DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

BvD-Herbstkonferenz

Security Breach Notification - Risiken der Meldepflicht

Stuttgart, 25.10.2018

RA Dr. Jens Eckhardt
Fachanwalt IT-Recht
Datenschutz-Auditor (TÜV) und Compliance-Officer (TÜV)

Security Breach Notification - Risiken der Meldepflicht
Agenda

- **Pflicht zur Meldung nach Artt. 33, 34 DS-GVO**
- Wer ist zur Meldung und Benachrichtigung verpflichtet?
- Auf den zweiten Blick: Mögliche Konsequenzen der (Nicht-)Meldung
- Überlegung für die Organisation und die Handhabung im Unternehmen
- Fragen und Diskussion

Pflicht zur Meldung nach Artt. 33, 34 DS-GVO

- **Melde-/Benachrichtigungspflicht**
  - Art. 4 Nr. 12, Artt. 33, 34, ErwGr 59, 67 ff. DS-GVO
  - *Handhabung: Art. 29 Gruppe, WP250rev.01: "Guidelines on …"*

- **Zweistufigkeit Meldepflicht**
  - **Auslöser:** Verletzung des Schutzes personenbezogener Daten
  - **1. Stufe: Meldung an Aufsichtsbehörde (Art. 33 DS-GVO)**
    - **Ausschluss, falls** „voraussichtlich **nicht zu einem Risiko** für die persönlichen Rechte und Freiheiten führt"
      - ***Art. 29 Gruppe, WP250rev.01: Risikoklassifizierungen in Anhang B***

    ➔ **Grundsatz:** Meldepflicht, aber Ausnahmen
  - **2. Stufe: Benachrichtigung der betroffenen Personen (Art. 34 DS-GVO)**
    - **sofern**: falls Wahrscheinlichkeit für **hohes Risiko**
    - aber dennoch: Ausnahmen möglich

    ➔ **nicht allein:** Verletzung des Schutzes pers.bez. Daten
    - Aufsichtsbehörden: Verlangen der Unterrichtung

Pflicht zur Meldung nach Artt. 33, 34 DS-GVO

- **„Verletzung des Schutzes personenbezogener Daten“ (Art. 4 Nr. 12 DS-GVO)**

  *„eine Verletzung der Sicherheit, die zur **Vernichtung, zum Verlust oder zur Veränderung**, ob zufällig oder unrechtmäßig, oder zur **unbefugten Weitergabe von beziehungsweise zum unbefugten Zugang** zu personenbezogenen Daten führt, die **übermittelt, gespeichert oder auf sonstige Weise verarbeitet** wurden “*

  - keine Beschränkung auf bestimmte personenbezogene Daten
  - nicht erforderlich: Verschulden
  - erforderlich: Kenntnis („*ihm die Verletzung bekannt wurde*“)

- **Risiko für die Rechte und Freiheiten natürlicher Personen**
  - Risiko (Art. 33 DS-GVO) oder hohes Risiko (Art. 34 DS-GVO)
  - keine Definition in der DS-GVO
  - ErwGr. 76 S. 2 DS-GVO: „*… Risiko sollte anhand einer objektiven Bewertung …* “
  - (keine) Deckungsgleicheit mit Risikoklassifizierung der DSFA?
  - Art. 29 Gruppe, WP250rev.01: Risikoklassifizierungen in Anhang B

Pflicht zur Meldung nach Artt. 33, 34 DS-GVO

- **Meldung an Aufsichtsbehörde (Art. 33 DS-GVO)**
  - ohne unangemessene Verzögerung und möglichst binnen höchstens 72 Stunden ab Kenntnis
    - falls später, dann Begründungserfordernis
  - an gemäß Artikel 51 DS-GVO zuständige Aufsichtsbehörde
  - Ausnahme: *„voraussichtlich nicht zu einem Risiko für die persönlichen Rechte und Freiheiten führt“*
  - Vorgaben zu Inhalt der Benachrichtigung und Dokumentation (Art. 33 Abs. 3)
    - **Art der Verletzung des Schutzes personenbezogener Daten plus (soweit möglich) Kategorien und der ungefähren Zahl der betroffenen Personen, betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze**
    - den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen
    - **Beschreibung der wahrscheinlichen Folgen** der Verletzung des Schutzes personenbez. Daten
    - Beschreibung der von dem Verantwortlichen **ergriffenen oder vorgeschlagenen Maßnahmen** zur Behebung der Verletzung des Schutzes personenbezogener Daten und gegebenenfalls Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.
  - **teilweise: Online-Meldeformulare bzw. Formulare der Aufsichtsbehörden**
    - Risiken der Verwendung?

Pflicht zur Meldung nach Artt. 33, 34 DS-GVO

- **Benachrichtigung der betroffenen Personen (Art. 34 DS-GVO)**
  - **Voraussetzung der Benachrichtigungspflicht**

    *„Hat die Verletzung des Schutzes personenbezogener Daten **voraussichtlich** ein **hohes Risiko** für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge, … “*
  - **Inhalt der Benachrichtigung**

    „… beschreibt in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten und enthält mindestens die in Artikel 33 Absatz 3 Buchstaben b, c und d genannten Informationen und Empfehlungen.“
  - **Ausnahmen von der Pflicht zur Benachrichtigung (Art. 34 Abs. 3 DS-GVO)**
    - geeignete technisch-organisatorische Maßnahmen
    - Ausschluss des hohen Risikos durch „Folgemaßnahmen“
    - Unverhältnismäßigkeit des Aufwands für individuelle Benachrichtigung: *„öffentliche Bekanntmachung oder eine ähnliche Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden“*

Security Breach Notification - Risiken der Meldepflicht
Agenda

- Pflicht zur Meldung nach Artt. 33, 34 DS-GVO
- **Wer ist zur Meldung und Benachrichtigung verpflichtet?**
- Auf den zweiten Blick: Mögliche Konsequenzen der (Nicht-)Meldung
- Überlegung für die Organisation und die Handhabung im Unternehmen
- Fragen und Diskussion

Wer ist zur Meldung und Benachrichtigung verpflichtet?

- **Rolle des Verantwortlichen**
  - Art. 33 Abs. 1 DS-GVO: *„… meldet der Verantwortliche …, nachdem ihm die Verletzung bekannt wurde …“*
  - Art. 34 Abs. 1 DS-GVO: *„… benachrichtigt der Verantwortliche …“*
- **Rolle des Auftragsverarbeiters**
  - Art. 33 Abs. 2 DS-GVO: *„Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.“*
- **Joint Controllership (Art. 26 DS-GVO)**
  - *„Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke der und die Mittel zur Verarbeitung fest, so sind sie gemeinsam Verantwortliche. Sie legen in einer Vereinbarung in transparenter Form fest, wer von ihnen welche Verpflichtung gemäß dieser Verordnung erfüllt …“*
- **Rolle des Datenschutzbeauftragten (vgl. Art. 33 Abs. 3 lit. b, Art. 34 Abs. 2 DS-GVO)**
  - *„… den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen“*

Security Breach Notification - Risiken der Meldepflicht
Agenda

- Pflicht zur Meldung nach Artt. 33, 34 DS-GVO
- Wer ist zur Meldung und Benachrichtigung verpflichtet?
- **Auf den zweiten Blick: Mögliche Konsequenzen der (Nicht-)Meldung**
- Überlegung für die Organisation und die Handhabung im Unternehmen
- Fragen und Diskussion

Auf den zweiten Blick: Mögliche Konsequenzen der (Nicht-)Meldung

- **Mögliche Konsequenzen der Nicht-Meldung**
  - **Geldbuße nach Art. 83 Abs. 4 lit. a DS-GVO**
    - sowohl Art. 33 als auch Art. 34 DS-GVO
    - *„… von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist …“*
    - gegen Verantwortlichen und Auftragsverarbeiter
    - Verschulden als Voraussetzungen einer Sanktion (scheinbar str.)
  - **Zivilrechtliche Ansprüche bei Unterlassen der Benachrichtigung nach Art. 34**
    - Schadensersatzanspruch nach Art. 82 DS-GVO, Vertrag, etc.
    - Schaden infolge Unterlassen der Benachrichtigung

Auf den zweiten Blick: Mögliche Konsequenzen der (Nicht-)Meldung

- **Mögliche Konsequenzen der Meldung**
  - **Neue Problemfelder / Risikolagen**
    - Mitteilung der Verletzung des Schutzes personenbezogener Daten
      - bspw. bisher keine Sanktion bei Verstoß gegen § 9 BDSG

      ➔ Mitteilung eines bußgeldbewehrten Vorfalls
    - Organisationspflichten der DS-GVO
      - bspw. bisher keine Organisationspflicht wie Art. 24 DS-GVO)

      ➔ Grundlage für Organisationsverschulden
  - **Geldbuße nach Art. 83 Abs. 4 lit. a DS-GVO**
    - je nach Ursache des Vorfalls
    - insbesondere Art. 32 DS-GVO i.V.m. **Art. 83 Abs. 4 lit. a DS-GVO**
      - *„… von bis zu 10 000 000 EUR oder im Fall eines Unternehmens von bis zu 2 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist …“*
      - gegen Verantwortlichen und Auftragsverarbeiter
    - Verschulden als Voraussetzungen einer Sanktion (scheinbar str.)

Auf den zweiten Blick: Mögliche Konsequenzen der (Nicht-)Meldung

- ***[Mögliche Konsequenzen der Meldung – Fortsetzung]***
  - **Zivilrechtliche Ansprüche bei Meldung und Benachrichtigung**
    - Schaden durch Ursache der Meldung und Benachrichtigung
      - materieller und immaterieller Schaden
    - Schadensersatzanspruch nach Art. 82 DS-GVO, Vertrag, etc.
    - Artt. 79, 82 DS-GVO: auch gegen Auftragsverarbeiter
    - Art. 82 DS-GVO: Gesamtschuldnerische Haftung von Artt. 26, 28 DS-GVO

➔***Besonderheit: Meldung = Grundlage für Sanktion und Schadensersatzansprüche***

Auf den zweiten Blick: Mögliche Konsequenzen der (Nicht-)Meldung

- ***[Mögliche Konsequenzen der Meldung – Fortsetzung]***
  - **str.: reduzierende Wirkung in Bezug auf Bußgeld in Bezug auf Ursache (Art. 83 Abs. 2)**
    - *„c) jegliche von dem Verantwortlichen oder dem Auftragsverarbeiter getroffenen Maßnahmen zur Minderung des den betroffenen Personen entstandenen Schadens;“*
    - *„h) Art und Weise, wie der Verstoß der Aufsichtsbehörde bekannt wurde, insbesondere ob und gegebenenfalls in welchem Umfang der Verantwortliche oder der Auftragsverarbeiter den Verstoß mitgeteilt hat;“*
  - **Konfliktlage**
    - Bußgeldbewehrung der Nicht-Meldung
    - Verstoß gegen Grundgesetz: nemo tenetur – Grundsatz
    - Verstoß gegen Art. 8 EMRK
    - §§ 42 Abs. 4, 43 Abs. 4 BDSG
      - „**Beweisverwendungsverbötchen“** bei Selbstanzeige
      - **Problem:** Schutz des Unternehmens, nicht der Organe und Handelnden
      - Zivilrechtliche Haftungsbegrenzung????

Security Breach Notification - Risiken der Meldepflicht
Agenda

- Pflicht zur Meldung nach Artt. 33, 34 DS-GVO
- Wer ist zur Meldung und Benachrichtigung verpflichtet?
- Auf den zweiten Blick: Mögliche Konsequenzen der Meldung
- **Überlegung für die Organisation und die Handhabung im Unternehmen**
- Fragen und Diskussion

Überlegung für die Organisation und die Handhabung im Unternehmen

- **Meldung oder Nicht-Meldung**
  - Unternehmerische Risikoentscheidung?
  - Vermeidung durch Wunsch nach Verneinung von Artt. 33, 34 DS-GVO
- **Organisatorische Vorbereitung im Unternehmen**
  - Sicherstellung der unternehmensinternen Meldung
  - Bewertungsschema vorbereiten?
  - Wer entscheidet?
    - Unterscheidung zwischen Vorbereitung und finaler Unterscheidung?
- **Auftragsverarbeitung**
  - Erfüllung der Pflicht nach Art. 33 Abs. 2 DS-GVO: Wie?
  - Vertragliche Ausgestaltung des Art. 33 Abs. 2 DS-GVO
  - Haftungsbegrenzung und Freistellung
- **Meldung an die Aufsichtsbehörde und Benachrichtigung der betroffenen Person(en)**
  - „hard ball“: Beginn der Verteidigung gegen Bußgeld und Schadensersatz
    - Sonderfall: Auftragsverarbeitung
  - Wird es wirklich so hart gespielt?
  - Wer erstellt die Information?

Fragen und Diskussion!

Rechtsanwalt Dr. Jens Eckhardt
Fachanwalt für IT-Recht
Datenschutz-Auditor (TÜV)
Compliance-Officer (TÜV)

Berliner Allee 55
40212 Düsseldorf
Tel.: +49 211 – 17 52 06 60
Fax: +49 211 – 17 52 06 66
eckhardt@derra-d.de
www.derra.eu

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB

Rechtsanwalt Dr. Jens Eckhardt

Fachanwalt für Informationstechnologierecht und Datenschutz-Auditor (TÜV) sowie Compliance-Officer (TÜV)

Derra, Meyer & Partner – www.derra.eu – eckhardt@derra-d.de

Seit 2001 berät er bundesweit nationale und internationale Unternehmen zu den Themen Datenschutz, Informationstechnologie, Telekommunikation und Marketing. Die Beratung umfasst die gerichtliche Vertretung, Vertretung gegenüber Aufsichtsbehörden, insbesondere im Datenschutz, die strategische Beratung bei der Einführung neuer Systeme, die Bewertung von bestehenden Systemen, das Outsourcing sowie die Vertragsgestaltung.

Funktionen als

- Mitglied im Vorstand des Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V (Ressort Recht)
- Mitglied im Vorstand von EuroCloud Deutschland_eco e.V. (Ressort Recht)
- Dozent zum Datenschutzrecht der udis Ulmer Akademie für Datenschutz und IT-Sicherheit – gemeinnützige Gesellschaft mbH
- Dozent der DeutscheAnwaltAkademie Gesellschaft für Aus- und Fortbildung sowie Serviceleistungen mbH (Fortbildung im Bereich Fachanwalt IT-Recht)
- Mitglied im Beirat der ZD Zeitschrift für Datenschutz, Verlag C.H. Beck München
- Lehrbeauftragter der SRH Fernhochschule Riedlingen zum Internet- und Medienrecht und Datenschutz im Studiengang Medien und Kommunikation
- Anhörung durch die Datenschutzaufsichtsbehörden als Fachexperte für Werbung und Adresshandel
- Head of Legal Advisory Board , EuroCloud Star Audit
- Moderator und Referent verschiedener Datenschutzveranstaltungen und Autor von Fachbeiträgen zum Datenschutz-, IT-, Zivil- und Wettbewerbsrecht und zur Datenschutz-Grundverordnung

Auswahl der Veröffentlichungen:

- **Herausgeber eines inhaltlichen aufbereiteten Gesetzestextes zur DS-GVO, TKMmed!a**
- **Rüpke/v. Lewinski/Eckhardt, Datenschutzrecht, 2018, Verlag C.H. Beck**
- Eckhardt/Kramer/Tausch, DS-GVO-Kompendium, TKMmed!a
- Datenschutz und Marketing – Praxisleitfaden für Datenschutzbeauftragte und Geschäftsleitung, TKMmed!a,
- **Bergmann/Möhrle/Herb, BDSG/DS-GVO , Mit-Autor, Boorberg Verlag**
- **Beck'scher Online-Kommentar, Wolff/Brink, BDSG/DS-GVO , Mit-Autor, Verlag C.H. Beck München**
- **Recht der elektronischen Medien, Kommentar, Mitautor seit 1. Aufl., Verlag C. H. Beck München**
- **Handbuch IT- und Datenschutzrecht, Mitautor seit 1. Aufl., Verlag C. H. Beck München**
- **Beck'scher TKG Kommentar, Mitautor seit 4. Aufl. 2013, Verlag C. H. Beck München**
- Bspw. „Wann ist ein Datum ein personenbezogenes Datum?", gemeinsam mit Dr. Brink (Landesbeauftragter für den Datenschutz Baden-Württemberg, ZD Editorial 1/2015 und ZD 2015, 205 ff.
- Leitfaden – Datenschutz und Cloud Computing, Mitautor und Leiter der Taskforce „Datenschutz" der AG „Rechtsrahmen im Cloud Computing", Trusted Cloud-Initiative des BMWi
- Big Data im Marketing – Chancen und Möglichkeiten für eine effektive Kundenansprache, 2015, Mitautor, Haufe Gruppe
- Digitalisierung und Transformation im Unternehmen, Mitautor, KS-Energy-Verlag

DERRA, MEYER & PARTNER
Rechtsanwälte PartGmbB