund für eine Nichtvornahme einer Meldung** dar.
  - Die Meldung muss vielmehr **schrittweise erfolgen**, um der Meldepflicht dennoch rechtskonform nachzukommen, vgl. Art. 33 Abs. 4 EU-DSGVO.
- **Verzögerte Meldung**
  - **Erfolgt die Meldung** an die Aufsichtsbehörde **nicht binnen 72 Stunden**, so **muss die Verzögerung begründet** werden, vgl. Artikel 33 Abs. 1 EU-DSGVO.
- **„Bündelung“**
  - Die **Meldung** von Datenschutzverletzungen **kann „gebündelt“** werden.
  - Voraussetzung ist, dass **dieselben Arten von personenbezogenen Daten auf dieselbe Weise in einem relativ kurzen Zeitraum beeinträchtigt** wurden*.

***Quelle**: ARTIKEL-29-DATENSCHUTZGRUPPE; WP 250rev.01; zuletzt überarbeitet und angenommen am 06.02.2018

KPMG

Meldung an Aufsichtsbehörde

Was muss gemeldet werden?

- **Mindestumfang an Informationen**
- **Art. 33 Abs. 3 EU-DSGVO**
  - **Art der Verletzung**
  - **Kategorien** und ungefähre **Zahl der betroffenen Personen**
  - Betroffene **Kategorien** und ungefähre **Zahl der betroffenen personenbezogenen Datensätze**
  - **Namen** und **Kontaktdaten des Datenschutzbeauftragten** oder einer sonstigen Informationsanlaufstelle
  - Wahrscheinliche **Folgen der Verletzung**
  - Vom Verantwortlichen ergriffene oder vorgeschlagene **Massnahmen zur Behebung der Verletzung** sowie **Massnahmen zur Abmilderung** möglicher **nachteiliger Auswirkungen**
- **Art. 15 Abs. 2 SDSG**
  - **Art der Verletzung**
  - **Folgen der Verletzung**
  - **Ergriffene oder vorgesehene Massnahmen um die Verletzung zu beheben**
- **Umfang der zu liefernden Informationen kann im Einzelfall auch umfassender sein**
  - **Aufsichtsbehörde muss beurteilen können, welche Risiken** sich aufgrund der Verletzungshandlung für die betroffenen Personen ergeben **und welche Massnahmen** zur Verhinderung oder Eindämmung daraus resultierender Schäden **ergriffen werden müssen**.

KPMG

Ausschluss der Meldepflicht

- **EU-DSGVO**
  - **Kein Risiko**:
    Verletzungshandlung führt voraussichtlich **nicht zu einem Risiko** für die betroffene Person,
    vgl. Art. 33 Abs. 1 EU-DSGVO.
- **SDSG**
  - **Kein hohes Risiko**:
    Verletzungshandlung führt voraussichtlich **nicht zu einem hohen Risiko** für die betroffene Person,
    vgl. Art. 15 Abs. 1 SDSG.
- **Risikoprognose ändert sich aufgrund neuer Erkenntnisse**
  - Kann dazu führen, dass eine Meldung erforderlich wird.

Meldung an Betroffene

Was muss gemeldet werden?

- **Mindestumfang an Informationen**
- **Art. 34 Abs. 2 EU-DSGVO** (i.V.m. Art. 33 Abs. 3 lit. b, c und d EU-DSGVO)
  - **Art der Verletzung**
  - **Namen** und **Kontaktdaten des Datenschutzbeauftragten** oder einer sonstigen Informationsanlaufstelle
  - Wahrscheinliche **Folgen der Verletzung**
  - Vom Verantwortlichen ergriffene oder vorgeschlagene **Massnahmen zur Behebung der Verletzung** sowie **Massnahmen zur Abmilderung** möglicher **nachteiliger Auswirkungen**
- **Art. 15 Abs. 2 SDSG**
  - **Keine Konkretisierung in inhaltlicher Hinsicht**; empfehlenswert **Anlehnung an Art. 15 Abs. 2 SDSG**, d.h.:
    - **Art der Verletzung**
    - **Folgen der Verletzung**
    - **Ergriffene oder vorgesehene Massnahmen um die Verletzung zu beheben**

Wie muss gemeldet werden?

- **Grundsatz***
  - **Direkte Kontaktaufnahme** bspw. per Telefon, E-Mail, SMS, postalische Mitteilungen.
- **Ausnahme***
  - Bei **unverhältnismässig hohem Aufwand** soll eine **öffentliche Bekanntmachung** oder eine **ähnliche Massnahme** erfolgen, mit der betroffene Personen wirksam benachrichtigt werden, bspw. Meldung auf Webseiten, Anzeigen in Printmedien.
  - Je nach Einzelfall **mehrere Benachrichtigungsmassnahmen über unterschiedliche Kommunikationskanäle.**
- **Transparenz***
  - Benachrichtigung soll **nicht zusammen mit anderen Informationen** verschickt werden, bspw. mit regelmässigen Updates, Newslettern oder Standardmitteilungen.
- **Verständnis***
  - Benachrichtigung muss **in den relevanten Sprachversionen** (bspw. Landessprache) erfolgen, damit die betroffenen Personen die vermittelten Informationen verstehen können.

***Quelle**: ARTIKEL-29-DATENSCHUTZGRUPPE; WP 250rev.01; zuletzt überarbeitet und angenommen am 06.02.2018

Ausschluss der Meldepflicht

➲ **EU-DSGVO**

- **Kein hohes Risiko**, vgl. Art. 34 Abs. 1 EU-DSGVO
- **Präventive Sicherheitsvorkehrungen**, vgl. Art. 34 Abs. 3 lit. a EU-DSGVO
- **Repressive Sicherheitsmassnahmen**, vgl. Art. 34 Abs. 3 lit. b EU-DSGVO
- **Unverhältnismässiger Aufwand**, vgl. Art. 34 Abs. 3 lit. c EU-DSGVO

➲ **SDSG**

- **Kein hohes Risiko**, Umkehrschluss zu Art. 15 Abs. 1 SDSG
- **Überwiegende Interessen Dritter**, vgl. Art. 15 Abs. 5 lit. a SDSG
- **Überwiegende öffentliche Interessen,** vgl. Art. 15 Abs. 5 lit. b SDSG
- **Gefährdung einer Ermittlung, einer Untersuchung oder eines behördlichen oder gerichtlichen Verfahrens**, vgl. Art. 15 Abs. 5 lit. c SDSG
- **Unmöglichkeit oder unverhältnismässiger Aufwand**, vgl. Art. 15 Abs. 5 lit. d SDSG
- **Information der betroffenen Person ist durch öffentliche Bekanntmachung sichergestellt**, vgl. Art. 15 Abs. 5 lit. e SDSG

KPMG

Risikobewertung

Was ist ein Risiko?

- **Vorliegen eines Risikos als Grundvoraussetzung**
  - Verpflichtung zur Meldung gegenüber der Aufsichtsbehörde resp. den betroffenen Personen ist an das **voraussichtliche Vorliegen eines Risikos resp. eines hohen Risikos** gebunden.
  - Deshalb erforderlich, dass **Verantwortlicher unmittelbar nachdem ihm eine Datenschutzverletzung bekannt wird prüft, welches Risiko** mit der Verletzungshandlung verbunden sein könnte.
- **Begriff des Risikos ist in der EU-DSGVO nicht ausdrücklich definiert.**
- **Deutsche Datenschutzkonferenz (DSK) liefert** unter Hinweis auf Erw. 75 und 94 Satz 2 EU-DSGVO **folgende Definition***:
  - „**Ein Risiko** im Sinne der DS-GVO **ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden** […] **darstellt oder zu einem weiteren Schaden** für eine oder mehrere natürliche Personen **führen kann**."
- **Schaden**
  - **Physischer, materieller oder immaterieller Schaden**, vgl. hierzu Folie „Folgen der Verletzung "

*__Quelle__: DSK Kurzpapier Nr. 18 - Risiko für die Rechte und Freiheiten natürlicher Personen, Stand: 26.04.2018

Zu berücksichtigende Faktoren

- **Prognoseentscheidung**
  - Risikobewertung **muss den spezifischen Umständen der Datenschutzverletzung Rechnung tragen**, insbesondere:
    - **Schwere** des potentiellen Schadens
    - **Eintrittswahrscheinlichkeit** des Schadens
- **In die Bewertung einzubeziehende Faktoren***
  - Art der Datenschutzverletzung
  - Art, Sensibilität und Umfang personenbezogener Daten
  - Identifizierbarkeit betroffener Personen
  - Schwere der Folgen für die betroffenen Personen
  - Besondere Eigenschaften der betroffenen Personen
  - Besondere Eigenschaften des Verantwortlichen
  - Die Anzahl der betroffenen Personen
  - Allgemeine Aspekte

*__Quelle__: ARTIKEL-29-DATENSCHUTZGRUPPE; WP 250rev.01; zuletzt überarbeitet und angenommen am 06.02.2018

Methodik

Die **Agentur der Europäischen Union für Netz- und Informationssicherheit (ENISA)** hat zusammen mit den Datenschutz-aufsichtsbehörden von Griechenland (Hellenic Data Protection Authority - HDPA) und Deutschland (Bundesbeauftragter für den Datenschutz und die Informationsfreiheit - BfDI) **eine Methodik zur Bewertung der Schwere von Datenschutzverletzungen entwickelt*, die sowohl von Aufsichtsbehörden als auch von Verantwortlichen verwendet werden kann:**

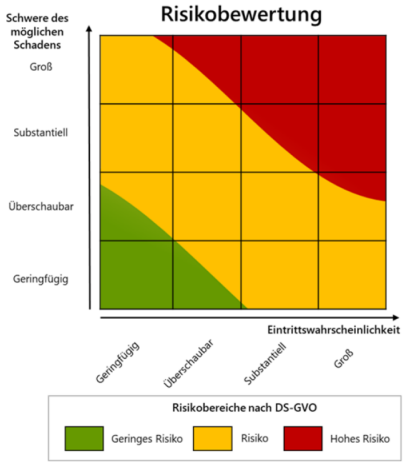
- **Hauptkriterien**, die bei der Beurteilung der Schwere einer Verletzung personenbezogener Daten berücksichtigt werden:
  - **Datenverarbeitungskontext (DPC)**: Berücksichtigt die Art der verletzten Daten sowie eine Reihe von Faktoren, die im Verarbeitungskontext stehen.
  - **Einfachheit der Identifizierung (EI)**: Legt fest, wie leicht sich die Identität der Personen aus den von der Verletzung betroffenen Daten ableiten lässt.
  - **Umstände der Verletzung (CB)**: Adressiert die spezifischen Umstände, die mit der Art des Verstosses zusammenhängen, einschliesslich des Verlustes der Vertraulichkeit, der Integrität, der Verfügbarkeit der Daten sowie des Vorliegens böswilliger Absicht.

- **Wert der Schweregradbeurteilung wird anhand folgender Formel berechnet : SE = DPC x EI + CB**
  - Ergebnis gehört zu einem bestimmten **Wertebereich**, der einem der folgenden **vier Schweregrade** entspricht: **niedrig, mittel, hoch und sehr hoch.**
  - Zusätzlich können **weitere mögliche relevante Kriterien** (bspw. Anzahl der Personen und Unverständlichkeit der Daten), in die Bewertung eingebunden werden.

- Berechneter **Schweregrad der Verletzung kann genutzt werden, um festzustellen, ob es notwendig ist, die Aufsichtsbehörde und betroffene Personen zu benachrichtigen**.

*__Quelle:__ ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches, Working Document, v1.0, December 2013

Risikomatrix



- **Orientierungshilfe der deutschen Datenschutzkonferenz** (DSK)*
- **Ziel** der Risikomatrix:
  - **Abschätzung des Risikos** der Verarbeitung, indem die **Eintrittswahrscheinlichkeit** mit **der Schwere des möglichen Schadens in Relation gesetzt** wird.

*__Quelle__: DSK Kurzpapier Nr. 18 - Risiko für die Rechte und Freiheiten natürlicher Personen, Stand: 26.04.2018

KPMG

Dokumentation

Dokumentationspflicht für Verantwortliche

- Folgt aus Art. 33 Abs. 5 EU-DSGVO
- Betrifft **alle Datenschutzverletzungen**, **unabhängig davon, ob diese meldepflichtig sind oder nicht**.
- Ergibt sich aus:
  - **Grundsatz der Rechenschaftspflicht** des Verantwortlichen nach Art. 5 Abs. 2 EU-DSGVO
  - **Generalnorm für die Rolle und Verantwortung** des Verantwortlichen nach Artikel 24 EU-DSGVO
- Anlegung eines **internen Verzeichnisses für Datenschutzverletzungen**
  - **Inhalt orientiert sich an Art. 33 Abs. 3 EU-DSGVO**
  - **Angaben zu folgenden Aspekten:**
    - Vorkommnisse und deren Ursachen
    - Beeinträchtigte personenbezogenen Daten
    - Auswirkungen der Datenschutzverletzung
    - Getroffenen Abhilfemassnahmen
    - Begründung, warum der Verantwortliche zu dem Schluss gekommen ist, dass die Datenschutzverletzung voraussichtlich zu einem (hohen) Risiko oder nicht zu einem (hohen) Risiko für die betroffenen Personen führt*.

***Quelle**: ARTIKEL-29-DATENSCHUTZGRUPPE; WP 250rev.01; zuletzt überarbeitet und angenommen am 06.02.2018

KPMG

Sanktionen und Haftung

Abhilfebefugnisse der Aufsichtsbehörden

- **EU-DSGVO**
  - **Abhilfemassnahmen**, vgl. Art. 58 Abs. 2 EU-DSGVO
    - Warnung, Verwarnung, Anweisung, Verhängung einer Beschränkung oder eines Verbots etc.
  - **Geldbussen**, vgl. Art. 58 Abs. 2 lit. i i.V.m. Art. 83 Abs. 4 lit. a EU-DSGVO
    - Bis zu **10 Mio. EUR** oder im Fall eines Unternehmens von bis zu **2 % des gesamten weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres.
    - Kann **zusätzlich oder anstelle von den übrigen** in Art. 58 Abs. 2 EU-DSGVO genannten **Abhilfemassnahmen verhängt** werden.
- **SDSG**
  - **Verwaltungsmassnahmen**, vgl. Art. 24 SDSG
    - Verwarnung, Verfügung, Aufschiebung oder Untersagung der Bekanntgabe von Personendaten.
    - Die mit der Untersuchung verbundenen Verfahren sowie die Verfügungen selbst richten sich nach dem VwVG, vgl. Art. 25 Abs. 1 SDSG.

Haftung für Schäden

- **EU-DSGVO**
  - **Anspruch auf Schadenersatz** gegen den Verantwortlichen oder gegen den Auftragsverarbeiter **als eigenständige datenschutzrechtliche Haftungsnorm**, vgl. Art. 82 Abs. 1 EU-DSGVO.
  - **Verschuldensvermutung**, vgl. Art. 82 Abs. 2 EU-DSGVO und **Beweislastumkehr**, vgl. Art. 82 Abs. 3 DSGVO i.V.m. Erw. 146.
  - **Betroffene Personen können** dadurch **einfacher** einen **erlittenen Schaden einklagen.**
- **SDSG**
  - **Anspruch auf Schadensersatz nicht im SDSG geregelt**.
  - **Anspruch richtet sich** nach dem **Bundesgesetz über die Verantwortlichkeit des Bundes sowie seiner Behördenmitglieder und Beamten** (Verantwortlichkeitsgesetz - VG).

KPMG

Hilfsmaterialien

Formulare, Leitlinien, Checklisten, FAQ

➲ **Meldeformulare:**

- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit: https://www.bfdi.bund.de/DE/Service/Datenschutzverstoesse/datenschutzverstoesse_node.html#bfdi
- Österreich, Datenschutzbehörde: https://www.dsb.gv.at/at.gv.bka.liferay-app/documents/227558/844171/Meldung+von+Verletzungen+des+Schutzes+personenbezogener+Daten+gem%C3%A4%C3%9F+Art.+33+DSGVO.pdf/cffc6756-1996-460d-a0bc-c5a29b4889ff
- Fürstentum Liechtenstein, Datenschutzstelle: https://formulare.llv.li/formserver_DSS/start.do?generalId=DSS_VD&event=PrintEmptyFormPdf&emptyFormPrint.isPrintSelectionList=false&emptyFormPrint.isPrintHelp=false&emptyFormPrint.block.repetition=INI&emptyFormPrint.block.selection=PS&emptyFormPrint.pdfHeaderFile=afs/html/Leerformular_Header.st
- Bayerisches Landesamt für Datenschutzaufsicht: https://www.lda.bayern.de/de/datenpanne.html
- Der Hessische Beauftragte für Datenschutz und Informationsfreiheit: https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Formular%20Art%2033.docx
- Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: https://www.ldi.nrw.de/mainmenu_Aktuelles/Formulare-und-Meldungen/Inhalt2/Meldeformular---Verletzung-des-Schutzes-personenbezogener-Daten/formular_art33.pdf

➲ **Leitlinien / Checklisten / FAQ:**

- Artikel-29-Datenschutzgruppe, WP 250rev.01: https://www.datenschutzkonferenz-online.de/media/wp/20180206_wp250_rev01.docx
- ENISA, Recommendations for a methodology of the assessment of severity of personal data breaches: https://www.enisa.europa.eu/publications/dbn-severity
- UK Information Commissioner's Office (ICO), Personal data breaches: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/personal-data-breaches/
- Datenschutzkonferenz - DSK, Kurzpapier Nr. 18: https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf
- Finland Office of the Data Protection Ombudsman: https://tietosuoja.fi/en/personal-data-breaches
- Europäischer Datenschutzbeauftragter, Leitlinien zur Meldung von Verletzungen des Schutzes personenbezogener Daten: https://edps.europa.eu/sites/edp/files/publication/18-12-14_edps_guidelines_data_breach_de.pdf
- Landesbeauftragte für den Datenschutz Niedersachsen, Meldung von Datenschutzverstössen; Fragen und Antworten zur DS-GVO: https://lfd.niedersachsen.de/startseite/datenschutzreform/dsgvo/faq/meldung-von-datenschutzverstoeen-167312.html

KPMG

Vielen Dank!

Fragen?

Dr. Robert Weniger
Director
Information Governance & Compliance

T: +41 58 249 70 19
E: rweniger@kpmg.com