Datenschutzverletzung und Meldung im Kontext des »Hafnium Hacks«

Leitfaden

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Rebekka Weiß, LL.M. | Bitkom e. V.
T 030 27576-161 | r.weiss@bitkom.org

Verantwortliches Bitkom-Gremium

AK Datenschutz

Titelbild

© Samuel Zeller – unsplash.com

Inhaltsverzeichnis

Einleitung

Verantwortliche und Auftragsverarbeiter benötigen Rechtssicherheit, auch bei der Erfüllung datenschutzrechtlicher Meldepflichten. Obwohl es seit 2017 von der Artikel-29-Datenschutzgruppe eine Leitlinie zum Umgang mit den Meldepflichten gibt, hat der Hafnium-Hack aufgezeigt, dass es zwischen den deutschen Landesdatenschutzbehörden eine große Differenz in der Auslegung der gesetzlichen Datenschutzregelungen gibt. Bei den vorliegenden Stellungnahmen der Datenschutz-Aufsichtsbehörden geht es nicht »nur« um geringfügige Abweichungen der Auslegungen der jeweiligen Datenschutz-Aufsichtsbehörden (z.B. welche Informationen von der jeweiligen Datenschutzaufsichtsbehörde für eine Meldung einer Datenschutzverletzung als »must-have« gefordert werden), sondern in diesem Fall sind die Differenzen der datenschutzrechtlichen Bewertung zur Meldepflicht bedeutend.

Diese uneinheitliche Auslegung der Anforderungen des Datenschutzrechts führte dazu, dass ein bundesweiter Unternehmensverbund für die Anwendung einer europäischen Richtlinie bundeslandspezifische Regelungen treffen muss und viele Kleinstunternehmen und KMU von der teilweise sehr überraschenden Auslegung der gesetzlichen Regeln völlig verunsichert wurden. Aus unternehmerischer Sicht müssen europäische Richtlinien in ihrem Anwendungsbereich einheitlich ausgelegt werden, auch und gerade vor dem europäischen Harmonisierungsgedanken.

Aus diesem Grund hat sich eine Unterarbeitsgruppe des AK Datenschutzes der Bitkom mit der Auslegung der Art. 33 und 34 DSGVO auseinandergesetzt, um Unternehmen bei Meldungen von Datenschutzverletzungen fachlich zu unterstützen. Insbesondere haben wir die herrschende Meinung über den Begriff des »Bekanntwerdens« einer Verletzung des Schutzes personenbezogener Daten untersucht, mit dem Ziel der Harmonisierung der Auslegung durch Unternehmen und den Behörden.

Der AK Datenschutz ist der größte freiwillige Zusammenschluss von regelmäßig tagenden Datenschutzexperten in Europa. Vom KMU bis zum international agierenden DAX-Konzern sind aus allen Bundesländern Experten vertreten.

Besonderer Dank gilt folgenden Mitgliedern des Arbeitskreises Datenschutz, die mit ihrer Expertise und wertvollen praktischen Erfahrung ganz maßgeblich zur Entstehung des Leitfadens beigetragen haben:

- Ulrike Glöde | DonLuigi IT-Service
- Ulrike Hauser | scope & focus Service-Gesellschaft mbH
- Stefan Hessel | reuschlaw Legal Consultants
- Hanno Hinrichs | scope & focus Service-Gesellschaft mbH
- Linus Klingberg | Deutsche Bahn AG
- Torsten Mühlhaus | P&I AG
- Stephan Rehfeld | scope & focus Service-Gesellschaft mbH
- Karin Tresp | Rewe-Group

Unterscheidung zwischen Verantwortlichem und Auftragsverarbeiter

Gibt es einen Verdacht auf die Verletzung des Schutzes personenbezogener Daten, dann richten sich die weiteren Schritte maßgeblich nach der Qualifikation, ob die öffentliche oder nichtöffentliche Stelle ein Verantwortlicher oder Auftragsverarbeiter im Sinne der DSGVO ist.

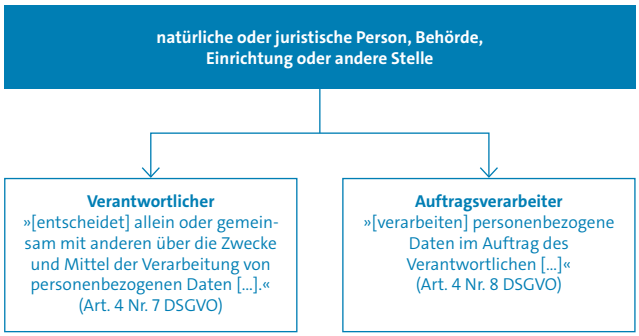

Abbildung 1: Unterscheidung zwischen Verantwortlichem und Auftragsverarbeiter

Die erforderlichen Schritte für einen Verantwortlichen werden in den folgenden zwei Kapiteln beschrieben. Die erforderlichen Schritte für einen Auftragsverarbeiter werden im vierten Kapitel dargestellt.

Generell muss der Verarbeiter personenbezogener Daten »alle geeigneten technischen Schutz- sowie organisatorischen Maßnahmen [treffen], um sofort feststellen zu können, ob eine Verletzung des Schutzes personenbezogener Daten aufgetreten ist, und um die Aufsichtsbehörde und die betroffene Person umgehend unterrichten zu können.« (Erwägungsgrund 87 DSGVO).

Weiterhin müssen zwei Geschäftsprozesse unterschieden werden,

- die Behandlung eines Informationssicherheitsvorfalls und
- die Behandlung einer Datenschutzverletzung.

Die Behandlung eines Informationssicherheitsvorfalls geschieht in Organisationen zunächst unabhängig von Datenschutzfragen. Der Schwerpunkt bei der Behandlung von Vorfällen im Bereich der Informationssicherheit liegt auf dem unverzüglichen Abstellen des Schadensereignisses und dem Einleiten von Korrekturmaßnahmen, damit ein derartiges Ereignis nicht erneut auftreten kann. Sollten von dem Informationssicherheitsvorfall auch personenbezogene Daten betroffen sein, so hat der europäische Gesetzgeber für den Umgang mit den Datenschutzaspekten der Datenschutzverletzung zusätzliche Regeln aufgestellt. Beide Geschäftsprozesse werden häufig von zwei unterschiedlichen Teams bearbeitet, die aber natürlich eng zusammenarbeiten sollten.

1 Meldungen nach Art. 33 DSGVO

1 Meldungen nach Art. 33 DSGVO

Der Gesetzgeber definiert in Art. 4 Abs. 12 DSGVO die »Verletzung des Schutzes personenbezogener Daten« als »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«.

Eine Verletzung des Schutzes personenbezogener Daten kann für den Verantwortlichen zu einer Meldung an die zuständige Aufsichtsbehörde führen.

Gesetzestext

Art. 33 DSGVO – Meldung von Verletzungen des Schutzes personenbezogener Daten an die Aufsichtsbehörde

[1]Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet der Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, diese der gemäß Artikel 55 zuständigen Aufsichtsbehörde, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt. 2 Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

Wenn von dem Verantwortlichen eine (potentielle) Datenschutzverletzung entdeckt oder ihm gemeldet wird, muss der Verantwortliche ermitteln, ob eine meldepflichtige Datenschutzverletzung vorliegt.

Als Datenschutzverletzung wird die Verletzung

- der Vertraulichkeit,
- der Integrität und/oder
- der Verfügbarkeit

von personenbezogenen Daten bezeichnet.[1]

Der Gesetzgeber beschreibt für das Vorliegen der Meldepflicht einer Verletzung des Schutzes personenbezogener Daten drei Voraussetzungen,

1. die konkrete Verletzung des Schutzes personenbezogener Daten,

2. das dem Verantwortlichen die Verletzung des Schutzes personenbezogener Daten bekannt geworden ist und

3. die Verletzung muss zu einem Risiko oder hohen Risiko für die Freiheiten und Rechte einer natürlichen Person führen.

1 Ausführlicher: Artikel-29-Datenschutzgruppe, »Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679« vom 3.10.2017 in der Fassung vom 6.2.2018, WP250rev.01, Seite 8 ff.

Die Artikel-29-Datenschutzgruppe führte in ihrer Leitlinie zum Umgang mit Datenschutzverletzungen aus »dass einem Verantwortlichen eine Datenschutzverletzung ›bekannt‹ wurde, wenn der betreffende Verantwortliche eine hinreichende Gewissheit darüber hat, dass ein Sicherheitsvorfall aufgetreten ist, der zu einer Beeinträchtigung des Schutzes personenbezogener Daten geführt hat.«[2]

In dem zugehörigen Beispiel wird in der Leitlinie illustriert, wie der Begriff »Bekanntwerden« zu verstehen ist:

> *»3. Ein Verantwortlicher bemerkt, dass möglicherweise in sein Netzwerk eingedrungen wurde. Der Verantwortliche prüft seine Systeme auf eine eventuelle Beeinträchtigung der darin gespeicherten Daten und stellt fest, dass dies der Fall ist. Auch in diesem Fall hat der Verantwortliche nun den eindeutigen Nachweis einer Datenschutzverletzung, sodass ihm der Vorfall zweifelsfrei ›bekannt‹ wurde.«*

Aktuell befindet sich die **↗Guideline des EDSA zu »Data Breach Notification«** in Abstimmung. Hier lässt sich – wenig überraschend – ein ähnlicher Ansatz entnehmen. In dem Papier wird ein Angriff durch Ransomware bewertet. In einer Beispielsvariante (Case No. 01), gab es zwar einen Angriff, die Systeme des Verantwortlichen haben indes »gegriffen« und es fand kein Datenabfluss statt, bzw. etwaige zerstörte Daten wurden durch ein Backup wiederhergestellt. Hier führt der EDSA aus:

> *»On the severity of the consequences for the data subjects, only minor consequences could be identified since the affected data was restored in a few hours, the breach did not result in any consequences on the day-to-day operation of the controller and had no significant effect on the data subjects (e.g. employee payments or handling client requests)« (Rz. 22)*

Der EDSA kommt sodann konsequent zum Ergebnis, dass dieser Vorgang zwar zu dokumentieren, indes aber keine Meldung an die Behörde erfolgen muss (Rz. 25 / Tabelle).

Wenn also schon bei »auswirkungslosen« Angriffen durch eine Ransomware (also bereits schadhafter Code in die Systeme des Verantwortlichen eingedrungen ist und dieses teils personenbezogene Daten korrumpiert hat) zu keiner Meldepflicht führt, muss dies entsprechend gelten, wenn nicht einmal ein »Angriff« von außen stattfand und »nur« eine Sicherheitslücke in einer Software vorliegt, die nicht korrumpiert wurde und es somit ebenfalls zu keinem Verlust / Offenlegung, etc. von personenbezogenen Daten kam.

Diese Auffassung der Auslegung durch die Artikel-29-Datenschutzgruppe und des EDSA wird auch durch die Literatur bestätigt, hier eine Zusammenfassung der Ausführungen von Dix in Simitis u.a (Hrsg.), Datenschutzrecht:

2 Ebd., Seite 12.

Eine Meldepflicht besteht nur dann, wenn eine Verletzung des Schutzes personenbezogener Daten im Sinne des Art. 4 Nr. 12 DSGVO vorliegt. Der Verantwortliche muss hinreichende Kenntnis von der Verletzung haben, sodass er eine sinnvolle Unterrichtung der Aufsichtsbehörde vornehmen kann. Bei bloßem Verdacht einer Schutzverletzung muss der Verantwortliche nicht melden, sondern erst, wenn ihm Informationen über Art, Umstände, Zeitpunkt der Schutzverletzung, sowie Kategorien der betroffenen Daten vorliegen (vgl. auch Paal/Pauly (Art. 33 Rn 18).

Auch Gierschmann in Gierschmann u.a (Hrsg.), Kommentar DSGVO kommt zum selben Bewertungsergebnis wie die Artikel-29-Datenschutzgruppe und der EDSA:

Art. 33 Abs. 1 DSGVO setzt das Bekanntwerden der Verletzung voraus. Bei juristischen Personen meint dies die Kenntnisnahme durch die Geschäftsführung bzw. durch einen Wissensvertreter (Art. 33 Rn. 39).

Nur die Kenntnis einer Sicherheitslücke durch den Verantwortlichen reicht nicht aus, sondern es müssen Hinweise vorliegen, dass Risiken für die Rechte und Freiheiten von Betroffenen bestehen. Ein Angriff auf ein System, mit dem personenbezogene Daten verarbeitet werden, kann jedoch genügen (Art. 33 Rn. 42).

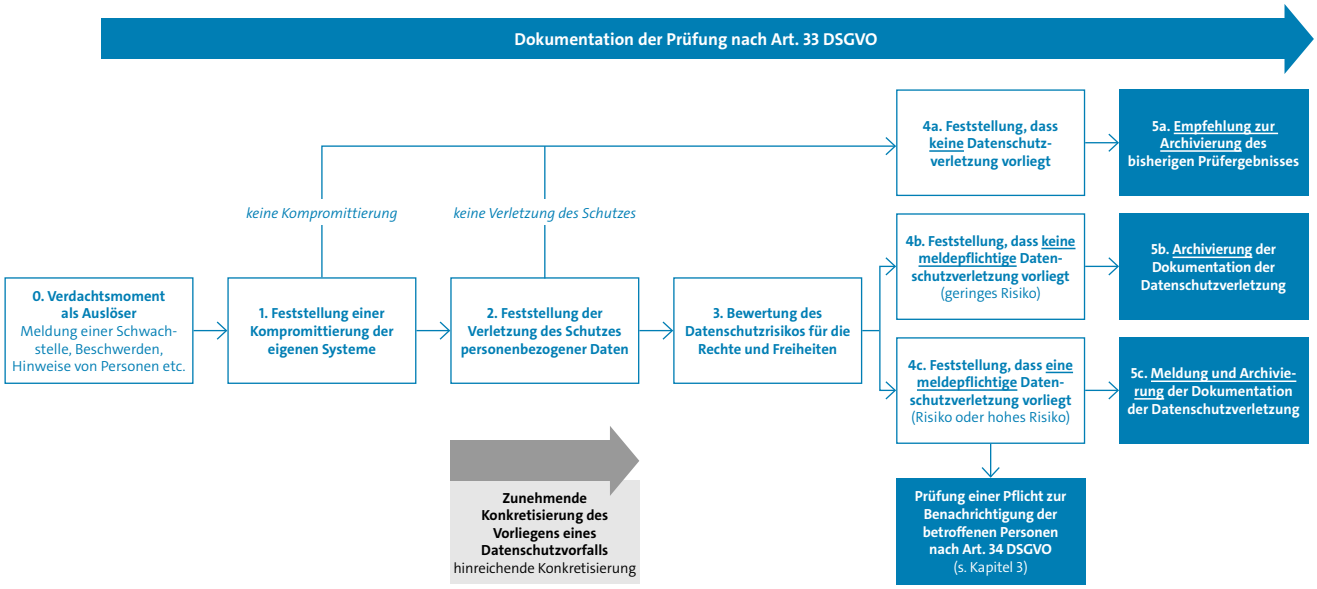

Abbildung 2: Prüfung der Pflicht zur Meldung einer Datenpanne an die zuständige Aufsichtsbehörde nach Art. 33 DSGVO

Am Beispiel des Hafnium-Hacks muss der Verantwortliche also

0. erfahren, dass von ihm betriebene Exchange-Server überhaupt eine Schwachstelle haben.

1. Dann die Überprüfung der etwaigen Kompromittierung seiner Systeme beauftragen (intern: IT-Abteilung, extern: Dienstleister). Da Exchange-Server in sehr unterschiedlichen Konfigurationen betrieben werden, kann nicht davon ausgegangen werden, dass nur wegen des Vorliegens einer Schwachstelle auch eine Kompromittierung stattgefunden hat.

2. Wenn der Verantwortliche das Feedback bekommt, dass eine Kompromittierung der eigenen Server vorliegt, muss er eine Untersuchung beauftragen, ob und in welchem Umfang eine Verletzung des Schutzes personenbezogener Daten vorliegt.

3. Wenn bei dem Verantwortlichen Kenntnis über eine Verletzung und den Umfang der Verletzung des Schutzes personenbezogener Daten vorliegt, dann muss der Verantwortliche eine Bewertung des Datenschutzrisikos für die Rechte und Freiheiten von natürlichen Personen vornehmen.[3]

4. Auf Basis der Bewertung des Datenschutzrisikos kann nun festgestellt werden, ob eine meldepflichtige Datenschutzverletzung vorliegt.

5. Abhängig von dem Ergebnis der Bewertung des Datenschutzrisikos wird die Dokumentation einer Verletzung des Schutzes personenbezogener Daten nur intern archiviert oder der zuständigen Aufsichtsbehörde gemeldet, eine Pflicht zur Benachrichtigung der betroffenen Person geprüft (siehe hierzu das folgende Kapitel) und die bisherige Prüfung archiviert.

Nur der Hinweis auf eine Schwachstelle kann nicht die Fiktion begründen, dass eine Datenschutzverletzung vorliegt. Da ein solches Vorgehen gesetzesfremd ist, würde dieses Vorgehen Folgefragen aufwerfen,

- Wer bestimmt, dass die Fiktion einer Datenschutzverletzung vorliegt?
- Wo und in welchem Intervall muss sich der Verantwortliche über die Fiktion einer Datenschutzverletzung informieren?
- Ab wann läuft die Meldepflicht bei der Fiktion einer Datenschutzverletzung?
- Wie wird bei der Fiktion einer Datenschutzverletzung mit der unverzüglichen Benachrichtigung der betroffenen Personen umgegangen?
- Welche Auswirkungen hat die Meldung einer angenommenen Datenschutzverletzung auf andere Rechtsgebiete (z.B. etwaige Verletzung eines Berufsgeheimnisses, § 203 StGB)?

Lässt sich aber nicht mit hinreichender Sicherheit feststellen, ob nach festgestellter Kompromittierung der Systeme auch eine konkrete Datenschutzverletzung vorliegt, so können nur wenige

3 Zum Datenschutzrisiko siehe auch ausführlich Bitkom, **↗Leitfaden »Risk Assessment & Datenschutz-Folgenabschätzung«**

Hinweise auf eine Verletzung des Schutzes personenbezogener Daten eine hinreichende Konkretisierung als Grundlage für eine spätere Meldung an die zuständige Aufsichtsbehörde sein. Ein solcher Hinweis kann z.B. in den Protokollen ein Hinweis auf eine umfangreichere Ausleitung von Informationen sein oder andere ungewöhnliche Aktivitäten. Aber nur die Feststellung einer Kompromittierung kann aus unserer Sicht noch keine Meldepflicht begründen. Eine weitere Konkretisierung ist erforderlich und aus unserer Sicht auch vom Gesetzgeber gefordert.

1.1 Wer muss melden?

Die Meldung einer Datenschutzverletzung hat durch den Verantwortlichen zu erfolgen. Dies ist bei nichtöffentlichen Stellen im Regelfall die Geschäftsleitung (z.B. bei GmbHs) oder der Vorstand (häufig bei Vereinen oder Verbänden), also ein Organ der Gesellschaft mit Vertretungsbefugnis. Natürlich darf der Datenschutzbeauftragte aber beim Ausfüllen eines Meldeformulars mitwirken sowie der Erstellung der ergänzenden Dokumentation.[4]

1.2 Wie muss gemeldet werden?

In den meisten Fällen bittet die zuständige Aufsichtsbehörde um eine elektronische Meldung. Entsprechende Meldeformulare werden dann durch die zuständige Aufsichtsbehörde bereitgestellt. Der Mindestumfang der Meldung einer Datenschutzverletzung wird in Art. 33 Abs. 3 DSGVO festgelegt.

Da eine Datenschutzverletzung innerhalb der 72-stündigen Meldefrist ab Bekanntwerden häufig nicht aufgeklärt werden kann, erlaubt der Gesetzgeber auch eine schrittweise Meldung einer Verletzung personenbezogener Daten (Art. 33 Abs. 4 DSGVO). Die Ergänzung der vorläufigen Meldung durch den Verantwortlichen hat dabei aber »ohne unangemessene weitere Verzögerung« zu erfolgen.

1.3 Exkurs: Begriff der »vorläufigen Meldung«

Einige Datenschutzbehörden ermöglichen es Verantwortlichen eine »vorläufige Meldung« eines Datenschutzvorfalls abzugeben. In seiner »Orientierungshilfe zur Meldepflicht und Benachrichtigungspflicht von Verantwortlichen« erklärt der LfD Bayern, welche Voraussetzungen für eine »vorläufige Meldung« vorliegen müssen und stellt fest:

Ein (potenzielles) Verletzungsverhalten ist belegt. Ob es zu einem ein Verletzungserfolg gekommen ist, bleibt aber unklar, weil es dem Verantwortlichen nicht gelingt, sich ein Bild von der Lage zu verschaffen. Reaktion: Der Verantwortliche legt seiner weiteren Beurteilung des Vorfalls zugrunde, dass eine Datenschutzverletzung eingetreten ist und erfüllt seine Pflichten nach

4 Quelle: ↗**https://www.datenschutz-bayern.de/datenschutzreform2018/OH_Meldepflichten.pdf**, Rz. 73

Art. 33 und 34 DSGVO, soweit die weiteren Voraussetzungen gegeben sind (vorläufige Meldung). Die Gleichbehandlung einer nur angenommenen Datenschutzverletzung mit einer nachweisbaren ist jedenfalls dann gerechtfertigt, wenn ein Verletzungserfolg mutmaßlich realisiert ist.

Der LfD Bayern hält das Konstrukt der »vorläufigen Meldung« für notwendig, damit »sich der Verantwortliche nicht durch den Vortrag entlasten kann, eine Datenschutzverletzung sei nicht feststellbar, weil das eigene System eine black box darstelle.«

Folgend soll erläutert werden, warum die Annahme einer »vorläufigen Meldung« sowohl aus juristischer als auch aus praktischer Sicht bedenklich ist.
Bei einer genauen Analyse der DSGVO ist festzustellen, dass das Gesetz den Begriff der «vorläufigen Meldung« einer Datenschutzverletzung nicht kennt.

In Art. 4 Nr. 12 DSGVO ist zunächst die »Verletzung des Schutzes personenbezogener Daten« legal definiert. Es handelt sich dabei um eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur unbefugten Offenlegung oder zum unbefugten Zugang zu personenbezogenen Daten führt.
Eine Verletzung der Sicherheit muss also kausal zur unbefugten Verwendung von personenbezogenen Daten geführt haben. Vermutungen allein reichen für die Annahme eines Datenschutzvorfalls im Sinne des Art.4 Nr. 12 DSGVO nicht aus.

Weiterhin müssen gemäß Art. 33 Abs. 3 DSGVO mindestens bestimmte Informationen vorliegen, damit eine Meldung eines Datenschutzvorfalls erfolgen kann.
Zu diesen Informationen gehören u.a. eine Beschreibung der Art der Verletzung, der wahrscheinlichen Folgen, und der Maßnahmen zur Behebung der Verletzung.
Auch hier lässt das Gesetz keinen Raum für Mutmaßungen, denn eine Schutzverletzung kann nur beschrieben werden, wenn sie auch tatsächlich erfolgt ist.

Art. 33 Abs. 4 DSGVO weist zwar auf die Möglichkeit hin, dass Informationen die nicht zur gleichen Zeit bereitgestellt werden können, schrittweise zur Verfügung gestellt werden können. Das setzt allerdings voraus, dass die Informationen auch tatsächlich zur Verfügung gestellt werden.
Eine schrittweise Meldung darf daher nicht mit einer »vorläufigen Meldung« verwechselt werden, die nur aufgrund der Mutmaßung eines Datenschutzvorfalls erfolgt.

2 Benachrichtigung nach Art. 34 DSGVO

2 Benachrichtigung nach Art. 34 DSGVO

Wenn eine meldepflichtige Verletzung des Schutzes personenbezogener Daten durch den Verantwortlichen festgestellt worden ist, dann muss vom Verantwortlichen in einem weiteren Prüfschritt festgestellt werden, ob eine Pflicht zur Benachrichtigung der betroffenen Personen besteht. Eine solche Benachrichtigung muss vom Verantwortlichen vorgenommen werden, wenn für die Rechte und Freiheiten natürlicher Personen voraussichtlich ein hohes Risiko besteht (Art. 34 Abs. 1 DSGVO) und nicht die Ausnahmen nach Art. 34 Abs. 3 DSGVO erfüllt sind:

a) »der Verantwortliche hat geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen und diese Vorkehrungen wurden auf die von der Verletzung betroffenen personenbezogenen Daten angewandt, insbesondere solche, durch die die personenbezogenen Daten für alle Personen, die nicht zum Zugang zu den personenbezogenen Daten befugt sind, unzugänglich gemacht werden, etwa durch Verschlüsselung,

b) der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 aller Wahrscheinlichkeit nach nicht mehr besteht«

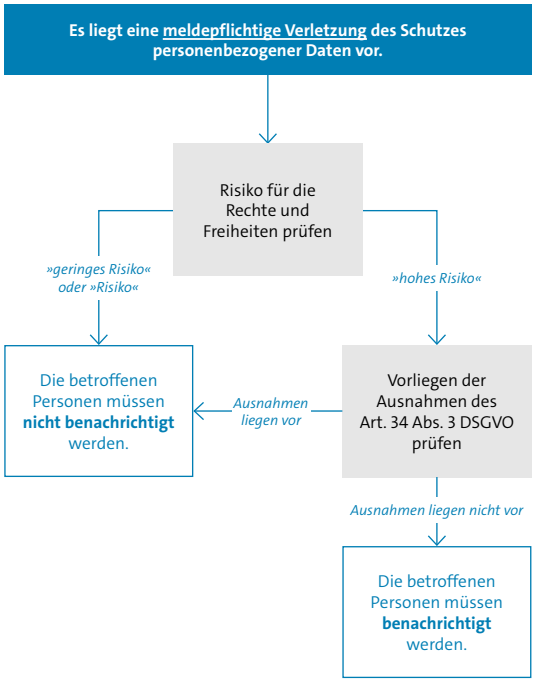

Abbildung 3: Prüfung der Pflicht zur Benachrichtigung der betroffenen Personen nach Art. 34 DSGVO

2.1 Identifizierung der Kategorien von Betroffenen

In der Praxis kann der Verantwortliche mithilfe des Verzeichnisses der Verarbeitungstätigkeiten ermitteln, in welchen Verarbeitungstätigkeiten Exchange-Server als Arbeitsmittel eingesetzt werden.

Beispiel: Rechnungswesen (Handwerk)

Verarbeitungstätigkeit: Versenden von Rechnungen

Kategorie von Betroffenen: Kunden

Kategorie von personenbezogenen Daten:
- Name und Anschrift
- Ausstellungsdatum
- Rechnungsnummer
- Menge und die Art (handelsübliche Bezeichnung) der gelieferten Gegenstände oder den Umfang und die Art der sonstigen Leistung

Eingesetzte Software: Exchange-Server, ...

Beispiel: Personalwesen

Verarbeitungstätigkeit: Bewerbungen für Behindertenwerkstätten

Kategorie von Betroffenen: Bewerber, abgelehnte Bewerber, eingestellte Bewerber

Kategorie von personenbezogenen Daten:
- Name und Anschrift
- schulische Bildung
- Ausbildung
- Weiterbildung
- beruflicher Werdegang
- Behinderungen
- Gehaltsvorstellungen
- Familienverhältnisse

Eingesetzte Software: Exchange-Server, ...

Beispiel: Vertrieb

Verarbeitungstätigkeit: Kommunikation mit Produktinteressenten

Kategorie von Betroffenen: Interessenten

Kategorie von personenbezogenen Daten:
- Name und Kommunikationsdaten
- Produktinteresse

Eingesetzte Software: Exchange-Server, ...

2.2 Beurteilung bezüglich eines Risikos oder eines hohen Risikos für die Betroffenen

Die Beurteilung des entstandenen Risikos für den Betroffenen kann nicht pauschal beantwortet werden. Die Risiken bei der Verletzung des Schutzes personenbezogener Daten resultieren aus

- der Verletzung der Vertraulichkeit,
- der Verletzung der Integrität und/oder
- der Verletzung der Verfügbarkeit.

Mögliche Schadenskategorien nach Erwägungsgrund 85 DSGVO können sein

- Diskriminierung,
- Identitätsdiebstahl,
- finanzieller Verlust,
- Rufschädigung,
- Verlust der Vertraulichkeit bei Berufsgeheimnis,
- unbefugten Aufhebung der Pseudonymisierung,
- andere wirtschaftliche oder gesellschaftliche Nachteile,
- Hinderung der Kontrolle der Betroffenen über eigene Daten und/oder
- Verarbeitung von sensiblen Daten (Politik, Religion, Sexualleben, Gesundheit, etc.).

Die Schwere oder Auswirkung kann sich für die betroffene Person in einem physischen, materiellen oder immateriellen Schaden manifestieren.[5]

Weiterhin haben auf die Schwere einer tatsächlichen Verletzung weitere Faktoren Auswirkung, z.B. wie einfach die betroffenen Personen durch einen Angreifer identifiziert werden können oder auch andere Umstände der Verletzung, ob z.B. der Angreifer böswillige Absichten hatte oder nur versehentlich handelte (so z.B. meist beim Versand von Irrläufern). Es muss bei der Klassifizierung in geringes Risiko, Risiko und hohem Risiko auf das Gesamtbild der Verhältnisse abgestellt werden. Für die oben genannten Beispiele könnte eine entsprechende Klassifizierung wie folgt vorgenommen werden:

5 Siehe für eine entsprechende Einstufungstabelle Bitkom, **↗Leitfaden »Risk Assessment & Datenschutz-Folgenabschätzung«**, Seite 50 ff.

Beispiel: Rechnungswesen (Handwerk)
Verarbeitungstätigkeit: Versenden von Rechnungen Durch eine Offenbarung der personenbezogenen Daten entsteht für die betroffenen Personen lediglich ein Risiko für ihre Rechte und Freiheiten.
Beispiel: Personalwesen
Verarbeitungstätigkeit: Bewerbungen für Behindertenwerkstätten Durch eine Offenbarung der personenbezogenen Daten entsteht für die betroffenen Personen ein hohes Risiko für ihre Rechte und Freiheiten.
Beispiel: Vertrieb
Verarbeitungstätigkeit: Kommunikation mit Produktinteressenten Durch eine Offenbarung der personenbezogenen Daten entsteht für die betroffenen Personen lediglich ein Risiko für ihre Rechte und Freiheiten.

Wichtig ist hier nochmal hervorzuheben, dass im Datenschutz das Risiko für die Rechte und Freiheiten der betroffenen Personen betrachtet wird und nicht das Risiko oder der Schaden für ein Unternehmen.

Beispiele für die Klassifizierung von Datenschutzverletzungen können den **↗»Guidelines 01/2021 on Examples regarding Data Breach Notification«** des EDSA entnommen werden, die aktuell allerdings nur in einem Entwurf vorliegen.

Wie sind die betroffenen Personen im Falle eines »hohen Risikos« zu informieren?

Wird das Risiko der Sicherheitslücke für die Rechte und Freiheiten natürlicher Personen als hoch eingestuft und greifen nicht die Ausnahmen des Art. 34 Abs. 3 DSGVO, ist die Folge, dass alle betroffenen Personen über die Datenschutzverletzung gemäß Art. 34 DSGVO unverzüglich informiert werden müssen.[6]

In den obigen Beispielen müssen also lediglich alle betroffenen Personen in der Verarbeitungstätigkeit »Bewerbungen für Behindertenwerkstätten« informiert werden, also alle Bewerber, abgelehnte Bewerber, eingestellte Bewerber, über die noch personenbezogene Daten aus dem Bewerbungsverfahren auf dem Exchange-Server gespeichert waren. Dies resultiert bei dem Beispiel aus der Prämisse, dass in Behindertenwerkstätten nur Personen mit körperlichen Behinderungen eingestellt werden und diese Daten besonders schützenswert sind.

6 Nähere Hinweise zur Informierung auch in Erwägungsgrund 88 DSGVO.

Eine besondere Form der Benachrichtigung schreibt die DSGVO nicht vor. Es kann sowohl per Brief, per E-Mail oder per Telefon informiert werden. Aus Sicht des Verantwortlichen empfiehlt sich dennoch die Textform, um eine lückenlose Dokumentation gewährleisten zu können. Grundsätzlich muss jeder Betroffene persönlich informiert werden. Dies gilt nur dann nicht, wenn die Betroffenen unbekannt sind oder der Aufwand für die Ermittlung unverhältnismäßig groß ist. In diesen Fällen ist auch eine öffentliche Bekanntmachung möglich z.B.,

- Website
- Fachliteratur
- Tagespresse

3 Auswirkungen auf Auftragsverarbeitung

3 Auswirkungen auf Auftragsverarbeitung

3.1 Datenschutzrechtliche Ausgangslage

Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, d.h. liegt ein Fall der sog. Auftragsverarbeitung vor, so muss der Auftragsverarbeiter gemäß Art. 28 Abs. 1 DSGVO hinreichende Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und der Schutz der Rechte der betroffenen Person gewährleistet wird. Darüber hinaus sind Auftragsverarbeiter nach Art. 28 Abs. 3 lit. f DSGVO verpflichtet den Verantwortlichen bei bestimmten Verpflichtungen zu unterstützen. Dies betrifft insbesondere die Pflicht zur Meldung nach Art. 33 DSGVO und die Pflicht zur Benachrichtigung nach Art. 34 DSGVO.

Der Auftragnehmer hat im Rahmen der Datenverarbeitung im Auftrag die Pflicht zur Meldung von Datenschutzverletzungen an den Auftraggeber. Er hat in diesem Fall nicht die Pflicht und auch nicht die Erlaubnis zur Meldung an die Aufsichtsbehörde. Im Auftragsverhältnis ist es nur die Aufgabe des Auftraggebers, die Anforderungen der Art. 33, 34 DSGVO einzuhalten.

3.2 Auswirkungen

Wird im Fall der aktuellen Schwachstellen ein Server durch einen Auftragsverarbeiter nicht oder nicht ordnungsgemäß mit Updates versorgt und auf eine Kompromittierung geprüft, kommt eine Vertragsverletzung des Auftragsverarbeiters sowie mögliche Regressansprüche in Betracht. Darüber hinaus trägt jedoch der Verantwortliche bei der Inanspruchnahme des Auftragsverarbeiters, das datenschutzrechtliche Risiko von Datenschutzverletzungen in der Sphäre des Auftragsverarbeiters. Er ist aus diesem Grund dazu verpflichtet den Auftragsverarbeiter mit Blick auf das Bestehen hinreichender Garantien sorgfältig auszuwählen und das Fortbestehen dieser regelmäßig zu überprüfen. Im Fall verspäteter Updates, einer unterlassenen Prüfung auf Kompromittierung oder anderen Gründen, die auf einen unsachgemäßen Umgang mit den Schwachstellen hindeuten, können diese Garantien jedoch erschüttert werden. Aus datenschutzrechtlicher Sicht stellt sich daher bei der unsachgemäßen Bewältigung IT-Sicherheitsvorfällen stets die Frage, ob der Auftragsverarbeiter zukünftig noch hinreichende Garantien für die nach Art. 28 Abs. 1 DSGVO erforderlichen geeigneten technischen und organisatorischen Maßnahmen vorweisen kann. Ist dies nicht mehr der Fall, hat der Verantwortliche das Auftragsverarbeitungsverhältnis in der Regel zu beenden. Verantwortliche und Auftragsverarbeiter sind daher gehalten mit Blick auf das beiderseitige Interesse an einer Fortsetzung der Datenverarbeitung tätig zu werden, wenn im Kontext von Hafnium Anhaltspunkte für einen Wegfall oder eine Einschränkung der erforderlichen Garantien bestehen.

Hierbei können sich die Parteien an dem folgenden abgestuften Prozess orientieren:

1. **Information durch den Auftragsverarbeiter:**

Auftragsverarbeiter, die einen Exchange-Server im Auftrag des Verantwortlichen betreiben, sollten diesen mit den notwendigen Informationen zur Dokumentation des Vorgangs sowie ggfs. auch zur Prüfung einer Meldung oder Benachrichtigung versorgen. Dies gilt auch, wenn der Betrieb eines Exchange-Servers nicht Vertragsgegenstand ist, die Datenverarbeitung beim Auftragsverarbeiter jedoch mit Hilfe eines Exchange-Servers durchgeführt wird und Daten des Auftraggebers betroffen sind. Die Informationen sollten möglichst genau Auskunft über die getroffenen Maßnahmen und eventuelle Schwächen bei der Umsetzung notwendiger Maßnahmen geben.

2. **Anfrage bei Kenntnis des Verantwortlichen vom Betrieb eines Exchange-Servers**

Erhalten Verantwortliche von Auftragnehmern keine Informationen nach Schritt 1, ist der Betrieb eines Exchange-Servers jedoch Gegenstand der Auftragsverarbeitung oder dem Verantwortlichen aus anderen Gründen bekannt, dass ein Exchange-Server im Rahmen der Auftragsverarbeitung eingesetzt wird, sollte er, um seinen Überwachungs- und Kontrollpflichten nach Art. 28 Abs. 1 DSGVO nachzukommen, die benötigten Informationen beim Auftragsverarbeiter anfragen.

3. **Information belegt ausreichende Gegenmaßnahmen**

Belegen die Informationen des Auftragsverarbeiter, dass dieser über die erforderlichen technischen und organisatorischen Maßnahmen verfügt hat, um angemessen auf die Schwachstelle zu reagieren, sind mit Blick auf die Auftragsverarbeitung keine weiteren Schritte erforderlich, da hinreichend Garantien fortbestehen bzw. diese nicht erschüttert werden. Dies wird bei Hafnium insbesondere der Fall sein, wenn der Auftragsverarbeiter die empfohlenen Gegenmaßnahmen kurzfristig und vollständig umgesetzt hat. Sind die Gegenmaßnahmen zwar ausreichend der Auftragsverarbeiter hat den Verantwortlichen jedoch nicht darüber informiert, sodass eine Anfrage nach Schritt 2 notwendig war, kann es jedoch erforderlich sein den Informationsprozess zwischen Auftragsverarbeiter und Verantwortlichen zu verbessern.

4. **Informationen belegen Mängel bei den technischen und organisatorischen Maßnahmen**

Ergibt sich aus den Informationen, dass ein Umgang mit den Schwachstellen nicht oder nicht vollständig oder zu spät erfolgt ist, sind die Garantien für eine Auftragsverarbeitung zumindest erschüttert oder können in schweren Fällen komplett wegfallen. In diesem Fall sollte sich der Verantwortliche ein umfassendes Bild von den technischen und organisatorischen Maßnahmen beim Auftragsverarbeiter verschaffen und der Auftragsverarbeiter den Verantwortlichen hierbei bestmöglich unterstützen. Dies kann insbesondere durch die Übersendung eines Fragebogens sowie eine Prüfung entsprechender Dokumente, z.B. des Notfallplans, erfolgen. In Ausnahmefällen können, insbesondere wenn keine Dokumente vorgelegt werden können, auch Vor-Ort-Kon-

trollen erforderlich sein. Entdecke Mängel bei den technischen und organisatorischen Maßnahmen müssen durch den Auftragsverarbeiter dann so angepasst werden, dass sie wieder das notwendige Niveau erreichen. Dies kann beispielsweise durch die Verbesserung des IT-Sicherheitsmanagements, aber insbesondere auch durch die Hinzuziehung externer Experten sowie die Anpassung bzw. Ergänzung der Vereinbarung zur Auftragsverarbeitung um vertragliche Vereinbarungen zum Umgang mit Schwachstellen erfolgen. Bei letzteren ist insbesondere an eine Ausgestaltung der Verpflichtungen zur Information und Dokumentation entsprechender Vorfälle zu denken. Die getroffenen Maßnahmen sind gegenüber dem Verantwortlichen nachzuweisen und durch diesen zu kontrollieren. Gelingt es trotz intensiver Bemühungen nicht hinreichend Garantien zu schaffen, was insbesondere der Fall sein wird, wenn sich der Auftragsverarbeiter einem entsprechenden Prozess verweigert, muss der Verantwortliche die Auftragsverarbeitung beenden.

4 Politische Forderungen

4 Politische Forderungen

Die Notwendigkeit der Koordinierung der Aufsichtsbehörden und europäischer ad hoc Kommunikation in ähnlich gelagerten, übergreifenden Fällen wurde im dargestellten Kontext erneut sehr deutlich.

Im Fall des Hafnium-Hacks haben insbesondere deutsche Aufsichtsbehörden unterschiedliche Handlungsempfehlungen gegeben und die Pflicht zur Meldung einer Datenschutzverletzung unterschiedlich bewertet.[7] So gingen einige Aufsichtsbehörden bereits per se von einer Kompromittierung der betroffenen Systeme aus, wenn Patches nach einem bestimmten Datum eingespielt wurden. Dies entspricht weder der Wertung bzw. dem Wortlaut der DSGVO noch etablierten Verfahrensweisen.

Zum Teil wurden auch bereits veröffentlichte Hinweise der Datenschutzaufsichtsbehörden nachträglich noch einmal angepasst. Während wir kritische Reflexion grundsätzlich sehr begrüßen und sie auch für notwendig halten, führte dies in einer akuten Umsetzungs- und Aufbereitungssituation wie nach dem Hafnium-Hack zu zusätzlicher Unsicherheit. Es zeigt vor allem auch, dass ein abgestimmtes Vorgehen insbesondere hier notwendig und richtig gewesen wäre.

Nicht nur, aber insbesondere in einer Situation, in der mehrere tausend Unternehmen mit der Bearbeitung und Aufbereitung eines Angriffs und der Absicherung ihrer Systeme beschäftigt sind, ist eine klare, einheitliche Kommunikation der Aufsichtsbehörden essenziell. Nur durch ein einheitliches Vorgehen kann Rechtssicherheit und Unterstützung für die Unternehmen sichergestellt werden. Dies gilt nicht nur für die deutschen Aufsichtsbehörden und Unternehmen, sondern vor allem auch auf europäischer Ebene, damit die Aufarbeitung des Hafnium-Hacks einheitlich erfolgt und die Unternehmen nicht zusätzlich dadurch belastet werden, dass sie mit verschiedenen Meldepflichten umgehen und sich dynamisch verändernde Hinweise der Aufsichtsbehörden verfolgen müssen.

7 Zu den zahlreichen Herausforderung der unterschiedlichen Interpretation seitens der Landesdatenschutzaufsichtsbehörden und Vorschlägen zur Verbesserung ausführlich hier: **↗https://www.bitkom.org/Bitkom/Publikationen/Struktur-der-Datenschutzaufsichtsbehoerden-in-Deutschland**.

5 Hilfe-Links

5 Hilfe-Links

Artikel-29-Datenschutzgruppe
↗Leitlinien für die Meldung von Verletzungen des Schutzes personenbezogener Daten gemäß der Verordnung (EU) 2016/679

Bitkom
↗Leitfaden »Risk Assessment & Datenschutz-Folgenabschätzung«

EDBP
↗Guidelines 01/2021 on Examples regarding Data Breach Notification

reuschlaw Legal Consultants
↗»Hafnium«-Schwachstellen bei Exchange: Melde- und Benachrichtigungspflichten nach der DSGVO? (mit fortlaufend aktualisierter Übersicht zu den Mitteilungen der Aufsichtsbehörden)
↗»Hafnium«: Mögliche Auswirkungen auf die Auftragsverarbeitung

Bitkom vertritt mehr als 2.700 Unternehmen der digitalen Wirtschaft, davon gut 2.000 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen mehr als 1.000 Mittelständler, über 500 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom