Deutsche Stiftung für Recht und Informatik

Aktuelle Entwicklungen bei der datenschutzrechtlichen Bewertung von Sicherheitsvorfällen

RA Stefan Hessel, LL.M / Dipl.-Jur. Karin Potel

reuschlaw Legal Consultants

Herbstakademie 2021

AGENDA

- Die Meldepflicht nach Art. 33 DSGVO
- Aktuelle Entwicklungen
- Auftragsverarbeitung
- Ausblick und Stand der Debatte in Deutschland

Meldepflicht nach Art. 33 Abs. 1 DSGVO

- Ein Verantwortlicher muss Datenschutzverletzungen unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, melden.
- Die Verpflichtung entfällt, wenn die Datenschutzverletzung voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.
- Resultiert aus der Datenschutzverletzung ein hohes Risiko muss der Verantwortliche nach Art. 34 Abs. 1 DSGVO auch die betroffene Person benachrichtigen.

Meldepflicht bei IT-Sicherheitsvorfällen

- Nicht jeder IT-Sicherheitsvorfall, d.h. zum Beispiel ein Hacking-Angriff, stellt eine Datenschutzverletzung dar.
- Ein IT-Sicherheitsvorfall berührt nur den Anwendungsbereich des Art. 33 DSGVO, wenn eine Verletzung des Schutzes personenbezogener Daten eingetreten ist, d.h. eine Vernichtung, ein Verlust, eine Veränderung, oder eine unbefugte Offenlegung beziehungsweise ein unbefugter Zugang zu personenbezogenen Daten vorliegt.
- Sinn und Zweck der Meldepflicht ist die Minimierung der negativen Auswirkungen von Datenschutzverletzungen.

Aktuelle Entwicklung – Neue Leitlinien des EDSA

- Zu Beginn des Jahres hat der EDSA die “Guidelines 01/2021 on Examples regarding Data Breach Notification” angenommen und eine öffentliche Konsultation gestartet.
- Ist die vorrübergehende Einschränkung der Verfügbarkeit (z.B. bei Ransomware oder DDoS) eine meldepflichtige Datenschutzverletzung?
  - Der EDSA argumentiert mit dem Wortlaut der englischen Fassung von Art. 4 Nr. 12 DSGVO: “[…] accidental or unauthorised loss of access to […] personal data […]”
  - Tatsächlich handelt es sich jedoch um getrennte Fälle: “‘personal data breach’ means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed;”

Aktuelle Entwicklungen – „Hafnium“-Sicherheitslücke

- Unter dem Begriff "Hafnium" werden mehrere Sicherheitslücken in Microsoft-Exchange-Servern zusammenfasst.
- Das BSI warnte nach Veröffentlichung der Updates, dass nicht-gepatchte Exchange Server über das Internet angreifbar oder bereits mit Schadsoftware infiziert worden sind und Angreifer in der Folge Zugriff auf Daten haben, Programme steuern und Malware – insbesondere Ransomware – installieren können.
- Ansichten der Datenschutzaufsichtsbehörden (Auswahl):
  - Niedersachen/Bayern: Sicherheitslücke stellt nicht nur eine Kompromittierung dar, auch das verspätete Einspielen eines Sicherheitsupdates kann eine Meldepflicht auslösen.
  - NRW: Lediglich eine Dokumentation nach Art. 33 Abs. 5 DSGVO ist erforderlich.

Aktuelle Entwicklungen – „Scraping“

- Es handelt sich um einen Überbegriff für das automatisierte Auslesen von Texten aus Computerbildschirmen sowie Webseiten.
- Unterliegt der Betreiber eines sozialen Netzwerks als Verantwortlicher einer Meldepflicht, wenn Scraping stattgefunden hat?
- Aus der Sicht eines Netzwerkanbieters liegt i.d.R. keine unbefugte Offen-legung i.S.v. Art. 4 Nr. 12 DSGVO vor.
- Die Voraussetzungen einer Datenschutzverletzung und daher auch der Meldepflicht sind damit i.d.R. nicht erfüllt.
- Die rechtswidrige Handlung des Angreifers hat auf den Verantwortlichen keine Auswirkung.

Auswirkungen auf die Auftragsverarbeitung

- Auftragsverarbeiter sind nach Art. 28 Abs. 3 lit. f DSGVO verpflichtet, den Verantwortlichen bei der Einhaltung der Art. 32 bis 36 DSGVO zu unterstützen.
- Patcht der Auftragsverarbeiter die Server unzureichend, kann dies Pflichten nach Art. 33 und Art. 34 DSGVO auslösen.
- Dies kann die Annahme begründen, dass der Auftragsverarbeiter nicht in der Lage ist, die nach Art. 28 Abs. 1 DSGVO erforderlichen geeigneten technischen und organisatorischen Maßnahmen zu garantieren.
- Konsequenz: Der Verantwortliche kann bzw. darf nicht mehr auf die Kompetenz des Auftragsverarbeiters vertrauen. Bei gravierenden Verstößen kann eine Beendigung des Auftragsverarbeitungsverhältnisses in Betracht kommen.

Ausblick und Stand der Debatte in Deutschland

- Die aufgezeigten Beispiele machen deutlich, dass IT-Sicherheitsvorfälle mit erheblichen Datenschutzverletzungen verbunden sein können.
- Sie sind damit ein deutliches Risiko für den Schutz personenbezogener Daten.
- Frühzeitige Meldungen und daran anschließende Maßnahmen der Aufsichtsbehörden können zu einer Stärkung des allgemeinen IT-Sicherheitsniveaus beitragen.

Kontakt

Stefan Hessel, LL.M.
Rechtsanwalt I Attorney-at-Law (Germany)
Master of Laws „Informationstechnologie und Recht“

reuschlaw Legal Consultants
Reusch Rechtsanwaltsgesellschaft mbH
Büro Saarbrücken
Stengelstr. 1
66117 Saarbrücken

T > + 49 681 / 859 160 0
F > + 49 681 / 859 160 11
E > stefan.hessel@reuschlaw.de
www.reuschlaw.de