**Datenschutz**

# Umgang mit Datenschutzverletzungen

Die in Artikel 33 und Artikel 34 DSGVO enthaltenen Melde- bzw. Benachrichtigungspflichten sind Teil eines umfassenden Konzeptes aktiver und passiver Transparenzpflichten. Die Praxisrelevanz dieser Bestimmungen wird anhand der von den Datenschutzaufsichtsbehörden des Bundes und der Länder veröffentlichten Statistiken eindrücklich belegt. Der folgende Beitrag widmet sich praxisrelevanten Fragen und gibt Lösungsvorschläge im Zusammenhang mit der Behandlung von Datenschutzverletzungen.

Die Berliner Beauftragte für den Datenschutz weist in ihrem Tätigkeitsbericht für 2021 insgesamt 1163 gemeldete Datenschutzverletzungen aus, 238 Meldungen mehr als ein Jahr zuvor. Der Hessische Beauftragte für Datenschutz gibt in seinem Tätigkeitsbericht für 2021 über 2016 Meldungen an, gegenüber 1433 Meldungen im Vorjahr. In Baden-Württemberg wurde ein Rekordwert von 3136 gemeldeten Vorfällen erreicht, 815 Fälle mehr als im Jahr 2020. Verantwortliche in Niedersachsen meldeten im vergangenen Jahr 1673 Datenschutzverletzungen. 2020 waren es noch 989, 2019 insgesamt 824.

Die denkbaren Sicherheitsverletzungen bzw. deren Entstehen können dabei vielfältige Ursachen haben. Dritte können von außen auf die IT-Strukturen einwirken und grundsätzlich gesicherte IT-Systeme kompromittieren, Daten können offen einsehbar auf einem ungesicherten IT-System liegen und durch Fehlverhaltensweisen einzelner Beschäftigter (vorsätzlich oder fahrlässig) veröffentlicht werden.

Zur Abwendung bzw. Begrenzung von reputativen und finanziellen Risiken ist es in jedem Fall notwendig, dass Verfahrensweisen zur Erkennung und Behandlung von Sicherheitsverletzungen in Form eines Data-Breach-Managements vorhanden sind.

## Wann und was ist zu melden?

Die Meldepflicht aus Art. 33 DSGVO wird grundsätzlich bei jeder Verletzung der Sicherheit ausgelöst, sofern diese zu einer Vernichtung, Veränderung, einer unbefugten Offenlegung von personenbezogenen Daten oder zum unbefugten Zugang zu solchen Daten führt (im Folgenden auch als Datenschutzverletzung bezeichnet). Im Zusammenhang mit Ransomware-Angriffen stellt sich jedoch bereits hier häufig die Frage, ob eine absolute Gewissheit einer unbefugten Kenntnisnahme verlangt werden kann oder ob bereits die reine Möglichkeit der Kenntnisnahme ausreicht. Nachdem beispielsweise im Frühjahr 2021 bekannt wurde, dass eine Sicherheitslücke bei lokal betriebenen Exchange- Servern durch Hackergruppen massenhaft ausgenutzt wurde, vertraten jedenfalls einige Aufsichtsbehörden die Ansicht, dass eine Meldung bereits im Falle eines nicht rechtzeitig durchgeführten Updates abzugeben ist. Ein offenkundiger „Erfolg“, z. B. in Form einer Verschlüsselung der Daten, war also nicht gefordert.

Eine Ausnahme von der Meldepflicht besteht nach dem Gesetz nur dann, wenn die Sicherheitsverletzung voraussichtlich zu keinem Risiko für die Rechte und Freiheiten natürlicher Personen führt. Diese Regelung ist Ausprägung des risikobasierten Ansatzes der DSGVO, wonach Verantwortliche einige Pflichten nur dann treffen, wenn z. B. ein Risiko oder ein hohes Risiko vorliegt. Abweichend von diesen gesetzlichen Rechtsbegriffen wird >

von den Aufsichtsbehörden mitunter auch eine Meldepflicht bei „geringen Risiken“ verneint.

Voraussetzung hierfür ist aber ebenfalls eine gewisse Wahrscheinlichkeit, die im Rahmen einer Risikoanalyse – neben der Eintrittsschwere – unter Berücksichtigung bekannter Umstände ermittelt werden muss. Die konkreten Grenzen zwischen Möglichkeit und Wahrscheinlichkeit sind dabei oftmals nur schwer zu ziehen. Um den praktischen Nachweis, wann etwas als wahrscheinlich gilt, zu erbringen, hat es sich in der Praxis als hilfreich erwiesen, vorab gewisse Regelbeispiele zu definieren.

Zudem bedarf es einer methodisch nachvollziehbaren Risikoanalyse, die neben den drohenden physischen, materiellen oder immateriellen Schäden auch die Art der Datenschutzverletzung aufgreifen muss: Insoweit hat die Risikoanalyse also auch die Anzahl der Betroffenen, den Umfang der Daten, die Datenkategorien, die Identifizierbarkeit und die Wahrscheinlichkeit des unbefugten Zugriffs Dritter einzubeziehen.

Nach Art. 34 DSGVO sind darüber hinaus die Betroffenen immer dann zu benachrichtigen, wenn die Sicherheitsverletzung voraussichtlich zu einem hohen Risiko für die Betroffenen führt.

Der Mindestinhalt einer Meldung an die zuständige Behörde ergib sich aus Art. 33 Abs. 3 DSGVO. Die Aufsichtsbehörden bieten jedoch mittlerweile vielfach Vordrucke oder Online-Formulare an, deren Inhalte z. T. weit über die gesetzlich geforderten Angaben hinausgehen. Im Hinblick auf eine eventuell bestehende Schutzwirkung gem. §§ 42 Abs. 4, 43 Abs. 4 BDSG stellt die Nutzung dieser Online-Formulare daher nicht immer die beste Strategie dar.

### Einhaltung der Meldefrist

Die Datenschutzverletzung ist durch den Verantwortlichen einer Datenverarbeitung „unverzüglich und möglichst binnen 72 Stunden“ zu melden. Bei der Beurteilung der Frage, ob eine Meldung „unverzüglich“ geschehen ist, sollen die Art und Schwere der Verletzung des Schutzes personenbezogener Daten sowie deren Folgen (die zum Zeitpunkt der Meldung bereits eingetreten sind) und nachteilige Auswirkungen für die betroffene Person berücksichtigt werden. Zusätzlich zu dem Kriterium der „unverzüglichen“ Meldung wird als Leitvorgabe ein 72-Stunden-Zeitraum festgelegt, der grundsätzlich nicht überschritten werden soll. Eine kurze Prüfung des Sachverhalts und die Risikoprognose lassen sich meist sehr zügig durchführen, daher sind bestehende Unsicherheiten in Bezug auf die Frist meist irrelevant. Eine unvollständige Ermittlung des Sachstandes (zumindest in Detailfragen) ist als Begründung für eine Überschreitung der Meldepflicht nicht geeignet, da die Möglichkeit einer stufenweisen Meldung besteht.

Wenn dies aufgrund der Umstände erforderlich ist, z. B. bei komplexen und unübersichtlichen Vorfällen, kann eine Meldung im Einzelfall aber auch später als 72 Stunden erfolgen, dies ist jedoch stichhaltig zu begründen. Zudem sind die fehlenden Angaben unverzüglich nachzureichen, sobald diese vorliegen.

### Meldepflichten von Auftragsverarbeitern

Da der Auftraggeber im Rahmen der Auftragsverarbeitung voll verantwortlich bleibt und dem Auftragsverarbeiter nur die technisch-infrastrukturelle Umsetzung des Verarbeitungsvorgangs obliegt, ist der Auftraggeber im Falle von Sicherheitsverletzungen auf zeitnahe und umfassende Informationen des Auftragsverarbeiters angewiesen. Das Gesetz sieht daher eine Meldepflicht des Auftragsverarbeiters gegenüber dem Verantwortlichen vor.

Diese Verpflichtung sieht keine risikoorientierte Ausnahme vor. Die Beurteilung, ob eine Datenschutzverletzung vorliegt, obliegt ausschließlich dem Auftraggeber. Folglich hat der Auftragsverarbeiter Sicherheitsverletzungen nicht erst dann zu melden, wenn er den Vorfall bereits ausermittelt hat und für ihn feststeht, dass es sich mit Gewissheit um eine Datenschutzverletzung handelt, sondern er hat auch unverzüglich jeden Verdachtsfall einer Sicherheitsverletzung zu melden.

In diesem Kontext stellt sich die Frage, ob sich der Auftraggeber bei der Berechnung der Meldefrist die Kenntnis des Auftragsverarbeiters über eine Sicherheitsverletzung zurechnen lassen muss, oder ob die gesetzliche Meldefrist erst mit Kenntnisnahme des Auftraggebers beginnt. Hierzu bestehen unterschiedliche Auffassungen. Der Auftragsverarbeiter ist jedenfalls gesetzlich verpflichtet, den Verantwortlichen bei der Einhaltung der Meldepflichten gegenüber Behörden und Betroffenen zu unterstützen und hat dazu alle erforderlichen Informationen über Sicherheitsverletzungen unverzüglich an den Verantwortlichen zu übermitteln. Ein Auftragsverarbeiter, der eine Sicherheitsverletzung zunächst intern aufarbeitet und den Auftraggeber erst nach mehreren Tagen oder Wochen informiert, würde nicht nur vertragswidrig handeln, sondern auch gegen ihn selbst betreffende gesetzliche Vorgaben verstoßen und sich damit erheblichen Bußgeldrisiken aussetzen.

Die Kenntnis einer Datenschutzverletzung wird dem Auftraggeber spätestens von dem Zeitpunkt an zugerechnet, an dem ein Mitarbeiter des Auftraggebers durch Information des Auftragsverarbeiters davon erfährt. Es ist daher durch entsprechende Verfahren sicherzustellen, dass sämtliche Mitteilungen des Auftragsverarbeiters immer und unmittelbar auch den für Datenschutzverletzungen intern zuständigen Stellen zugehen.

Bereits bei der Gestaltung des Auftragsverarbeitungsvertrages können geeignete Vorkehrungen getroffen werden, um den o. g. Herausforderungen zu begegnen. Denkbar sind etwa die Festschreibung interner Meldefristen, Klauseln zur Einbeziehung von externen Sicherheitsexperten sowie die ausdrückliche Vereinbarung von Kommunikationswegen.

### Dokumentationspflichten und Lessons learned

Als Ausformung der allgemeinen Rechenschaftspflicht bestimmt Art. 33 Abs. 5 DSGVO eine Dokumentationspflicht bei Sicherheitsverletzungen. Diese Pflicht bezieht sich auch auf Sicherheitsverletzungen, die vom Verantwortlichen als nicht meldepflichtig eingestuft wurden, da diese im Zweifel der Kontrolle durch die Aufsichtsbehörden unterliegen.

Mit der etwaigen Meldung, der Ursachenbehebung und Dokumentation des Vorgangs ist es jedoch noch nicht getan. Die DSGVO verlangt ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen. Die aufgetretenen Defizite sind daher als Anlass zu nehmen, um im Rahmen des geforderten kontinuierlichen Verbesserungsprozesses die Wirksamkeit der Schutzmaßnahmen im betroffenen und in ähnlichen Verarbeitungsverfahren zu prüfen. Unternehmen, die über ein funktionierendes Informationssicherheitsmanagementsystem >

(ISMS) verfügen, können diese Prüfungshandlungen in Abstimmung mit dem Datenschutzbeauftragten in den bereits etablierten Verbesserungsprozess (PDCA) einsteuern. In Unternehmen ohne ISMS kann die Prüfung durch den Datenschutzbeauftragten erfolgen. Dieser hat der Datenschutzverletzung ohnehin Rechnung zu tragen und seinen Prüfplan entsprechend anzupassen.

Auch die bei der Bearbeitung der Sicherheitsverletzung gewonnenen Erkenntnisse über die Angemessenheit und Wirksamkeit der Data-Breach-Management-Prozesse sollten im Rahmen von „Lessons learned" regelmäßig ausgewertet werden, um deren Effektivität messen und verbessern zu können.

### Zu beteiligende Stellen

Unternehmen sollten die Zuständigkeiten und Verfahrensweisen für die Erkennung, Bewertung, Umsetzung von Nachsorgemaßnahmen und die Dokumentation von Datenschutzverletzungen (Data-Breach-Management) als Teil des Gesamtprozesses für das Management von Informationssicherheitsvorfällen festlegen.

Ein Informationssicherheitsvorfall sollte innerhalb der vorhandenen Prozesse und Verfahren demnach immer auch dahingehend bewertet werden, ob es sich dabei um eine Datenschutzverletzung handeln könnte. Darüber hinaus sollte in Anlehnung an erprobte Verfahren aus dem Notfallmanagement für die Bewältigung von Datenschutzverletzungen eine geeignete „Bewältigungsorganisation" in Form eines Teams oder Ausschusses mit verschiedenen Rollen bestimmt werden. Dieses kann je nach Art, Umfang und Schwere der Datenschutzverletzung aktiviert und in unterschiedlicher Konstellation temporär zusammengesetzt werden.

Das Kernteam zur Behandlung der Datenschutzverletzung sollte mindestens aus dem Leiter der betroffenen Organisationseinheit bzw. einem Bereichsverantwortlichen, dem Datenschutz-Referenten (alternativ dem Datenschutzmanager, Datenschutzspezialisten oder Datenschutzkoordinator), einem Vertreter des IT-Betriebs, dem Informationssicherheitsbeauftragten und dem Datenschutzbeauftragten bestehen.

Dem Leiter der betroffenen Organisationseinheit kommt dabei eine zentrale Rolle zu. Ihm obliegt die Risikobewertung ebenso wie die Entscheidung über die Durchführung einer Meldung bei der Aufsichtsbehörde und die Benachrichtigung der Betroffenen. Unterstützt wird er in erster Linie vom Datenschutz-Referenten (in kleineren Unternehmen vom Datenschutzkoordinator, bei Kleinstunternehmen vom Datenschutzbeauftragten). Kommt der Leiter der Organisationseinheit zu dem Bewertungsergebnis, dass voraussichtlich kein Risiko besteht, so hat er dennoch sicherzustellen, dass sämtliche Informationen zum Vorgang dokumentiert und dem Datenschutzbeauftragten zur Verfügung gestellt werden.

Für den Datenschutzbeauftragten sehen weder die DSGVO noch das BDSG Aufgaben im Rahmen der Behandlung von Datenschutzvorfällen vor. Gleichwohl ist es möglich und überdies sinnvoll, den Datenschutzbeauftragten in alle Beratungen und Entscheidungen einzubinden. Dabei ist jedoch zu beachten, dass er gem. Art. 38 Abs. 3 DSGVO stets unabhängig und weisungsfrei agiert. Aufgaben, die zu einem Interessenkonflikt führen könnten, dürfen ihm nicht delegiert werden. Mithin darf ihm die Zuständigkeit für die Umsetzung und Einhaltung datenschutzrechtlicher Vorschriften nicht übertragen werden.

Den Datenschutzbeauftragten mit der Durchführung der Sachverhaltsermittlung und Risikoermittlung zu beauftragen, ist demnach unzulässig. Allenfalls die Aufgabe zur Meldung an die Aufsichtsbehörde kann an ihn delegiert werden (die Entscheidung über die Meldung darf er jedoch nicht selbst treffen). Zulässig ist es zudem, dass der Datenschutzbeauftragte um eine Stellungnahme und Einschätzung zu der vom Leiter der betroffenen Organisationseinheit angefertigten Risikoprognose gebeten wird, da dies Bestandteil seines Beratungsauftrages ist.

Je nach Art und Ausmaß der Datenschutzverletzung können zum Team weitere Stellen hinzugezogen werden. Dazu zählen beispielsweise der Notfallbeauftragte, der Compliance-Officer, der IT-Leiter, das Justitiariat, die Personalabteilung (sofern die Datenschutzverletzung auf das Fehlverhalten eines Beschäftigten zurückgeht), die Presse-/Öffentlichkeitsabteilung (für eine kommunikativ versierte Begleitung) und die Arbeitnehmervertretung (soweit Mitarbeiterdaten betroffen sind).

## Fazit

Bei Datenschutzverletzungen ist besonders schnelles Handeln gefragt.

Bei Verzögerungen drohen hohe finanzielle und reputative Risiken. Unternehmen müssen daher Prozesse zur Behandlung von Datenschutzverletzungen sinnvoll in bestehende Strukturen eingliedern und mit bereits bestehenden Managementsystemen synchronisieren. Soweit etwaige Meldepflichten aus anderen Regulierungen und Normen gelten (zu denken ist hier etwa an das BaFin-Rundschreiben zur Meldung schwerwiegender Zahlungssicherheitsvorfälle, an § 8b Abs. 4 BSIG oder an sonstige zivilrechtliche Meldepflichten), sind sie diese dabei ebenfalls zu berücksichtigen.

Verantwortliche, die es fahrlässig unterlassen, ein Data-Breach-Management (welches auch die Sensibilisierung von Mitarbeitern umfasst) zu implementieren und damit für schnelle Informationswege und kurze Bearbeitungszeiten zu sorgen, müssen sich ein Organisationsverschulden vorwerfen lassen und riskieren die Verwirklichung gleich mehrerer Bußgeldtatbestände.

Sind entsprechende Prozesse einmal vorhanden, kann auch ein im Einzelfall nachlässiger Umgang mit personenbezogenen Daten durch eine sorgfältige und entschlossene Aufarbeitung sowohl der Öffentlichkeit als auch der zuständigen Aufsichtsbehörde gegenüber als singulärer und gleichwohl positiver Vorgang dargestellt werden, welcher zudem den eigenen Kunden zeigt, wie wichtig die Einhaltung des Datenschutzes dem betroffenen Unternehmen ist. ▬

**AUTOR UND ANSPRECHPARTNER**

**Maximilian Schmidt**
Beauftragter Informationssicherheit und Datenschutz
E-Mail: maximilian.schmidt@dz-cp.de