Spezialausgabe September 2025

PRIVACY@WORK

FÜR DATENSCHUTZBEAUFTRAGTE

Datenpannen geschickt managen

PRIVACY PERTS

ANDREAS WÜRTZ – IHR EXPERTE FÜR DATENSCHUTZ
ANDREAS WÜRTZ VERFÜGT ÜBER MEHR ALS 17 JAHRE BERUFSERFAHRUNG ALS VOLLZEIT-DATENSCHÜTZER IM UNTERNEHMEN. ER ZEIGT IHNEN, WIE SICH DATENSCHUTZ PRAGMATISCH UMSETZEN LÄSST.

Kennen Sie Edward Aloysius Murphy junior?

Liebe Leserin, lieber Leser,

Sie fragen sich, wer Edward A. Murphy junior ist? Das war ein amerikanischer Ingenieur, der folgende Gesetzmäßigkeit als „Murphy's Law" bekannt machte: „Alles, was schiefgehen kann, geht schief." Und vielleicht kennen auch Sie Beispiele, die dieses „Naturgesetz" zu bestätigen scheinen, möglicherweise auch im Datenschutz. Doch weil etwas schiefgehen kann, sollte man nicht warten, bis es so weit ist. Vorbeugen ist immer besser, und zwar erst recht im Datenschutz. Kommt es etwa gar nicht erst zu einer Datenpanne, ist viel gewonnen. Und Sie haben die Bestätigung, dass Murphy's Law eben nicht immer zutrifft.

Viele Grüße

Andreas Würtz, Rechtsanwalt und Chefredakteur des Ratgebers „Datenschutz aktuell"

DATENSCHUTZPANNEN: KÖNNEN SIE DIESE FRAGEN BEANTWORTEN?

Wo gehobelt wird, da fallen Späne. An dieser Weisheit ist natürlich viel dran, schließlich kann auch im Umgang mit personenbezogenen Daten mal etwas schiefgehen. Doch wenn das der Fall ist, sind vor allem Sie als Datenschutzbeauftragter gefragt. Denn Sie sind derjenige, der sich den dann aufkommenden Fragen stellen muss. So können Sie auf einige typische Fragen rund um Datenschutzpannen antworten.

Was versteht man unter einer Datenschutzpanne?

Wenn von Datenschutzpannen, Datenpannen oder Datenlecks die Rede ist, wird damit umgangssprachlich zum Ausdruck gebracht, was die Datenschutz-Grundverordnung (DSGVO) mit dem Begriff „Verletzung des Schutzes personenbezogener Daten" meint. Was der Gesetzgeber darunter versteht, ergibt sich aus Art. 4 Nr. 12 DSGVO. Bei einer „Verletzung des Schutzes personenbezogener Daten" handelt es sich um eine Verletzung der Sicherheit der Verarbeitung personenbezogener Daten. Diese kann unrechtmäßig oder unbeabsichtigt zu Folgendem führen:

- zur Vernichtung,
- zum Verlust,
- zur Veränderung oder
- zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu

personenbezogenen Daten, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.

Dabei ist wichtig hervorzuheben: Es kommt nicht darauf an, ob das zufällig schiefgeht, absichtlich passiert oder ob Kriminelle ihre Finger im Spiel haben. Dass es zu einer Verletzung gekommen ist, reicht aus.

Auch das zweite Merkmal ist wichtig, und zwar die „Sicherheit der Verarbeitung". Was damit gemeint ist, ergibt sich aus Art. 32 DSGVO. Die dortige Festlegung können Sie wie folgt auf den Punkt bringen: Ihr Unternehmen muss geeignete technische und organisatorische Maßnahmen treffen und

umsetzen. Diese müssen dazu führen, dass personenbezogene Daten risikoangemessen geschützt sind. Dabei gilt als Faustformel: Je schützenswerter personenbezogene Daten und je größer die Risiken etwa bei Diebstahl, Missbrauch oder Veröffentlichung sind, desto mehr Aufwand muss getrieben werden, um das Risiko auf ein vertretbares Maß zu reduzieren.

Praxisbeispiele schaffen Verständnis

Eventuell meinen manche: Datenpannen sind etwas, das in Ihrem Unternehmen eigentlich nicht vorkommen kann. Zeigen Sie auf, dass das Gegenteil der Fall sein dürfte. Überlegen Sie, was schiefgehen und beispielsweise zu einer unbefugten Offenlegung von personenbezogenen Daten führen könnte. Typische Beispiele sind:

- Fehlkonfiguration des Onlineshops. Kundendaten sind so durch Unbefugte einsehbar.
- Falsche Adressierung einer Werbe-E-Mail (Nutzung An-/Cc-Feld anstatt Bcc-Feld) oder falsche Nutzung eines E-Mail-Verteilers, sodass alle Empfänger erfahren, wer Empfänger ist. Je nach Inhalt, kann die Kenntnis der Empfänger erhebliche Nachteile für die Betroffenen mit sich bringen.
- Vertauschte Adressen oder Inhalte bei Gehaltsabrechnungen, Schreiben der Personalabteilung oder Rechnungen an Kunden. Informationen gelangen so an die falschen Empfänger.

Spielen auch andere Pannen im Unternehmen eine Rolle?

Auch wenn bei einer Panne personenbezogene Daten nicht konkret betroffen sind, sollte niemand im Unternehmen die Sache auf die leichte Schulter nehmen. Das hat gleich mehrere Gründe:

- Auch geschäftliche Informationen, z. B. zu Produkten, Preisen oder Herstellungsverfahren, sind natürlich wertvoll. Geraten sie in falsche Hände, kann das für Ihr Unternehmen teuer werden, gerade wenn etwa die Konkurrenz dadurch besser, schneller oder kostengünstiger wird.
- Meist sind Pannen oder Defizite im IT-Umfeld auch Ausgangspunkt für Datenschutzpannen. Werden Systeme oder Netzwerke gehackt, sind

Kriminelle meist nicht wählerisch. Sie nehmen alles mit, was sie finden, und beurteilen deren Wert bzw. deren Eignung für weitere Aktivitäten (z. B. Lösegelderpressung) erst später.

- Je nach Geschäftstätigkeit Ihres Unternehmens können weitere Meldepflichten bestehen. So z. B., wenn es zur kritischen Infrastruktur zählt. Haben Störungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit von informationstechnischen Systemen, Komponenten oder Prozessen zu einem Ausfall oder zu einer erheblichen Störung der kritischen Infrastruktur geführt, muss das dem Bundesamt für Sicherheit in der Informationstechnik (BSI) unverzüglich gemeldet werden (§ 8b Abs. 4 BSI-Gesetz).

Was ist zu tun, wenn es zu einer Datenschutzpanne kommt?

Zunächst ist erforderlich, dass die Panne behoben bzw. die Datenlücke geschlossen wird, sprich, es darf nicht weiter zu einem Verstoß kommen. Das

kann auch bedeuten, dass eine Verarbeitung vorübergehend eingestellt wird. Daneben muss Ihr Unternehmen auch Folgendes auf dem Radar haben:

- **Dokumentation:** Ihr Unternehmen muss jede Datenschutzpanne dokumentieren, sprich jede Verletzung des Schutzes personenbezogener Daten. Dies umfasst alle im Zusammenhang mit der Datenschutzpanne stehenden Fakten, deren Auswirkungen und die ergriffenen Abhilfemaßnahmen. Ferner ergibt sich aus Art. 33 Abs. 5 Satz 2 DSGVO, dass die Dokumentation der Aufsichtsbehörde die Überprüfung der Einhaltung der Anforderungen aus Art. 33 DSGVO ermöglichen muss. Die Behörde muss den Vorfall bewerten können. So auch die Frage, ob etwa eine Meldung an die Aufsichtsbehörde oder eine Information der Betroffenen erforderlich ist.
- **Meldung:** Kommt es zu einer Datenschutzpanne, muss Ihr Unternehmen grundsätzlich unverzüglich, spätestens jedoch binnen 72 Stunden, der zuständigen Datenschutzaufsichtsbehörde den Vorfall melden (Art. 33 Abs. 1 DSGVO). Nur wenn die Datenschutzpanne voraussichtlich zu keinem Risiko für die Rechte und Freiheiten natürlicher Personen führt, kann die Meldung dem Wortlaut nach unterbleiben. Aber: Manche Aufsichtsbehörden bestehen nicht auf einer Meldung, wenn das Risiko niedrig ist. Checken Sie daher unbedingt die Webseite der zuständigen Aufsichtsbehörde bezüglich deren Handhabung.
- **Information:** Ergibt sich aus der Risikobewertung der Datenschutzpanne, dass diese zu einem voraussichtlich hohen Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen führt, muss Ihr Unternehmen zusätzlich die betroffenen Personen unverzüglich über die Datenschutzpanne informieren (Art. 34 Abs. 1 DSGVO).

Schadensbegrenzung ist oberste Pflicht

Einfach die Hände in den Schoß legen und hoffen, dass sich alles irgendwie in Wohlgefallen auflösen werde, ist nicht drin. Machen Sie stets klar, dass Ihr Unternehmen auch bezüglich Folgendem aktiv werden muss:

- So muss es alles unternehmen, um das Schadensereignis, etwa einen Hackerangriff bzw. einen unbefugten Datenzugriff, zu stoppen.

- Es muss den Schaden, so gut es geht, begrenzen, sprich Maßnahmen ergreifen, damit sich der Schaden für Ihr Unternehmen bzw. die Betroffenen nicht weiter ausbreitet.
- Auch geheim gehaltene Datenschutzpannen finden oft irgendwie ihren Weg in die Öffentlichkeit. Wird darüber berichtet und geht Ihr Unternehmen zu locker damit um, riskiert es einen folgenschweren Imageschaden. Und der ist meist verbunden mit erheblichen Umsatzrückgängen.

Gibt es zeitliche Vorgaben für eine Meldung?

Ja, die gibt es! Schauen Sie in Art. 33 Abs. 1 Satz 1 DSGVO, finden Sie dort die grundsätzliche Frist, dass ein relevanter Vorgang „unverzüglich, also ohne schuldhaftes Zögern, und möglichst binnen 72 Stunden“ bei der zuständigen Datenschutzaufsichtsbehörde zu melden ist.

Lässt sich die 72-Stunden-Frist nicht einhalten, ist das noch nicht automatisch ein Problem und muss nicht zu einem Bußgeld führen. Kann die Frist nicht gehalten werden, muss Ihr Unternehmen eine Begründung für die Verspätung beifügen (Art. 33 Abs. 1 Satz 2 DSGVO).

Allerdings darf man den Bogen auch nicht überspannen. Wird beispielsweise erst eine Woche nach dem Bekanntwerden die Datenschutzpanne an die Datenschutzaufsichtsbehörde gemeldet, kann dies als verspätete Meldung auch zu einem Bußgeld führen. Übrigens: Was konkret zu melden bzw. worüber zu informieren ist, ergibt sich aus Art. 33 Abs. 3 und 34 Abs. 2 DSGVO.

Welche Rolle spielen Sie als Datenschutzbeauftragter?

Sie als Datenschutzbeauftragter nehmen bei Datenpannen bzw. ggf. erforderlichen Meldungen die Ihnen zugewiesenen gesetzlichen Aufgaben wahr. Und die ergeben sich in erster Linie aus Art. 39 Abs. 1 DSGVO. Kurz und knapp gilt: Sie beraten und kontrollieren die Einhaltung der Anforderungen. Das machen Sie in fachlicher Hinsicht unabhängig und weisungsfrei. Was bei einer Panne unternommen wird bzw. ob eine Meldung an die Aufsicht erfolgt oder Betroffene informiert werden, obliegt der Entscheidung des Verantwortlichen. Diese Entscheidungen sind Teil der Umsetzungsverantwortung.

DATENPANNEN ERKENNEN: AUF DIE BESCHÄFTIGTEN KOMMT ES AN

Bei Datenpannen, Datenlecks oder einfach dann, wenn etwas bei der Arbeit mit personenbezogenen Daten schiefgeht, muss vor allem eines passieren: Es muss sofort gehandelt werden. Nur so kann Schaden verhindert oder zumindest begrenzt werden. Damit alles Nötige schnell veranlasst werden kann, muss ruckzuck gemeldet werden. Und hier sind die Beschäftigten der entscheidende Faktor.

Einfach entscheidend: die Awareness der Beschäftigten

Klar ist: Zwar können technische Systeme gerade bei Angriffen von Cyberkriminellen, ungewöhnlichen Aktivitäten oder Datenpannen Alarm schlagen. Doch keine Technik ist unfehlbar. Und daher kommt es oft auf den einzelnen Beschäftigten und darauf an, dass diesem etwas auffällt oder komisch vorkommt. Gerade das „Bauchgefühl" können weder Technik noch künstliche Intelligenz ersetzen. Awareness ist also das A und O.

Gehen Sie mehrstufig vor

Wichtig ist, dass alle im Unternehmen erreicht werden und niemand durchs Raster fällt. Daher sollten Sie überlegen, wie Sie auf allen Ebenen für die nötige Sensibilität sorgen können. Hier bietet es sich an, dass Sie mehrstufig vorgehen:

- **Stufe 1: Sie sensibilisieren die Führungskräfte.** Weil Führungskräfte für Beschäftigte, aber auch für Verarbeitungen Verantwortung tragen, müssen diese Bescheid wissen. Ihnen muss klar sein, dass sie Pannen nicht unter den Teppich kehren dürfen. Auch Hinweise von Beschäftigten dürfen bei ihnen nicht versanden.
- **Stufe 2: Sie sorgen für Awareness bei allen Beschäftigten.** Informieren Sie beispielsweise mit einer E-Mail darüber, worauf es ankommt. Hierzu können Sie auf das folgende Muster setzen. Flankierend kann auch eine Arbeitsanweisung sinnvoll sein, damit die Pflichten klar sind und die eigene Verantwortung nicht ignoriert werden kann.
- **Stufe 3: Sie bauen das Thema in Ihre Beratung und Kontrollen ein.** Verdeutlichen Sie, dass schnelles Reagieren auf Vorfälle nur durch zeitnahes Melden möglich wird. Bei Kontrollen können Sie das Vorgehen im Fall der Fälle prüfen. So können Sie leicht identifizieren, ob es in Sachen Awareness noch hapert.

Muster: Mitarbeiterinformation „Vorfälle melden“ Datenpannen, -lecks & Co. – Ihre schnelle Meldung ist entscheidend

Liebe Mitarbeiterin, lieber Mitarbeiter,

bei Ihrer Arbeit haben Sie mehr oder weniger viel mit personenbezogenen Daten zu tun. Kommt es bei der Arbeit mit solchen Daten zu Pannen oder Patzern, dürfen Sie nicht wegschauen und den Kopf in den Sand stecken. Nicht anders ist es, wenn etwa Hacker oder Cyberkriminelle am Werk sind.

Warum müssen gerade Sie tätig werden?

Das ist ganz einfach: Sie arbeiten an „vorderster Front“ und sind die Augen und Ohren des Unternehmens. Zwar nutzen wir einige Tools, um etwa Unregelmäßigkeiten in unseren Systemen und Netzwerken zu erkennen. Doch Sie sind besser als jede Technik. Schon Ihr Bauchgefühl kann Sie ahnen lassen, dass etwas nicht stimmt.

Geben Sie die entscheidenden Tipps

Wird mit personenbezogenen Daten gearbeitet, kann auch mal etwas schiefgehen. Das ist zwar nicht gut und sollte nicht passieren. Aber Menschen machen nun mal Fehler. Wird etwa gegen Regeln verstoßen, egal ob absichtlich oder aus Versehen bzw. Unkenntnis, sollten Sie nicht zögern und

zum Telefon greifen. Informieren Sie sofort den Datenschutzbeauftragten oder die IT-Hotline. Auch wenn Ihnen Dinge seltsam oder verdächtig vorkommen, sollten Sie nicht abwarten. Nehmen Sie sich ein Herz und greifen Sie zum Telefon oder schicken Sie eine E-Mail.

In diesen Fällen müssen Sie handeln!

Alles Schützenswerte, etwa personenbezogene Daten oder Geschäftsgeheimnisse, verdienen angemessenen Schutz. Ist dieser in Gefahr, sollten Sie sofort aktiv werden. So z. B., wenn Sie

- glauben, dass Unbefugte auf Daten zugreifen oder es zu einem Angriff von Cyberkriminellen gekommen oder dieser im Gange ist. Hier ist das Risiko nämlich groß, dass Daten in falsche Hände geraten;
- feststellen, dass Daten oder Dateien und Ordner nicht verfügbar, erreichbar bzw. verschlüsselt sind. Auch ungewöhnliche und unbekannte Dateiformate sollten Sie stutzig machen;
- bemerken, dass Systeme, Datenbanken, Computer oder Dateiablagen ungewöhnlich reagieren;
- Unzulänglichkeiten oder Fehler bei Konfigurationen von Systemen erkennen;
- Opfer einer Phishing-E-Mail oder eines Social-Engineering-Angriffs werden sollten oder wahrscheinlich geworden sind;
- feststellen, dass Schützenswertes entwendet, unerlaubt kopiert, gelöscht oder verändert wurde;
- Ihnen auffällt, dass Informationen falsch weitergeleitet wurden, etwa an falsche Empfänger oder eine unpassende Empfängergruppe (z. B. offener E-Mail-Verteiler), und/oder
- bemerken, dass Computer, Smartphones oder sonstige Datenträger gestohlen wurden oder sonst wie abhandengekommen sind.

Melden Sie schnellstens!

Liegt ein entsprechender Fall vor oder haben Sie auch nur einen diesbezüglichen Verdacht, ist Handeln oberste Pflicht. Informieren Sie den Datenschutzbeauftragten oder die IT-Hotline. Die Eile hat ihren Grund: Einerseits müssen wir aktiv werden, um Schaden zu vermeiden. Andererseits muss das Unternehmen manche Vorfälle unverzüglich und binnen weniger Stunden den Behörden melden.

Danke für Ihre Unterstützung!

WENN'S PASSIERT IST: SO ARBEITEN SIE PANNE, LECK & CO. AB

Wird mit personenbezogenen Daten gearbeitet, kann auch dann etwas schiefgehen, wenn auf den ersten Blick gerade das ausgeschlossen sein sollte. Schließlich gibt es immer den Faktor Mensch und damit auch das Risiko, dass – aus welchen Gründen auch immer – ein Fehler passiert. Wie dem auch sei: Gehen die Dinge schief, heißt es professionell vorgehen.

Ganz wichtig: Eile mit Weile

Kommt es zu einer Datenpanne, ist eines meist garantiert: Die Sache schockiert, und zwar auch diejenigen, die nicht direkt involviert sind, etwa die Unternehmensleitung oder auch Sie als Datenschutzbeauftragten. Umso wichtiger ist, dass Sie sich und andere beruhigen und einen kühlen Kopf bewahren. Denn klar ist: Panik ist kein guter Berater. Zu leicht werden falsche Entscheidungen getroffen, die unter Umständen die Dinge nur noch schlimmer machen. Besser ist es, wenn Sie die Weisheit „Eile mit Weile" beherzigen. Zügig arbeiten und entscheiden ist wichtig und richtig, die Dinge zu überstürzen oder Entscheidungen überhastet zu treffen, jedoch nicht.

Bringen Sie Ihr Wissen auf Zack

Als Datenschutzbeauftragter sind Sie bei einer Datenpanne einer der wichtigsten Ansprechpartner. Um im Fall der Fälle leichter die Ruhe bewahren zu können, sollten Sie die Rahmenbedingungen kennen. Dazu sollten Sie nicht nur die einschlägigen Artikel in der Datenschutz-Grundverordnung (DSGVO) parat haben, nämlich Art. 33, 34, 4 Nr. 12 DSGVO. Werfen Sie auch einen Blick in Gesetzeskommentare zur DSGVO. Schließlich lassen sich manche Aspekte unterschiedlich interpretieren. Auch der Blick auf Hinweise der zuständigen Datenschutzaufsichtsbehörde oder einen vorgegebenen Meldeprozess ist wichtig.

Auf die Zusammenarbeit kommt es an

Im Falle einer Datenpanne müssen viele Dinge berücksichtigt, Fragen geklärt oder nächste Schritte diskutiert werden. Oft betrifft dies auch Bereiche, in denen Ihnen die nötigen Informationen oder Kenntnisse fehlen.

Gibt es kein festgelegtes Verfahren für Datenschutzvorfälle oder -pannen, muss dennoch schlagkräftig reagiert werden. Es bedarf eines Teams oder einer „Task Force“, die sich des Problems annimmt und gemeinsam an einer Lösung arbeitet. In dieser Arbeitsgruppe sollten vertreten sein:

- Mitglieder der Unternehmensleitung
- für die betreffenden Daten oder die betroffene Verarbeitung zuständige bzw. verantwortliche Ansprechpartner
- Spezialisten aus der IT-Abteilung oder von extern
- Kollegen aus der Rechts- und/oder Complianceabteilung
- Kollegen aus der internen bzw. externen Unternehmenskommunikation
- Datenschutzbeauftragter

Behalten Sie das Wichtige im Blick

Bei Datenpannen bleibt keine Zeit für endlose Diskussionen. Das pragmatische und schnelle Lösen des Problems muss im Vordergrund stehen. So muss nicht nur dafür gesorgt werden, dass das Schadensereignis gestoppt und weiterer Schaden vermieden wird. Achten Sie bei Besprechungen darauf, dass es in erster Linie nicht zur Suche nach den Schuldigen kommt, das heißt, für ein „Schwarze-Peter-Spiel“ ist keine Zeit. Jetzt müssen die erforderlichen Maßnahmen beschlossen und in die Wege geleitet werden. Stellen Sie fest, dass man die wichtigen Dinge aus dem Fokus verliert, sollten Sie die Beteiligten zur sachorientierten Arbeit auffordern. Gerade als „unabhängige Instanz“ im Unternehmen können Sie als Datenschutzbeauftragter viel zu einer effizienten Bewältigung der aktuellen Datenpanne beitragen.

Beugen Sie Missverständnissen vor

„Ah, eine Datenpanne. Das ist doch Sache des Datenschutzbeauftragten!“ So oder so ähnlich denkt vielleicht auch mancher in Ihrem Unternehmen, wenn es darum geht, sich um die Panne zu kümmern. Und vielleicht meint man, dass Sie im Alleingang die damit einhergehenden Probleme lösen würden. Hier sollten Sie direkt klarmachen: Sie können im Zusammenhang mit der Datenschutzpanne beratend unterstützen. Auch können Sie mit Ihrer Expertise etwa bei der Beantwortung der Frage helfen, ob ein Vorfall gegenüber der Datenschutzaufsichtsbehörde nach Art. 33 DSGVO zu melden oder Betroffene über den Vorfall zu informieren sind (Art. 34 DSGVO).

Das Treffen der nötigen Entscheidungen ist und bleibt Sache des Verantwortlichen, sprich schlussendlich der Unternehmensleitung.

Lassen Sie nichts durchrutschen

Datenschutzpannen sind vielschichtig und herausfordernd. Und weil alles zügig passieren muss, kann es hektisch und unübersichtlich werden. Damit Sie keinen wichtigen Aspekt übersehen und Ihnen kein relevanter Punkt durchrutscht, können Sie auf der folgenden Checkliste aufbauen:

Checkliste: Prüfpunkte bei Datenschutzpannen

Prüfpunkt	Erläuterung	✔
Klärung von Sachverhalt und Umständen		
Was hat sich zugetragen?	Lassen Sie sich möglichst konkret beschreiben, was passiert ist. Wichtig ist hier, dass Sie zunächst nur zuhören und etwa durch Verständnisfragen den Sachverhalt tiefer erfassen.	○
Wer hat die Sache wann und wie bemerkt?	Diese Information kann wichtig sein, um das mögliche Ausmaß einer Datenschutzpanne besser einordnen zu können. Auch können so Rückfragen erleichtert werden.	○
Welche Daten sind betroffen?	Sprechen Sie allgemein von Daten, um das ganze Bild zu bekommen. Bewerten Sie erst später, ob es sich um personenbezogene Daten handelt. Dabei gilt: Nicht nur personenbezogene Daten sind schützenswert.	○
Um wessen Daten handelt es sich?	Dies kann Aufschluss darüber geben, woher die Daten stammen und wie schutzwürdig eine Personengruppe ist. Denken Sie etwa an Kinder.	○
Wie hoch ist der Schutzbedarf der betroffenen Daten?	Je sensibler Daten sind, desto brisanter ist der Vorfall. Entsprechend muss schnell bzw. entschlossen gehandelt werden. Klären Sie insbesondere, ob etwa besondere Datenkategorien, Anmeldeinformationen oder Bankverbindungsdaten betroffen sind.	○
Welches Ausmaß hat der Vorfall?	Hier geht es um die Zahl der Betroffenen bzw. die Datenmenge. Die Tragweite kann die zu ergreifenden Maßnahmen erheblich beeinflussen.	○
Welche Verarbeitungen sind betroffen?	Prüfen Sie, um welche Verarbeitungen es geht. Manchmal umfassen Datenpannen auch mehrere Verarbeitungsprozesse.	○

Wer ist an den Verarbeitungen beteiligt?	Denken Sie hier insbesondere an andere Unternehmen, auch innerhalb und außerhalb eines Konzerns. Daneben dürfen Auftragsverarbeiter bzw. Dritte nicht vergessen werden.	○
Welche technischen und organisatorischen Schutzmaßnahmen sind umgesetzt?	Klären Sie, wie die Sicherheit der Verarbeitung gewährleistet wurde (Art. 32 DSGVO) und welche Maßnahmen auf den ersten Blick wohl nicht ausreichten oder überwunden wurden.	○
Was ist im Verzeichnis von Verarbeitungstätigkeiten enthalten?	Werfen Sie einen Blick in das Verzeichnis. Dort können wertvolle Informationen rund um die betreffende Verarbeitung enthalten sein.	○
Wurde das Schadensereignis beendet?	Das Schadensereignis muss gestoppt werden. Wichtigster Akteur ist hier meist die IT-Abteilung. Diese muss schnellstens eingebunden werden.	○
Wurden Beweise gesichert?	Das kann wichtig sein, um etwa später eine Strafverfolgung zu ermöglichen bzw. Schadensersatz oder Versicherungsleistungen geltend zu machen.	○
Information und Abstimmung		
Wurden relevante Stellen ausgemacht, informiert und eingebunden?	Denken Sie hier nicht nur an die Unternehmensleitung und die IT-Abteilung. Je nach Vorfall können Fachabteilungen einzubinden sein. Weitere wichtige Stelle: die Unternehmenskommunikation bzw. Pressestelle.	○
Sind andere Stellen außerhalb des Unternehmens zu informieren?	Hier lohnt der Blick in relevante Verträge und Vereinbarungen. Selbst bei Daten ohne Personenbezug kann über Zwischenfälle oder Pannen zu informieren sein. Eventuell gelten hier auch Fristen.	○
Wird die Bewertung der Situation gemeinsam durchgeführt?	Verschiedene Meinungen oder Überlegungen sind bei der Lösungsfindung wichtig. Dadurch fließen wichtige Aspekte, Standpunkte und Sichtweisen ein. Das kann auch vor Fehlentscheidungen schützen.	○
Sind beabsichtigte (Erst-)Maßnahmen abgestimmt?	Hier sollten vorgesehene Maßnahmen mit denen besprochen werden, die betroffen sind. Nur so lassen sich die Auswirkungen in der Praxis ausmachen.	○
Bewertung der datenschutzrechtlichen Situation		
Inwieweit bestehen Gefahren für die Betroffenen?	Machen Sie mit anderen Stellen, etwa der IT-Abteilung, aus, welche Gefahren drohen können. Einige typische Gefahren finden Sie in Erwägungsgrund 85 zur DSGVO.	○

Welche Risiken lassen sich aus den Gefahren ableiten?	Die Gefahr müssen Sie hinsichtlich Schadenshöhe und Eintrittswahrscheinlichkeit bewerten. Auf die Schnelle können Sie Werte vergeben, etwa 1 für niedrig, 2 für mittel, 3 für hoch. Durch Multiplizieren ergibt sich eine Risikozahl, die das Einordnen des Risikos erleichtert.	○
Wer ergreift welche Gegenmaßnahmen?	Lassen Sie sich erläutern, welche Gegenmaßnahmen schon ergriffen wurden oder zu ergreifen sind, damit die Risiken bestmöglich reduziert werden.	○
Feststellung der Meldepflicht gegenüber der Datenschutzaufsicht		
Besteht ein Risiko für die Rechte und Freiheiten natürlicher Personen?	Ergibt die Einordnung der Risiken, dass kein bzw. nur ein geringes Risiko besteht, scheidet die Meldepflicht aus. Andernfalls muss Ihr Unternehmen den Vorfall melden.	○
Wurde eine Meldung an die Datenschutzaufsichtsbehörde vorbereitet bzw. durchgeführt?	Besprechen Sie, inwieweit man hier aktiv geworden ist. Ist das noch offen, unterstützen Sie beratend bei der Umsetzung der Meldepflicht.	○
Erfolgt die Meldung rechtzeitig und ordnungsgemäß?	Nehmen Sie Art. 33 Abs. 3 DSGVO zur Hand. Dort finden Sie eine Übersicht, welche Informationen in der Meldung zumindest enthalten sein müssen. Denken Sie auch an die 72-Stunden-Frist bzw. eine Begründung, wenn diese nicht eingehalten werden kann.	○
Beurteilung der Benachrichtigungspflicht gegenüber Betroffenen		
Liegt ein voraussichtlich hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen vor?	Ergibt sich, dass durch die Datenschutzpanne zum Ereigniszeitpunkt ein voraussichtlich hohes Risiko existiert, muss Ihr Unternehmen die Betroffenen unverzüglich benachrichtigen.	○
Kann eine Benachrichtigung der Betroffenen unterbleiben?	Prüfen Sie, ob etwa ein Fall des Art. 34 Abs. 3 DSGVO gegeben und eine Benachrichtigung nicht mehr erforderlich ist. So z. B. wenn das hohe Risiko durch nachträgliche Gegenmaßnahmen nicht mehr besteht.	○

Erfolgt eine unverzügliche Benachrichtigung der betroffenen Personen?	Ist ein hohes Risiko anzunehmen, muss eine Benachrichtigung erfolgen. Der Inhalt ergibt sich aus Art. 34 Abs. 2 in Verbindung mit Art. 33 Abs. 3 Buchst. b, c und d DSGVO. Beteiligen Sie unbedingt die Unternehmensleitung und die Pressestelle bei der Umsetzung!	○
Dokumentation des Vorfalls		
Sind die Datenpanne und alle diesbezüglichen Aktivitäten dokumentiert?	Beachten Sie, dass unabhängig von einer Melde- oder Benachrichtigungspflicht jede Datenpanne dokumentiert werden muss (Art. 33 Abs. 5 DSGVO). Das ist generell Sache des Unternehmens.	○
Werden Entscheidungen, Erwägungen und Beweggründe festgehalten?	Insbesondere für eine spätere Nachvollziehbarkeit sollten Entscheidungen und der Weg dorthin schriftlich dokumentiert werden.	○
Ist die Beratung als Datenschutzbeauftragter belegbar?	Wichtig ist, dass Sie auch später noch zeigen können, dass und wie Sie beraten haben. Dann kann man Ihnen danach keine Vorwürfe machen.	○

Impressum:

PRIVACYXPERTS

PrivacyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, D-53177 Bonn; Großkundenpostleitzahl: D-53095 Bonn; Handelsregister: HRB 8165, Registergericht: Amtsgericht Bonn, Vertreten durch den Vorstand: Richard Rentrop, ISSN: 1614 – 5674; Kontakt: Telefon: 0228 – 9 55 01 60 (Kundendienst); Telefax: 0228 –– 3 69 64 80, E-Mail: kundendienst@privacyxperts.de, Internet: https://www.privacyxperts.de, Umsatzsteuer: Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372, V.i.S.d.P.: Michael Jodda; Theodor-Heuss-Straße 2–4; D-53177 Bonn, Herausgeber: Michael Jodda, Bonn, Autor: Andreas Würtz, Freiberg am Neckar, Produktmanagement: Lisa Greiling, Bonn, Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen,
Bildrechte S. 1: VZ_Art, S. 5 thataroth, S. 8 La Famiglia – alle Adobe.Stock.com,
Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim
Erscheinungsweise: 16 mal im Jahr; im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. Alle Angaben in Privacy@Work wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden. Dieses Produkt besteht aus FSC®-zertifiziertem Papier.