Recht

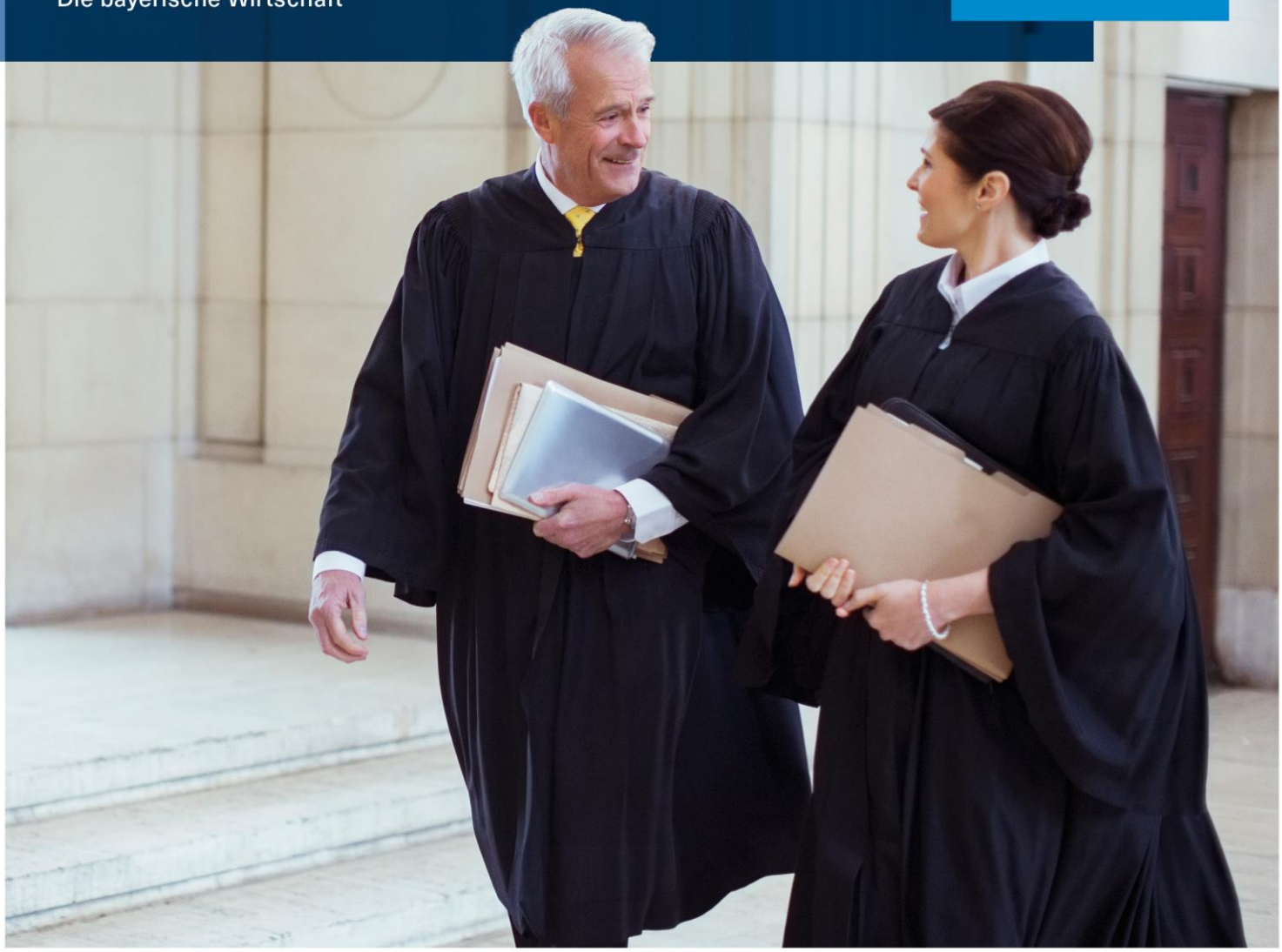
# Datenschutzvorfälle nach Cyberangriffen

FAQ
Stand: Mai 2024

vbw

bayme vbm

Die bayerische Wirtschaft



## Hinweis

# Vorwort

## Schnelles Handeln bei Cyberangriffen

Nach dem aktuellen Bericht des Bundesamtes für Sicherheit in der Informationstechnik ist die Bedrohung im Cyber-Raum so hoch wie nie. Im Falle einer Attacke aus dem Internet müssen die Betroffenen unverzüglich handeln. Es ist daher sinnvoll, einen unternehmensinternen Notfallplan zu erstellen, der bei Bedarf abgearbeitet werden kann. Der Notfallplan sollte mindestens Meldewege, Pläne zur Alarmierung, zum Wiederanlauf, zur Wiederherstellung und Geschäftsfortführung enthalten. In dem Plan sollten auch alle wichtigen Informationen und Aufgabenzuordnungen für die Mitglieder des Notfallteams enthalten sein.

Bei einem Cyberangriff auf IT-Systeme muss neben der Sicherstellung von Daten geprüft werden, ob es zu einer Verletzung des Schutzes personenbezogener Daten gekommen ist. In diesem Fall besteht unter gewissen Voraussetzungen eine Meldepflicht an die zuständigen Datenschutzaufsichtsbehörden und davon betroffene Personen.

Wir haben die häufigsten Fragen zur Melde- und Benachrichtigungspflicht gesammelt und beantwortet. Praxisrelevante Beispiele helfen Ihnen zudem bei der Beurteilung eines Datenschutzvorfalls in Ihrem Unternehmen.

Bertram Brossardt
02. Mai 2024

# Inhalt

# 1 Meldepflicht an die Datenschutzaufsichts-behörde

## Rechtsgrundlage und Voraussetzungen

### 1.1 Wann muss ein Vorfall einer Datenschutzaufsichtsbehörde gemeldet werden?

Im Falle einer Verletzung des Schutzes personenbezogener Daten hat ein Verantwortlicher dies gem. Art. 33 Abs. 1 S. 1 DS-GVO unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde, der zuständigen Datenschutzaufsichtsbehörde zu melden, es sei denn, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Eine Meldepflicht gegenüber der zuständigen Datenschutzaufsichtsbehörde besteht demnach, wenn folgende zwei Voraussetzungen vorliegen:

1. Verletzung des Schutzes personenbezogener Daten (siehe hierzu 1.1.1)
2. Bestehen eines Risikos für die Rechte und Freiheiten natürlicher Personen (siehe hierzu 1.1.2)

#### 1.1.1 Eine Verletzung des Schutzes personenbezogener Daten

Der Begriff der Verletzung des Schutzes personenbezogener Daten ist wie folgt in Art. 4 Nr. 12 DS-GVO definiert:

„Verletzung des Schutzes personenbezogener Daten“ eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.“

Verletzungen des Schutzes personenbezogener Daten lassen sich in folgende drei Kategorien unterteilen, welche als „Folgen der Verletzung des Schutzes personenbezogener Daten“ im Meldeformular des Hessischen Beauftragten für Datenschutz und Informationsfreiheit abgefragt werden und im Falle einer Meldung anzugeben sind:

– Verletzung der Vertraulichkeit, d. h. die unbefugte oder beabsichtigte Preisgabe von oder Einsichtnahme in personenbezogene Daten (z. B. das unbefugte Eindringen in IT-Systeme und die Einsichtnahme in personenbezogene Daten durch einen Hacker);

– Verletzung der Integrität, d. h. die unbefugte oder unbeabsichtigte Änderung personenbezogener Daten (z. B. die unbefugte Änderung von personenbezogenen Daten durch einen Hacker);
– Verletzung der Verfügbarkeit, d. h. der unbefugte oder unbeabsichtigte Verlust des Zugangs zu personenbezogenen Daten oder die unbeabsichtigte oder unrechtmäßige Vernichtung personenbezogener Daten (z. B. Nichtverfügbarkeit eines Krankenhausinformationssystems aufgrund eines Systemfehlers).

Im Meldeformular des Bayerischen Landesamtes für Datenschutzaufsicht werden im Übrigen folgende Arten der Verletzungen des Schutzes personenbezogener Daten mittels Checkboxen abgefragt, woraus man ebenso eine Vorstellung von typischen Vorfällen gewinnen kann:

– Exchange Server Sicherheitslücke
– Cyberangriff
– Schadsoftware (z. B. Malware, Ransomware)
– Software- oder Konfigurationsfehler
– Diebstahl (z. B. gezielte Entwendung von Datenträgern nach Einbruch)
– Verlust (z. B. Unauffindbarkeit eines Notebooks)
– Fehlversendung
– Buchungs- oder Eingabefehler
– Anderweitige Informationsweitergabe
– Sonstiges […]

### 1.1.2 Risiko für die Rechte und Freiheiten natürlicher Personen

Eine Meldepflicht besteht nur dann, wenn neben einer Verletzung des Schutzes personenbezogener Daten ein Risiko für die Rechte und Freiheiten natürlichen Personen besteht. Da es vollständig risikolose Vorfälle nicht gibt, wird die unklare Formulierung in Art. 33 Abs. 1 S. 1 DS-GVO „nicht zu einem Risiko“ von ihrem Sinn und Zweck ausgehend als „nur zu einem geringen Risiko“ führend verstanden.

Der Begriff des Risikos ist in der DS-GVO nicht ausdrücklich definiert. Die Datenschutzkonferenz (DSK), das Gremium der unabhängigen Datenschutzbehörden des Bundes und der Länder definiert den Begriff des Risikos als „das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (einschließlich ungerechtfertigter Beeinträchtigung von Rechten und Freiheiten natürlicher Personen) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann“.

Das Risiko bestimmt sich aus dem Zusammenspiel zwischen der Schwere des möglichen Schadens und der Eintrittswahrscheinlichkeit.

In S. 1 des Erwägungsgrundes 85 der DS-GVO sind insoweit folgende mögliche Schäden genannt:

- Verlust der Kontrolle über ihre personenbezogenen Daten
- Einschränkung ihrer Rechte
- 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 für die betroffene natürliche Person

Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten der betroffenen Person sollten in Bezug auf die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung bestimmt werden.

### Hinweis

---

Bei der abschließenden Bewertung und Prüfung, ob nur ein geringes Risiko oder ein „echtes“ Risiko bzw. hohes Risiko gegeben ist, sollte man sich an der Risikomatrix der DSK im Kurzpapier Nr. 18, Risiko für die Rechte und Freiheiten natürlicher Personen, 26.04.2018, S. 5, orientieren https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_18.pdf

---

Beispiele bei denen in der Regel ein geringes Risiko vorliegt und somit keine Meldepflicht besteht:

- Unbefugte erhalten Zugang zu personenbezogenen Daten, die nach dem neuesten Stand der Technik verschlüsselt sind (z. B. auf Server oder USB-Stick).
- Fehlversandter Brief kommt ungeöffnet zurück.
- Durch menschliches Versagen werden zwei Lieferscheine verwechselt, so dass die Produkte samt Lieferscheinen mit personenbezogenen Daten an den jeweils falschen Kunden verschickt werden und diese die falschen Lieferungen erhalten. Nach Kenntnis fordert der Händler die Bestellungen zurück und sendet sie anschließend an die richtigen Empfänger.

Zahlreiche weitere Beispiele sowie Beispiele, bei denen eine Meldepflicht besteht, sind in Abschnitt III aufgelistet.

## 1.2 Welche Informationen müssen der zuständigen Datenschutzaufsichtsbehörde gemeldet werden und wie geht man bei der Meldung am besten vor?

Gemäß Art. 33 Abs. 3 DS-GVO muss die Meldung zumindest folgende Informationen enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Kategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine 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.

### Hinweis

Die Landesdatenschutzaufsichtsbehörden stellen in der Regel Meldeformulare bereit. Es empfiehlt sich diese auszufüllen und an die Behörde zu versenden. In diesen Formularen werden alle erforderlichen Informationen abgefragt.

Das Formular des Bayerischen Landesamts für Datenschutzaufsicht finden Sie unter https://www.lda.bayern.de/de/datenpanne.html

Erläuterungen zum Formular des LDA Bayern sind dort zu entnehmen. Dieser Online-Service des LDA Bayern richtet sich ausschließlich an Verantwortliche und nicht an die vom Vorfall betroffenen Privatpersonen, die stattdessen den ebenfalls auf dieser Webseite verfügbaren Online-Service zur Beschwerde nutzen können. Als Meldenachweis erhält der Meldende unmittelbar nach Absenden eine eigene ID (Kennung) zur Meldung über das Webformular des LDA Bayern. Diese wird beim LDA Bayern dem gemeldeten Vorgang zugewiesen und kann als erster Nachweis der Meldung inklusive des Meldezeitpunkts verwendet werden. Es handelt sich nicht um ein offizielles Behördenaktenzeichen. Ein solches Aktenzeichen wird dem Verantwortlichen im weiteren schriftlichen Verfahren gegebenenfalls mitgeteilt.

## 1.3 An welche Behörde ist ein meldepflichtiger Vorfall zu melden?

Der Vorfall ist an die für den Verantwortlichen zuständige Datenschutzaufsichtsbehörde zu melden. Aus Art. 55 DS-GVO ergibt sich, dass jede Aufsichtsbehörde „für die Erfüllung der Aufgaben und die Ausübung der Befugnisse, die ihr […] übertragen wurden, im Hoheitsgebiet ihres eigenen Mitgliedstaats zuständig“ ist. In Art. 55 DS-GVO ist das Territorialprinzip niedergelegt, ohne allerdings Einfluss auf die innerstaatliche Aufteilung der Zuständigkeit zu nehmen.

Welche Datenschutzaufsichtsbehörde in Deutschland für die Meldung zuständig ist, ergibt sich aus § 40 BDSG in Verbindung mit den Landesdatenschutzgesetzen. Demnach ist ein Datenschutzvorfall bei einem Unternehmen in Bayern beim Bayerischen Landesamt für Datenschutzaufsicht zu melden.

Bei einer Datenverarbeitung in Deutschland, bei der Niederlassungen mehrerer Bundesländer beteiligt sind, ist die Meldung in Anlehnung an § 40 Abs. 2 BDSG nur bei der Behörde der Hauptniederlassung erforderlich.

Beispiel: Unternehmen A hat die Hauptniederlassung in Wiesbaden und eine Zweigstelle in München. Ein Angreifer erhält Zugriff auf das CRM-System, das in Wiesbaden betrieben wird, auf das aber auch Mitarbeiter von München aus zugreifen können. In diesem Fall ist nur eine Meldung beim Hessischen Beauftragten für Datenschutz und Informationsfreiheit erforderlich.

In vielen Fällen empfiehlt es sich aber, dennoch mehrere Datenschutzaufsichtsbehörden zu informieren.

## 1.4 Welche Frist gilt für die Meldung des Vorfalls bei der Datenschutzaufsichtsbehörde?

Aus Art. 33 Abs. 1 S. 1 DS-GVO ergibt sich, dass der „Verantwortliche unverzüglich und möglichst binnen 72 Stunden, nachdem ihm die Verletzung bekannt wurde“ zu melden hat.

Die Artikel-29-Datenschutzgruppe, das ehemalige unabhängigen Beratungsgremium der Europäischen Kommission in Fragen des Datenschutzes, ging dann von einer Kenntnisnahme aus, „wenn der betreffende Verantwortliche eine hinreichende Gewissheit darüber hat, dass ein Sicherheitsvorfall aufgetreten ist, der zu einer Beeinträchtigung des Schutzes personenbezogener Daten geführt hat. […] Wann genau davon auszugehen ist, dass einem Verantwortlichen eine bestimmte Datenschutzverletzung „bekannt“ wurde, hängt von den konkreten Umständen der Datenschutzverletzung ab. In einigen Fällen dürfte von Anfang an klar sein, dass eine Datenschutzverletzung vorliegt, in anderen hingegen kann womöglich erst nach einer gewissen Zeit festgestellt werden, ob personenbezogene Daten beeinträchtigt wurden.“

Nach ganz überwiegender Ansicht läuft die 72-Stundenfrist auch am Wochenende bzw. an Feiertagen weiter und das Fristende verlängert sich auch nicht bis zum nächsten Arbeitstag, wenn die 72-Stunden-Frist an einem Feiertag oder am Wochenende endet.

Sofern dem Verantwortlichen innerhalb der angemessenen Reaktionszeit nicht alle notwendigen Informationen zur Verfügung stehen, ist er dennoch zur Meldung verpflichtet. Fehlende Informationen sind der Behörde dann nachzureichen.

Erfolgt die Meldung an die Datenschutzaufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen (Art. 33 Abs. 1 S. 2 DS-GVO).

## 1.5 Welche Vorbereitungen sollten getroffen werden, damit die Meldefrist eingehalten werden kann?

Es sollte präventiv ein Prozess implementiert werden, der eine schnelle Meldung sicherstellen kann. Hierzu zählt insbesondere folgendes:

- Sensibilisierung bzw. Schulung der Mitarbeiter;
- Bereitstellung eines Formulars für die Mitarbeiter, um Vorfälle schnell dokumentieren zu können;
- Festlegung von Verantwortlichkeiten und internen Meldeprozessen, über die in den oben genannten Schulungen informiert werden sollte;
- Ggf. Vorhalten von Kontaktdaten von spezialisierten Rechtsanwälten und IT-Forensikern.

## 1.6 Wer muss einen meldepflichtigen Vorfall melden – der Verantwortliche oder der Auftragsverarbeiter (Dienstleister)?

Der Verantwortliche (in Auftragsverarbeitungsverhältnisse, auch häufig als Auftraggeber bezeichnet) muss einen meldepflichtigen Vorfall bei der Datenschutzaufsichtsbehörde melden. Der Auftragsverarbeiter ist im Regelfall dazu verpflichtet, den Verantwortlichen über entsprechende Vorfälle zu informieren, so dass dieser seinen Meldepflichten nachkommen kann (vgl. Art. 28 Abs. 3 lit. f DS-GVO).

### Exkurs

Die Definition des Verantwortlichen ergibt sich aus Art. 4 Nr. 7 DS-GVO:

*„Verantwortlicher“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten*

*vorgegeben, so kann der Verantwortliche beziehungsweise können die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.*

---

## 1.7 Kann die Datenschutzaufsichtsbehörde die gemeldeten Informationen im Rahmen eines Straf- oder Bußgeldverfahrens nutzen?

§ 42 Abs. 4 und § 43 Abs. 4 BDSG regeln, dass eine Meldung nach Art. 33 DS-GVO oder eine Benachrichtigung nach Art. 34 DS-GVO in einem Straf- oder Bußgeldverfahren nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden darf. Inwieweit dieses Zustimmungserfordernis tatsächlich gilt und ob die genannten Normen aufgrund einer Europarechtswidrigkeit nicht anzuwenden sind, ist im Einzelnen umstritten. Im Zweifel muss man damit rechnen, dass die Angaben, insbesondere solche, die nicht zwingend erforderlich sind, zumindest im Rahmen eines Bußgeldverfahrens verwendet werden.

## 1.8 Was macht die Datenschutzaufsichtsbehörde nach einer Meldung? Welche Risiken bestehen?

Sofern (i) in der Meldung geeignete Maßnahmen zu ergriffenen und geplanten Maßnahmen genannt werden und (ii) der Behörde der Eindruck vermittelt wird, dass die Situation unter Kontrolle ist und bei der Bearbeitung des Vorfalls professionell vorgegangen wird, teilt die Behörde in den meisten Fällen lediglich mit, dass der Fall für sie erledigt ist.

Sofern in der Meldung erwähnt wird, dass ein Forensiker den Fall untersucht, kommt es gelegentlich vor, dass die Behörde den forensischen Abschlussbericht anfordert. Ein Problem kann dies ggf. dann darstellen, wenn im forensischen Abschlussbericht Mängel bei den technischen und organisatorischen Maßnahmen aufgeführt werden, wie z. B. dass die Angreifer vermutlich aufgrund schwacher Passwörter Zugriff auf die Systeme erhalten konnten. Entsprechende Mängel könnte die Behörde ggf. beanstanden.

In Einzelfällen fordert die Behörde weitere Detailinformationen an.

Nicht ganz auszuschließen ist auch, dass die Behörde sich das Unternehmen bzw. die entsprechende Website genauer ansieht und beispielsweise prüft,

- ob für das Unternehmen ein Datenschutzbeauftragter bestellt und gemeldet wurde;
- ob die Datenschutzhinweise auf der Website ausreichend sind und
- ob bei Kontaktformularen auf der Website eine ausreichende Verschlüsselung sichergestellt ist.

In Ausnahmefällen nimmt die Behörde auch die Meldung zum Anlass, weitergehende datenschutzrechtliche Prüfungen vorzunehmen, die nicht zwingend im Zusammenhang mit dem Vorfall stehen und entsprechende Informationen anzufordern.

## 1.9 Welche Pflichten bestehen neben der Meldung an die Datenschutzaufsichtsbehörde?

Gem. Art. 33 Abs. 5 S. 1 DS-GVO besteht die Pflicht „Verletzungen des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang mit der Verletzung des Schutzes personenbezogener Daten stehenden Fakten, ihrer Auswirkungen und der ergriffenen Abhilfemaßnahmen“ zu dokumentieren.

## 1.10 Was ist zu tun, wenn ein Vorfall nicht gemeldet wird?

In diesem Fall ist der Vorfall und die Gründe, warum keine Meldung erfolgt ist (Risikoanalyse), zu dokumentieren. Die Dokumentation sollte im Bedarfsfall der zuständigen Datenschutzaufsichtsbehörde vorgelegt werden können.

# 2 Benachrichtigungspflicht gegenüber betroffenen Personen

## Rechtsgrundlage und Voraussetzungen

Neben der Pflicht zur Meldung der Datenpanne gegenüber der zuständigen Datenschutzaufsichtsbehörde kann der Verantwortliche – je nach den Umständen des Einzelfalls – auch dazu verpflichtet sein, die betroffene Person direkt über den Vorfall zu benachrichtigen.

### 2.1 Wann besteht eine Benachrichtigungspflicht gegenüber betroffenen Personen?

Eine Benachrichtigungspflicht gegenüber den betroffenen Personen setzt gemäß Art. 34 Abs. 1 DS-GVO voraus, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat. Während eine Meldepflicht gegenüber der zuständigen Datenschutzaufsichtsbehörde häufig gegeben sein wird, muss dies im Hinblick auf die Verpflichtung zur Benachrichtigung der betroffenen Person intensiver überprüft werden und wird im Regelfall die Ausnahme sein. Auch bei der hierbei anzustellenden Risikobeurteilung, sind die in Abschnitt 1.1.2 aufgeführten Kriterien maßgeblich zu berücksichtigen.

In Abschnitt III sind zahlreiche Fälle aufgelistet, bei denen jeweils angegeben ist, ob eine Benachrichtigungspflicht besteht.

### 2.2 Welche Ausnahmen von der Benachrichtigungspflicht gegenüber betroffenen Personen gibt es?

Eine Meldung ist gemäß Art. 34 Abs. 3 DS-GVO dann nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

- 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;
- der Verantwortliche hat durch nachfolgende Maßnahmen sichergestellt, dass das hohe Risiko für die Rechte und Freiheiten der betroffenen aller Wahrscheinlichkeit nach nicht mehr besteht;
- die Benachrichtigung wäre mit einem unverhältnismäßigen Aufwand verbunden. In diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche

Maßnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

## 2.3 Welche Informationen müssen den betroffenen Personen mitgeteilt werden?

Die betroffenen Personen müssen über folgende Informationen in Kenntnis gesetzt werden:

- die Art der Verletzung des Schutzes personenbezogener Daten (Art. 34 Abs. 2 DS-GVO);
- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen (Art. 34 Abs. 2 DS-GVO i. V. m. Art. 33 Abs. 3 lit. b DS-GVO);
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten (Art. 34 Abs. 2 DS-GVO i. V. m. Art. 33 Abs. 3 lit. c DS-GVO);
- eine 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 (Art. 34 Abs. 2 DS-GVO i. V. m. Art. 33 Abs. 3 lit. b DS-GVO).

### Praxistipp

Wie bei der Meldung gegenüber der Behörde gilt auch hier, dass es oftmals ratsam ist, für die Information an die betroffenen Personen entsprechend spezialisierte Rechtsanwälte hinzuzuziehen.

## 2.4 Welche Frist gilt für die Benachrichtigung gegenüber betroffenen Personen?

Die Benachrichtigung muss „unverzüglich“, also ohne schuldhaftes Zögern erfolgen. Anders als für die Meldung gegenüber der Datenschutzaufsichtsbehörde gibt es aber keine 72-Stunden-Frist.

Nach den Erwägungsgründen der DS-GVO (vgl. Erwägungsgrund 86) sollen solche Benachrichtigungen der betroffenen Person stets so rasch wie nach allgemeinem Ermessen möglich, in enger Absprache mit der Datenschutzaufsichtsbehörde und nach Maßgabe der von dieser oder von anderen zuständigen Behörden, wie beispielsweise Strafverfolgungsbehörden, erteilten Weisungen erfolgen. Um beispielsweise das Risiko eines unmittelbaren Schadens mindern zu können, müssen betroffene Personen sofort benachrichtigt werden, wohingegen eine längere Benachrichtigungsfrist gerechtfertigt sein kann, wenn es

darum geht, geeignete Maßnahmen gegen fortlaufende oder vergleichbare Verletzungen des Schutzes personenbezogener Daten zu treffen.

## 2.5 Was ist zu tun, wenn die betroffenen Personen nicht über einen Vorfall benachrichtigt werden?

In diesem Fall sind die Gründe für die Nichtbenachrichtigung zu dokumentieren. Im Meldeformular des Bayerischen Landesamtes für Datenschutzaufsicht wird ohnehin ausdrücklich nach einer Begründung gefragt, so dass dies dort zu dokumentieren ist.

# 3 Was sind typische meldepflichtige und benachrichtigungspflichtige Fälle?

## Beispiele aus der Praxis

Typische meldepflichtige Fälle sind beispielsweise Hacking-Angriffe, bei denen durch den Angreifer ein Zugriff auf personenbezogene, wie z. B. Kunden- oder Mitarbeiterdaten, erfolgt oder ein E-Mail-Fehlversand mit Daten zahlreichen betroffenen Personen und sensiblen personenbezogenen Daten.

### Hinweis

Umfangreiche Übersichten mit zahlreichen weiteren Beispielen zu Melde- und Benachrichtigungspflichten sind unter folgenden Links einsehbar:

- Das Bayerische Landesamt für Datenschutzaufsicht, Art. 33 und 34 DS-GVO – Was gemeldet werden muss, https://www.lda.bayern.de/media/veroeffentlichungen/Flyer_Datenschutzverletzung.pdf
- Die Landesbeauftragte für den Datenschutz Niedersachsen, Meldung von Datenschutzverstößen, Fragen und Antworten zur DS-GVO, https://lfd.niedersachsen.de/download/157941 (abgerufen am 11. März 2022)
- Artikel-29-Datenschutzgruppe, WP250 rev.1, 6 February 2018, Guidelines on Personal data breach notification under Regulation 2016/679 – endorsed by the EDPB, https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612052
- Europäischer Datenschutzausschuss, Guidelines 9/2022 on personal data breach notification under GDPR, Guidelines 9/2022 on personal data breach notification under GDPR | European Data Protection Board (europa.eu)

Der EDSA hat in der Konsultationsfassung der Guidlines 01/2021 on Examples regarding Data Breach Notification vom 14. Januar 2021 Beispiele zur Verfügung gestellt. Diese sind im Folgenden der besseren Übersicht halber zusammengefasst:

Tabelle 1
Examples regarding Data Breach Notification

| Case No. | Fallbeschreibung | Meldepflicht an die Aufsichtsbehörde | Benachrichtigungspflicht an betroffene Personen |
|---|---|---|---|
| 1 | Erfolgreicher Ransomware-Angriff mit Verschlüsselung der Daten eines IT-Systems zwecks Lösegelderpressung. Mittels Back-up können alle Daten innerhalb weniger Stunden wiederhergestellt werden. Die Daten waren zuvor mittels At-Rest-Verschlüsselung gesichert und der Entschlüsselungsschlüssel hierfür wurde nicht von den Angreifern erlangt. Die Protokollauswertungen des angegriffenen Unternehmens zeigen, dass keine Daten nach außen übermittelt wurden. | Nein | Nein |
| 2 | Wie 1, aber ohne elektronisches Back-up. Die Daten konnten aber größtenteils mittels Papieraufzeichnungen innerhalb von 5 Tagen wiederhergestellt werden, wodurch es zu geringen Lieferverzögerungen gegenüber Kunden kam. | Ja | Nein |
| 3 | Wie 1 mit dem Unterschied, dass ein Krankenhausinformationssystem betroffen ist und dass die Datenwiederherstellung 2 Tage gedauert hat und die Patientenversorgung beeinträchtigt hat. | Ja | Ja |
| 4 | Erfolgreicher Ransomware-Angriff mit Verschlüsselung der Daten eines IT-Systems zwecks Lösegelderpressung. Es werden Datenabflüsse festgestellt. Es sind Daten von Kunden und Mitarbeitern betroffen. Das Back-up wird vom Angreifer ebenfalls verschlüsselt. | Ja | Ja |

| | | | |
|---|---|---|---|
| 5 | Kompromittierung eines Systems eines Personalvermittlers mit Bewerberdaten. Die aufgespielte Malware hat Funktionen, um Daten abzurufen und die Historie des Datenabflusses zu löschen. Die Malware wird einen Monat nach der Installation erkannt. | Ja | Ja |
| 6 | Ausnutzung einer SQL-Schwachstelle einer Koch-Website durch Angreifer und Zugriff auf 1200 Nutzernamen und auf ebenso viele mit starkem Algorithmus gehashte Passwörter, wobei auf das „Salz“ im Zusammenhang mit dem Hash-Algortihmus nicht zugegriffen werden konnte. Die betroffenen Personen wurden per E-Mail über die Sicherheitsverletzung informiert und zur Passwortänderung aufgefordert, insbesondere wenn das gleiche Passwort für andere Dienste verwendet wird. | Nein | Nein |
| 7 | Cyberangriff auf Online-Banking-Website und Zugriff auf Daten von 100.000 Kunden und Zugriff auf Konten von 2.000 Kunden. Es kann ausgeschlossen werden, dass der Angreifer Zahlungstransaktionen durchgeführt hat. | Ja | Ja |
| 8 | Ein Mitarbeiter kopiert nach seiner Kündigung innerhalb der Kündigungsfrist Geschäftsdaten (insbesondere Kontaktdaten von Geschäftspartnern) und nutzt diese später, um die Geschäftskontakte für Geschäftszwecke seines neuen Arbeitgebers zu kontaktieren. | Ja | Nein |
| 9 | Versehentliche Übermittlung von Daten über zwei Duzend Kunden an einen Berufsgeheimnisträger, der auch vertraglich verpflichtet ist, entsprechende Verletzungen des Schutzes personenbezogener Daten dem Absender mitzuteilen. Der Berufsgeheimnisträger teilt dies mit, löscht die Daten und bestätigt die Löschung. | Nein | Nein |
| 10 | Diebstahl von mit starken Passwörtern verschlüsselten Tablets und bei vorhandenem Back-up und bei erfolgtem Fernbefehl die Daten auf den Tablets zu löschen. | Nein | Nein |

| | | | |
|---|---|---|---|
| 11 | Ein (elektronisches) Notebook mit Daten von 100.000 Kunden wird gestohlen. Die Festplatte ist nicht passwortgeschützt. | Ja | Ja |
| 12 | In einer Reha-Einrichtung für Drogenabhängige wird ein Notizbuch in Papierform gestohlen. Das Buch enthält grundlegende Identitäts- und Gesundheitsdaten der in der Reha-Einrichtung aufgenommenen Patienten. Die Daten waren nur auf Papier gespeichert und den behandelnden Ärzten stand keine Sicherungskopie zur Verfügung. | Ja | Ja |
| 13 | Bei einem Einzelhandelsunternehmen werden durch menschliches Versagen zwei Lieferscheine verwechselt, so dass die Produkte samt Lieferscheine mit personenbezogenen Daten an den jeweils falschen Kunden verschickt werden und diese die falschen Lieferungen erhalten. Nach Kenntnis fordert der Händler die Bestellungen zurück und sendet sie anschließend an die richtigen Empfänger. | Nein | Nein |
| 14 | Eine öffentliche Arbeitsvermittlungsstelle schickt eine E-Mail-Nachricht - über bevorstehende Schulungen - an die in ihrem System als Arbeitsuchende registrierten Personen. Versehentlich wird ein Dokument mit den persönlichen Daten dieser Arbeitsuchenden (Name, E-Mail-Adresse, Postanschrift, Sozialversicherungsnummer) an diese E-Mail angehängt. Die Zahl der betroffenen Personen beträgt mehr als 60.000. | Ja | Ja |
| 15 | Eine Teilnehmerliste für einen Kurs in Rechtsenglisch, der 5 Tage lang in einem Hotel stattfindet, wird versehentlich an 15 ehemalige Teilnehmer des Kurses statt an das Hotel geschickt. Die Liste enthält die Namen, E-Mail-Adressen und Essenspräferenzen der 15 Teilnehmer. Zwei Teilnehmer haben bei Essenspräferenzen angegeben, dass sie laktoseintolerant sind. Der für die Verarbeitung Verantwortliche entdeckt den Fehler unmittelbar nach dem Versenden der Liste und informiert die Empfänger über den Fehler und fordert sie auf, die Liste zu löschen. | Nein | Nein |

| | | | |
|---|---|---|---|
| 16 | Aufgrund eines mechanischen Fehlers werden von einem Versicherungsunternehmen zwei Briefe für verschiedene Versicherungsnehmer in einen Umschlag gesteckt und per Briefpost an einen Versicherungsnehmer verschickt. Folgende Daten sind betroffen: Name, Anschrift, amtliches Fahrzeugkennzeichen, Versicherungstarife für das laufende und das nächste Versicherungsjahr, ungefähre Kilometerleistung und Geburtsdatum des jeweiligen Versicherungsnehmers. Nicht betroffen sind Gesundheitsdaten gemäß Art. 9 DS-GVO Zahlungsdaten (Bankverbindung). Auch sind neben den bereits genannten Daten keine weiteren Wirtschafts- oder Finanzdaten betroffen. | Ja | Nein |
| 17 | Identitätdiebstahl:<br>Der Callcenter eines Telekommunikationsunternehmens erhält einen Telefonanruf von jemandem, der sich als Kunde ausgibt. Der angebliche Kunde fordert das Unternehmen auf, die E-Mail-Adresse zu ändern, an die die Rechnungsinformationen von nun an gesendet werden sollen. Der Mitarbeiter des Callcenters überprüft die Identität des Kunden, indem er entsprechend den festgelegten Prozessen zwecks Authentifizierung nach bestimmten persönlichen Daten fragt. Der Anrufer gibt korrekt die Steuernummer und die Postanschrift des angefragten Kunden an. Ihm war dies möglich, da er Zugang zu diesen Daten hatte. Anschließend nimmt das Telekommunikationsunternehmen die gewünschte Änderung vor und die Rechnungsdaten werden an die neue E-Mail-Adresse gesendet. Das Verfahren sieht keine Benachrichtigung des früheren E-Mail-Kontakts vor. | Ja | Ja |

| | | | |
|---|---|---|---|
| 18 | Eine Supermarktkette entdeckt 3 Monate nach der Konfiguration, dass einige E-Mail-Konten verändert worden waren und Regeln erstellt worden waren, nach denen E-Mails verschoben und weitergeleitet wurden. Ferner wurde durch einen Social-Engineering-Angriff erreicht, dass Kontodaten geändert wurden und es wurden gefälschte Rechnungen mit falschen Kontodaten verschickt.<br><br>Der Angreifer gelangte somit an Daten von 99 Mitarbeitern bezüglich Name, Familienstand, Anzahl der Kinder, Lohn, Arbeitszeiten und Restinformationen über den Gehaltseingang (nicht alle diese Informationen zu allen betroffenen Mitarbeitern). | Ja | Ja |

Weitere Beispiele finden Sie in den EDSA Guidelines 9/2022 on personal data breach notification under GDPR, Guidelines 9/2022 on personal data breach notification under GDPR | European Data Protection Board (europa.eu).

# Ansprechpartner/Impressum

## Kristina Fink
Grundsatzabteilung Recht

Telefon 089-551 78-234
kristina.fink@vbw-bayern.de

## Impressum

Alle Angaben dieser Publikation beziehen sich ohne jede Diskriminierungsabsicht grundsätzlich auf alle Geschlechter.

### Herausgeber

**bayme**
Bayerischer Unternehmensverband Metall und Elektro e. V.

**vbm**
Verband der Bayerischen Metall- und Elektro-Industrie e. V.

**vbw**
Vereinigung der Bayerischen Wirtschaft e. V.

Max-Joseph-Straße 5
80333 München

www.baymevbm.de www.vbw-bayern.de

### Autor:

Dr. Oliver Hornung
SKW Schwarz Rechtsanwälte

Telefon 069-63 00 01-65
o.hornung@skwschwarz.de