SCHÜRMANN
ROSENTHAL
DREYER
RECHTSANWÄLTE

DIGITALES BUSINESS · TECHNOLOGIE · MEDIEN

Meldepflichten bei Datenschutzvorfällen

Wie sieht proaktiver Datenschutz aus?

Simone Rosenthal
Rechtsanwältin, Partnerin

Ilan Leonard Selz, LL.M. (Minnesota)
Rechtsanwalt, Senior Associate

Empfehlungen:

JUVE HANDBUCH 2020|2021

JUVE AWARDS 2020
Kanzlei des Jahres für IT und Datenschutz

JUVE AWARDS 2020
Kanzlei des Jahres für Technologie und Medien

The LEGAL 500 DEUTSCHLAND
FÜHRENDE KANZLEI 2022

Referenten

Simone Rosenthal

Rechtsanwältin, Partnerin

rosenthal@srd-rechtsanwaelte.de

Ilan Leonard Selz, LL.M. (Minnesota)

Rechtsanwalt, Senior Associate

selz@srd-rechtsanwaelte.de

Agenda
Proaktives Management von DS-Vorfällen

01 Einführung

02 Meldepflicht nach Art. 33, 34 DSGVO

03 Präventive Maßnahmen zur Verhinderung von Datenschutzvorfällen

04 Fazit

1. Einführung

1.1 Datenschutzvorfall bei booking.com

- Im Dezember 2018 wurden Datensätze von über 4.000 Kundinnen und Kunden von booking.com gestohlen
- Darunter waren insbesondere Namen, Adressen, Telefonnummern, Buchungsangaben sowie Kreditkarteninformationen (einschließlich Sicherheitsnummern) betroffen
- Booking.com erfuhr am 13.01.2019 von dem Vorfall
- Die Betroffenen wurden erst am 04.02.2019 darüber informiert
- Eine Meldung an die Datenschutzbehörde erfolgte erst am 07.02.2019 – mehr als 3 Wochen nach Bekanntwerden des Vorfalls
- Deswegen verhängte die Niederländische Datenschutzaufsichtsbehörde (Autoriteit Persoonsgegevens) ein Bußgeld in Höhe von 475.000 Euro wegen verspäteter Meldung

1.2 Typische Vorfälle

- E-Mail-Versand an falschen Adressaten
- Empfänger im Cc statt Bcc
- Hacking, Phishing, Ransomware, Abgreifen von Passwörtern, Brute-Force etc.
- Kontodaten aus Rechnung werden veröffentlicht
- Socail-Engineering
- Vorfälle bei Dienstleistern
- Zugangsmöglichkeit zu internen Datenbanken
- unbefugte interne Verarbeitungen (z.B. Zugriff auf Beschäftigtendaten durch Belegschaft)
- Verlust von Datenträgern
- Datendiebstahl durch einen ehemaligen Mitarbeiter

2. Grundlagen zur Meldepflicht (Art. 33, 34 DSGVO)

2.1 Melde- bzw. Benachrichtigungspflicht nach Art. 33, 34 DSGVO

2.2 Übersicht über die Meldepflichten

Risiko\Pflichten	Interne Dokumentationspflicht (Art. 33 Abs. 5 DS-GVO)	Meldepflicht an zuständige Aufsichtsbehörde (Art. 33 Abs. 1 DS-GVO)	Benachrichtigungspflicht gegenüber den betroffenen Personen (Art. 34 DS-GVO)
Voraussichtlich kein Risiko (geringes Risiko streitig)	ja	nein	nein
Risiko	ja	ja	nein
Hohes Risiko	ja	ja	ja

2.3 Prüfungsschema Art. 33 DSGVO

1. Verletzung des Schutzes pbD
   a. Verletzung der Sicherheit
   b. Drauf beruhend Verlust, Veränderung, Offenlegung, Zugang
2. Risikoanalyse (Prognoseentscheidung)
   a. Welche Risiken für die Betroffenen Personen bestehen?
   b. Für Jedes Risiko Eintrittswahrscheinlichkeit
3. Rechtsfolge: unverzügliche Meldung, es sei denn *voraussichtlich* kein Risiko

2.4 Was ist eine Verletzung des Schutzes personenbezogener Daten?

Verletzung des Schutzes personenbezogener Daten ist nach Art. 4 Nr. 12 DSGVO (vgl. auch WP 250) eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig zu

- Vernichtung oder Verlust von Daten (*„Availability breach“*)
- Veränderung von Daten (*„Integrity breach“*)
- Unbefugte Offenlegung von Daten oder unbefugter Zugang zu Daten (*„Confidentiality breach“*)

führt.

Unerheblich ist, ob der Vorfall **absichtlich** oder **rechtmäßig** oder durch **wen** er erfolgte!

Versand von Daten an **falsche Person** (z.B. falsche E-Mail-Adresse)

Diebstahl oder **Verlust** von (unverschlüsselten) Datenträgern / Dokumenten

Datenlecks durch Softwarefehler (z.B. fehlende Updates)

Abgreifen von Daten durch **Cyberangriffe** (und ggf. anschließende Veröffentlichung im Internet)

Versehentliche Änderung von Daten

Unbeabsichtigte Löschung von Daten

(Vorrübergehende) Nicht-Verfügbarkeit aufgrund von DDOS-Attacke ?!

2.4 Was ist ein Risiko für die Rechte und Freiheiten natürlicher Personen? (1)

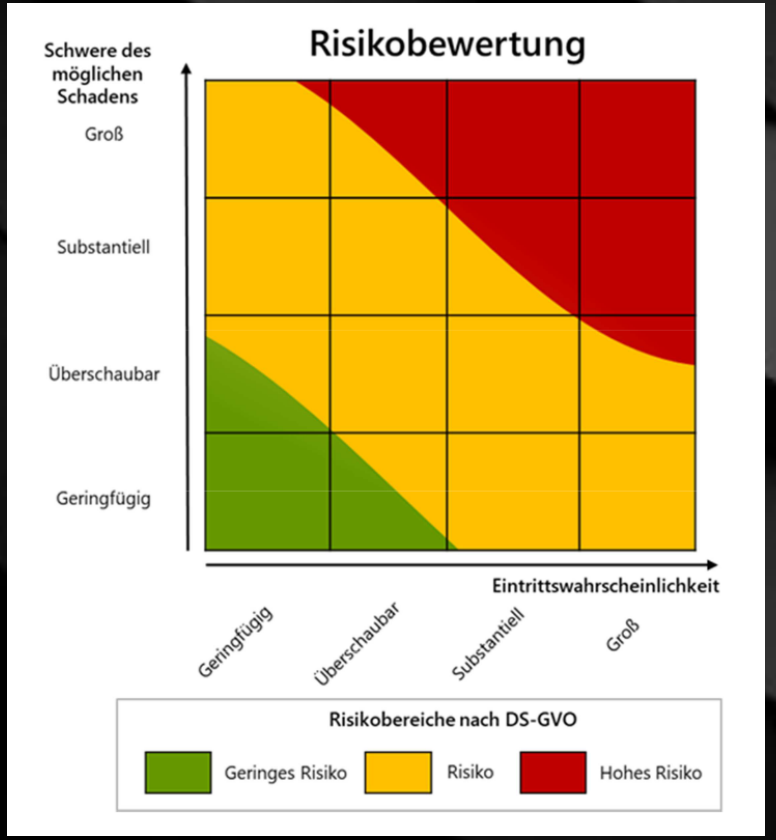
„Rechte und Freiheiten natürlicher Personen“ umfassen insbesondere die **Rechte der Europäischen Grundrechtecharta** (GRCh) – nicht nur informationelle Selbstbestimmung, z.B.:

- Recht auf körperliche und geistige Unversehrtheit (Art. 3 GRCh)
- Achtung des Privat- und Familienlebens (Art. 7 GRCh)
- Schutz personenbezogener Daten (Art. 8 GRCh)
- Gedanken-, Gewissens- und Religionsfreiheit (Art. 10 GRCh)
- Meinungs- und Informationsfreiheit (Art. 11 GRCh)
- Eigentumsrecht (Art. 17 GRCh)
- Nichtdiskriminierung (Art. 21 GRCh)

→ Beispiele im EDSA „Guidelines 01/2021 on Examples regarding Data Breach Notification“ – V 2.0 für Einschätzung hilfreich

2.4 Was ist ein Risiko für die Rechte und Freiheiten natürlicher Personen? (2)

- ***„Risiko“*** = die **Möglichkeit des Eintritts** eines Ereignisses, das **selbst einen Schaden darstellt** oder **zu einem weiteren** Schäden für eine oder mehrere natürliche Personen **führen kann** (vgl. ***DSK Kurzpapier 18***)
- ***„Schaden“*** = alle möglichen **physischen**, **materiellen** und **immateriellen Beeinträchtigungen** (vgl. ***ErwG 75***)
- Das Risiko wird aus der **Schadenshöhe** (Schwere der Folgen) und der **Eintrittswahrscheinlichkeit** ermittelt (vgl. ***DSK Kurzpapier 18***) – siehe nächste Folie
- Notwendig ist eine **Risikoanalyse** anhand abstrakter und konkreter Kriterien, gemäß ***ErwG 76*** und ***WP 250*** u.a.
  - **Art** des **Datenschutzvorfalls**
  - **Art**, **Sensibilität** und **Umfang** der betroffenen Daten
  - **Kategorie**, **Anzahl** und **Identifizierbarkeit** der betroffenen Personen
  - **Auswirkungen** für die betroffenen Personen
- In der Praxis kann die Ermittlung des Risikos mithilfe einer **Risikomatrix** erfolgen – so ergeben sich geringe, mittlere und hohen Risiken



2.4 Was ist ein Risiko für die Rechte und Freiheiten natürlicher Personen? (3)

Eintrittswahrscheinlichkeit

- Beschreibt die Wahrscheinlichkeit, **dass ein Schaden eintritt**
- Mit umfasst ist auch die Wahrscheinlichkeit von **Folgeschäden**
- Somit sind sowohl die **unmittelbaren Folgen**, etwa einer Offenlegung, und die **mittelbaren Folgen**, etwa der Weiternutzung der offengelegten Daten, zu berücksichtigen
- Relevant ist auch, wie **viele Risikoquellen** die Schäden hervorrufen können und welche **Erfahrungen in der Vergangenheit** bereits gemacht wurden

Schadenshöhe

Ein hoher Schaden könnte insbesondere anzunehmen sein bei (vgl. ***DSK Kurzpapier 18***):

- Sensible Daten nach **Art. 9 DSGVO** (z.B. Gesundheitsdaten)
- Besonders **geschützte Personengruppen** (z.B. Kinder, Beschäftigte)
- Eindeutig identifizierbare Daten (z.B. IBAN, Personalausweisnummer, sonstige **Identifikationsnummern**)
- **Profiling** (z.B. Nutzungsprofil)
- **Nicht rückgängig** zu machende Schäden
- **Große Anzahl** betroffener Personen oder Daten

2.4 Was ist ein Risiko für die Rechte und Freiheiten natürlicher Personen? (4)

Beispiele für Risiken aus dem Erwägungsgrund 75

Kontrollverlust	Einschränkung der Rechte der Betroffenen	Diskriminierung	Identitätsdiebstahl	Aufhebung der Pseudonymisierung
Rufschädigung	Finanzielle Verluste (außer marginale Vermögensschäden)	Verlust der Vertraulichkeit von dem Berufsgeheimnis unterliegenden Daten	Offenlegung sensibler Daten nach Art. 9 DSGVO	Offenlegung der Bewertung persönlicher Aspekte oder eines persönlichen Profils

2.5 Wann wird dem Unternehmen eine Verletzung „bekannt“?

- Verlangt wird ein ***„angemessener Grad an Gewissheit“***, dass eine Verletzung personenbezogener Daten stattgefunden hat (so ***WP 250***)
- Der genaue Zeitpunkt ist jedoch von den **Umständen des Einzelfalls** abhängig, insbesondere ob weitere **Nachforschungen / Untersuchungen** nötig sind
- Die Nachforschungen **müssen umgehend erfolgen** – dies ist durch entsprechende Prozesse sicherzustellen
- Umstritten ist, ob die **Kenntnis des Auftragsverarbeiters zugerechnet** wird oder die Frist erst nach Informierung über den Vorfall beginnt (so ***WP 250***)
- In jedem Fall besteht jedoch die **Pflicht**, **Prozesse** zu etablieren, damit der Auftragsverarbeiter Datenschutzvorfälle **schnell** an den Verantwortlichen **meldet**

Verloren gegangener **unverschlüsselter USB-Stick** mit Kundendaten
= Frist beginnt mit Kenntnisnahme

Auftragsverarbeiter **informiert Verantwortlichen einschließlich Beweisen** über einen Vorfall
= Frist beginnt mit Kenntnisnahme

Verantwortlicher geht **ungewöhnlichen Aktivitäten im Netzwerk** nach
= Frist beginnt erst, nachdem ein unbefugtes Eindringen festgestellt wurde

Cyberkrimineller behauptet den **Diebstahl von Kundendaten**
= Frist beginnt erst, nachdem der Cyberangriff durch die IT bestätigt wurde

2.6 Wie erfolgt eine Meldung an die Aufsichtsbehörde? (Art. 33 DSGVO)

Wie?	An wen?

• **Unverzüglich** nach Kenntniserlangung – Details siehe nächste Folie
• „Möglichst **binnen 72 Stunden**“
• Mindestens folgende **Angaben:**
  • **Beschreibung** des Vorfalls (Wer? Was? Wann? Wo? Wie?)
  • **Name und Kontaktdaten**
  • Beschreibung der **wahrscheinlichen Folgen**
  • Ergriffene / geplante **Maßnahmen**
	• *„zuständige Aufsichtsbehörde“* (Art. 55, Art. 4 Nr. 22), i.d.R. am **Unternehmenssitz**
	• Ausnahme bei mehreren zuständigen Behörden: die ***„federführende Aufsichtsbehörde“*** (Art. 56), d.h. bei der Niederlassung, welche die Mittel und Zwecke der Verarbeitung bestimmt

2.7 Wie erfolgt eine Benachrichtigung an die betroffene Person? (Art. 34 DSGVO)

Wie?	An wen?

• **Unverzüglich** nach Kenntniserlangung
• Mindestens folgende **Angaben:**
  • **Beschreibung** des Vorfalls in **klarer** und **einfacher Sprache** (Wer? Was? Wann? Wo? Wie?)
  • **Name und Kontaktdaten**
  • Beschreibung der **wahrscheinlichen Folgen**
  • Ergriffene / geplante **Maßnahmen**
	• Grundsätzlich an die **betroffene Person direkt**
	• Ausnahme: die individuelle Benachrichtigung wäre mit einem **unverhältnismäßigen Aufwand** verbunden (Art. 34 Abs. 3 lit. c) – dann reicht eine **öffentliche Bekanntmachung oder ähnliches** aus

2.8 Wie kann eine fehlende Meldung bzw. Benachrichtigung sanktioniert werden?

Verhängung von Bußgeld bei

- **Verstoß** gegen die **Melde-** bzw. **Benachrichtigungspflicht** nach Art. 33 oder 34 DSGVO (Art. 83 Abs. 4 lit. a DSGVO)
- **Weigerung** gegen die **Anweisung** der Behörde nach Art. 58 Abs. 2 lit. e, die Betroffenen zu informieren (Art. 83 Abs. 6 DSGVO)

Weitere behördliche Befugnisse

- **Aufforderung** nach Art. 34 Abs. 4, die Benachrichtigung der betroffenen Person nachzuholen
- **Anweisung** nach Art. 58 Abs. 2 lit. e, die betroffene Person zu benachrichtigen
- **Benachrichtigung** der Betroffenen **durch die Behörde** selbst? Umstritten! – aber mehrheitlich **abgelehnt**

3. Präventive Maßnahmen zur Verhinderung von Datenschutzvorfällen

3.1 Einführung eines Datenschutz-Managementsystems (1): Inhalte

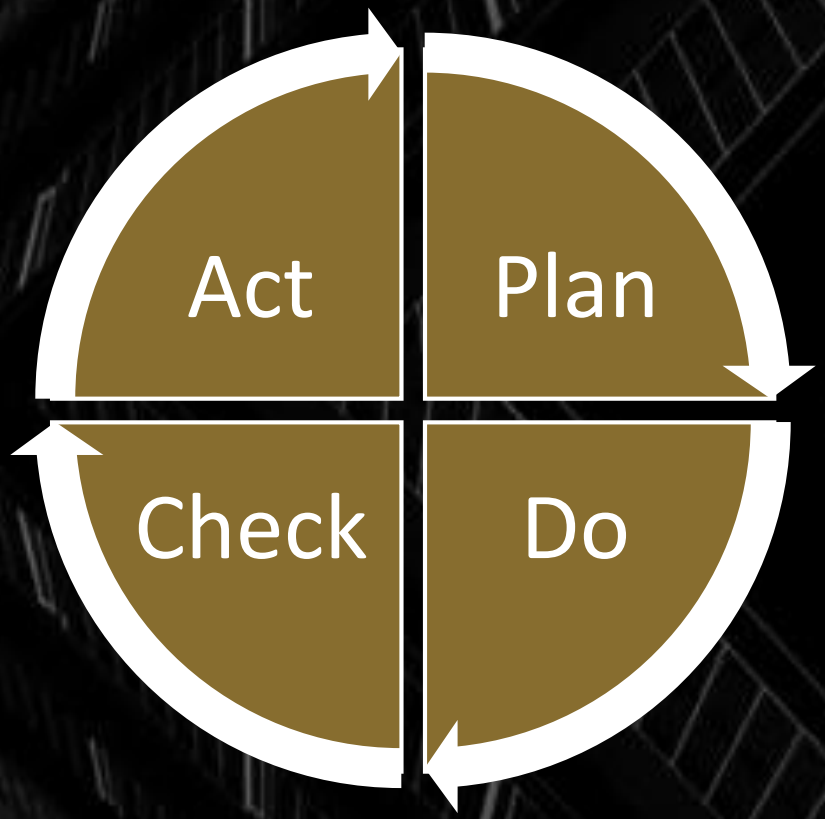
3.1 Einführung eines Datenschutz-Managementsystems (2): Umsetzung

1. Plan:
- Bestandsaufnahme der vorhandenen Prozesse
- Ziele formulieren, Umsetzungsplan erstellen

2. Do:
- Implementierung der Maßnahmen, Sensibilisierung
- Festlegung der Verantwortlichkeiten

3. Check:
- Überprüfung der Wirksamkeit der Maßnahmen
- Laufende Überwachung der umgesetzten Prozesse

4. Act:
- Optimierung und Beseitigung von Mängeln
- Änderung von Zielen, Maßnahmen oder Richtlinien



3.2 Sensibilisierung der Dienstleister

- Dem Verantwortlichen obliegt die **Pflicht zur Meldung eines Datenschutzvorfalls** (Art. 33 Abs. 1 DSGVO) – auch wenn dieser beim Auftragsverarbeiter passiert
- Daher sollten Auftragsverarbeiter auf ihre besondere Pflicht sensibilisiert werden, bei ihm auftretende Datenschutzvorfälle **umgehend an den Verantwortlichen zu melden** (Art. 33 Abs. 2 DSGVO)
- Praxistaugliche Meldewege sicherstellen (Ansprechpartner, Kanäle, Inhalte usw.)
- Dies sollte im **Auftragsverarbeitungsvertrag** festgehalten werden (z.B. Frist von 24 – 48 Stunden für Meldung)

3.3 Technische Maßnahmen umsetzen und aktuell halten

- Art. 32 DSGVO – “Stand der Technik“ erreichen, überprüfen und halten
- Werden die aktuellen **Empfehlungen des BSI zur IT-Sicherheit** eingehalten?
- Werden die neuesten Versionen für die **Inhalts-** (z.B. AES 256 bit) und **Transportverschlüsselung** (z.B. min. TLS 1.2) verwendet?
- Wird der **Zugriff** durch unberechtigte Personen **effektiv beschränkt**?
- Werden neue Funktionen erst nach erfolgreicher **Testphase** installiert?

3.4 Meldeprozess etablieren

1. Notieren der **Frist** nach **Kenntnis des Datenschutzvorfalls**
2. **Interne Meldung** und **Prüfung** des Sachverhalts – ggf. Schließen der **Sicherheitslücke**
3. **Einbeziehung** des/der **Datenschutzbeauftragten + Krisen-Team**
4. **Entscheidung** über Meldung (ggf. vorsorgliche Meldung) – ausgehend vom Risiko
5. **Dokumentation** und ggf. **Meldung** an Aufsichtsbehörde und/oder Betroffene

Zentrale Fragen:

- Was, wann und wo ist es **passiert**?
- Welches **Ausmaß** hat der Vorfall?
- Welche **Personengruppen** sind betroffen?
- Welche Kategorien personenbezogener **Daten** sind betroffen?
- Sind **sensible** Daten betroffen?
- Wurde die **Sicherheitslücke** geschlossen?
- Welches **Risiko** bestand und besteht weiterhin für die betroffenen Personen?

3.5 Krisenmanagement

- Krisenstab aus IT, Fachbereich, Recht, DSB, ISB, Presseabteilung (ggf. externe Kommunikations-management)
- Sorgfältige Prüfung des Sachverhalts:
  - alles was kommuniziert wird muss sicher feststehen
  - Fragebogenbasierte Abfrage des Sachverhalts in den Fachbereichen und der IT
- Effizienter Krisenstab mit starkem Management im Vorfeld festlegen:
  - Strategie festlegen
  - Niemand rennt alleine los
  - Keine Salami-Taktik
- nur mit Krisenstab abgestimmte Kommunikation
- nicht gegenüber Betroffenen und Behörden und Presse unnötig selbst belasten (Schadensersatzansprüche und Bußgeldverfahren)

4. Fazit

Fazit

- Datenschutzvorfälle können **durch ein effektives Datenschutz-Managementsystem verhindert** werden
- Wenn es doch zu einem (meldepflichtigen) Vorfall kommt, **sollten alle Prozesse und Zuständigkeiten klar definiert sein**
- Denn die **Frist zur Meldung** ist kurz und sollte eingehalten werden
- Krisenstab im Vorfeld aufbauen und testen

Kontakt

SCHÜRMANN
ROSENTHAL
DREYER
RECHTSANWÄLTE

DIGITALES BUSINESS . TECHNOLOGIE . MEDIEN

Schürmann Rosenthal Dreyer Rechtsanwälte

Am Hamburger Bahnhof 4
10557 Berlin
Deutschland

Tel: +49 (0)30 213 002 80
Fax: +49 (0)30 213 002 849

info@srd-rechtsanwaelte.de
www.srd-rechtsanwaelte.de