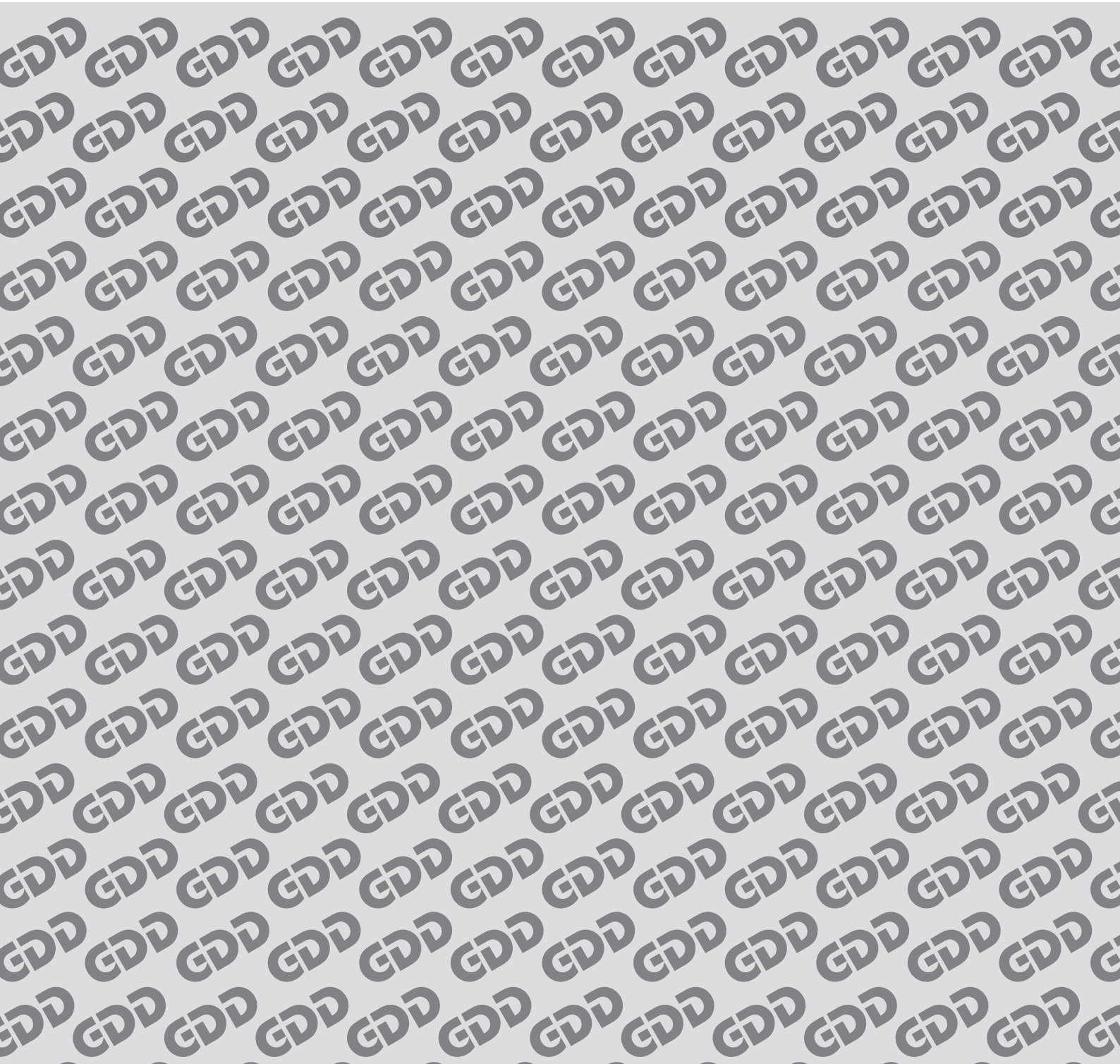
Gesellschaft für Datenschutz
und Datensicherheit e.V.

GDD-Praxisreport 2021

Datenschutzverletzungen



INHALT

Datenschutzverletzungen

Im Rahmen der Konsultation des Europäischen Datenschutzausschusses zu Beispielsfällen einer Datenschutzverletzung[1] hat die GDD eine Umfrage für die Öffentlichkeit initiiert, um einen tieferen Einblick in den Umgang von Datenverarbeitern mit den "Datenpannen" zu erhalten[2].

Die Vielzahl der uns zugetragenen Praxisfälle verdeutlicht, welch große Bedeutung dieser Thematik insbesondere in der unternehmerischen Praxis zukommt. Jüngstes Beispiel der Kontroversen um die Verletzung des Schutzes personenbezogener Daten bilden Schwachstellen von On-Premise-Installationen des E-Mail-Servers Microsoft Exchange. Hier wurden Meldepflichten für Organisationen von Aufsichtsbehörden sehr unterschiedlich beurteilt, was zu einer großen Rechtsunsicherheit bei den datenverarbeitenden Stellen führte.

1 https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2021/guidelines-012021-examples-regarding-data-breach_de
2 https://www.gdd.de/aktuelles/startseite/umfrage-zu-datenschutzvorfaellen-im-unternehmen

Gestaltung der Umfrage und Ergebnisse

Den Schwerpunkt der GDD-Umfrage bildete die Frage nach der konkreten Beschreibung einer Datenschutzverletzung. Um auch den Umgang von Verantwortlichen mit den gesetzlichen Pflichten aus Art. 33 u. 34 DS-GVO insgesamt in Erfahrung zu bringen, wurden weitere Informationen abgefragt.

Die Fragen lauteten wie folgt:

Bitte schildern Sie uns einen Datenschutzvorfall, der Ihnen zu Prüfungszwecken (Melde-/Benachrichtigung-/Dokumentationspflicht) vorgelegt wurde. Beschreiben Sie hierbei auch

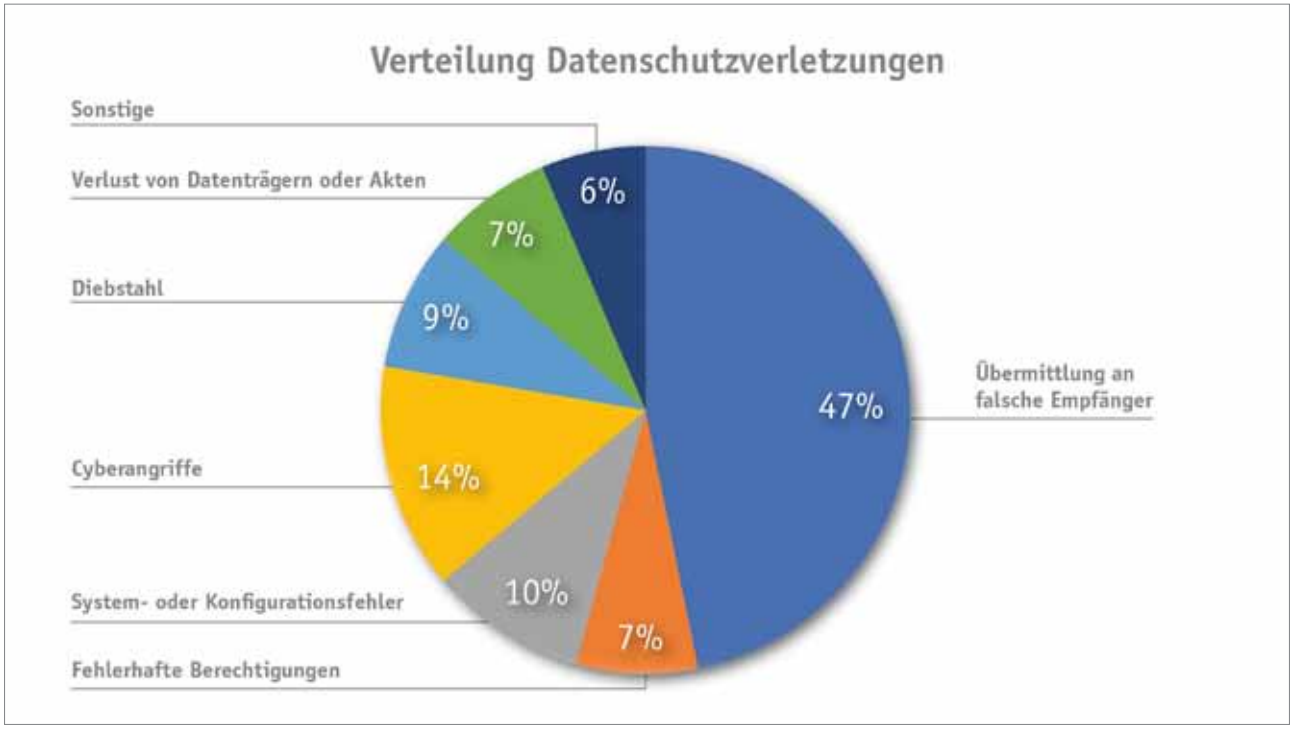
>> die betroffenen Daten und Personen (z.B. Kategorien oder genauere Bezeichnung ohne Personenbezug; z.B. Kontodaten von Beschäftigten, Kunden oder B2B-Kontakten),
>> die Zahl der betroffenen Datensätze (z.B. E-Mail-Verteiler mit 30 Empfängern),
>> ob der Vorfall an die zuständige Aufsichtsbehörde gemeldet wurde und - falls ja - wie schnell nach Kenntniserlangung,
>> ob ein unbefugter Zugriff auf Daten festgestellt werden konnte.

Insgesamt wurden 94 vollständige Beispiele für eine Datenschutzverletzung an die GDD übermittelt. Die berichteten Datenschutzverletzungen lassen sich folgenden Kategorien zuordnen:

>> Übermittlung an falsche Empfänger
>> Cyberangriffe
>> System-/Konfigurationsfehler
>> Diebstahl
>> Verlust von Datenträgern oder Akten

Daneben existieren einzelne Meldungen in der Kategorie "Sonstiges", die sich keiner der obigen Kategorien eindeutig zuordnen lassen, z.B. gezielte Maßnahmen zur unbefugten Verarbeitung personenbezogener Daten auf Veranlassung des Verantwortlichen bzw. einzelner Beschäftigter. Ebenso wurde ein Fall einer versehentlichen Löschung besonderer Kategorien personenbezogener Daten gemeldet, der Anlass für die Meldung einer Datenschutzverletzung war.

Die **prozentuale Verteilung** der gemeldeten Vorfälle gestaltete sich wie folgt (siehe Grafik unten):

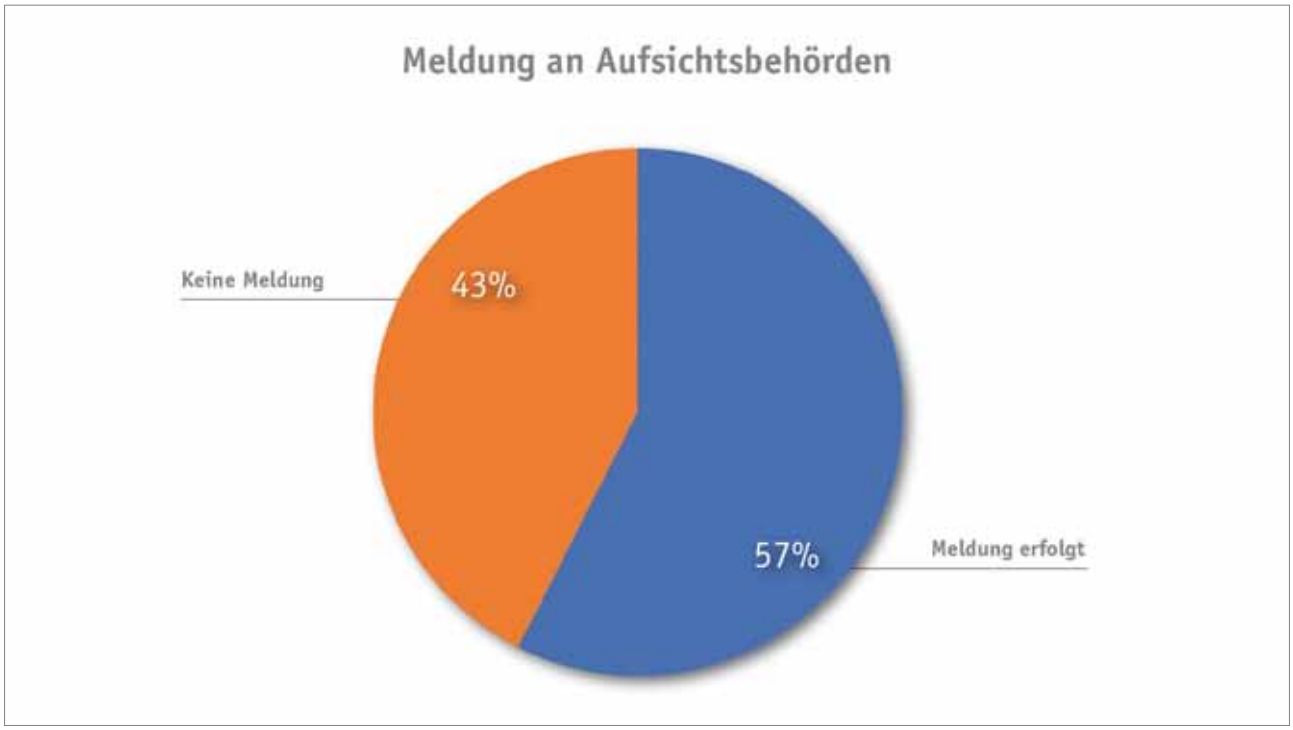


Die **unbeabsichtigte Übermittlung personenbezogener Daten** an falsche Empfänger ist die mit Abstand am häufigsten gemeldete Kategorie (47 %). **Cyberangriffe** gaben ebenfalls einen Anlass für Datenschutzverletzungen (14 %), wobei sich diese nochmals in Unterkategorien einteilen lassen, so bspw. Phishing-, Ransomware- oder andere Attacken zur Umgehung von Zugangsbeschränkungen bzw. Rechteeskalation.

Bei den **System- oder Konfigurationsfehlern (10 %)** wurden entweder fehlerhafte Konfigurationen in Systemen oder Applikationen vorgenommen oder Fehler im Programmcode lösten eine Sicherheitsverletzung aus. In diesen Fällen beruhten die Verletzungen entsprechend auf einem menschlichen Verhalten. Aufgrund der direkten Auswirkungen auf den Schutz personenbezogener Daten werden **fehlerhafte Berechtigungen** als eigene Kategorie geführt, die in Systemen oder Applikationen irrtümlich gesetzt wurden. Die Kategorie **Diebstahl** oder **Verlust** bezog sich im Wesentlichen auf Hardware zur Speicherung personenbezogener Daten (USB-Sticks, externe Festplatten, Smartphones, Laptops), wobei es auch Einzelfälle des Verlustes oder des Diebstahls von Akten gab. Auffällig war, dass hinsichtlich der elektronischen Hardware nur bei drei von sieben der gemeldeten Szenarien eine Verschlüsselung der Datenträger eingesetzt wurde.

Bei den erfassten Kategorien einer Datenschutzverletzung lag die folgende prozentuale Verteilung hinsichtlich ihrer Meldung gegenüber einer Aufsichtsbehörde vor (siehe Grafik unten):

57 % der gemeldeten Sachverhalte wurden an die zuständige Aufsichtsbehörde gemeldet. Ein Vergleich zwischen Sachverhaltsdarstellung und dem Ergebnis der Prüfung der Anforderungen aus Art. 33 DS-GVO zeigt eine bestehende Sensibilisierung der Umfrageteilnehmer/innen hinsichtlich gesetzlicher Meldepflichten. Dies führte jedoch nicht zu einer erweiterten Interpretation von Art. 33 DS-GVO. Diese Erkenntnisse decken sich in Teilen mit einem Vergleich der inneuropäischen Meldebereitschaft ausgewählter Mitgliedstaaten, den die Datenschutzkonföderation CEDPO in ihrer Stellungnahme zu den Beispielsfällen einer Datenschutzverletzung veröffentlicht hat[3]:



3 https://cedpo.eu/wp-content/uploads/20210302-CEDPO_Comments_Gudelines_01-2021.pdf

"A high variation in personal data breach notifications in EU Member States is noticed. Breach notifications in 2020 at several higher population EU countries were as follows:

- Netherlands: 66,257 (388 per 100,000 of country population)
- Germany: 77,747 (93 per 100,000 of country population)
- France: 5,389 (8 per 100,000 of country population)
- Italy: 3,460 (6 per 100,000 of country population)"

Ausgewählte Beispielfälle

Relevante Normen

Art. 33 DS-GVO - 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 Art. 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**. Erfolgt die Meldung an die Aufsichtsbehörde nicht binnen 72 Stunden, so ist ihr eine Begründung für die Verzögerung beizufügen.

(2) Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich.

[…]

Art. 34 DS-GVO - Benachrichtigung der von einer Verletzung des Schutzes personenbezogener Daten betroffenen Person

(1) Hat die Verletzung des Schutzes personenbezogener Daten **voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge**, so benachrichtigt der Verantwortliche die betroffene Person unverzüglich von der Verletzung.

[…]

(3) Die Benachrichtigung der betroffenen Person gemäß Absatz 1 ist nicht erforderlich, wenn eine der folgenden Bedingungen erfüllt ist:

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,

c) 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.

Definitionen

Art. 4 Nr. 12 DS-GVO

Im Sinne dieser Verordnung bezeichnet der Ausdruck:
„Verletzung des Schutzes personenbezogener Daten“ 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.

Beispielfälle

Fall 1: Der verlorene Schlüssel

Sachverhalt
Ein Beschäftigter eines Krankenhauses verliert einen Schlüsselbund. Bei dem Schlüsselbund handelt es sich um einen Gruppenschlüssel mit Transponder, der Zutritt zu verschiedenen Bereichen des Krankenhauses ermöglicht, so auch zum Sekretariat oder zu verschiedenen Ärztezimmern. Dadurch können Unbefugte Zugang zu IT- und Medizintechnik sowie Patientendokumentationen erhalten. Hinweise auf entwendete Unterlagen oder eine Einsichtnahme in Dokumente bestehen für das Krankenhaus nicht.

Nachdem der Verlust bemerkt wird, erfolgt eine unverzügliche Sperrung des Transponders sowie ein Ersetzen des Schließsystems für den Gruppenschlüssel. Patientendokumentationen werden aus den Räumlichkeiten entfernt.

Risikoanalyse
Die Besonderheit in diesem Fall liegt darin, dass zum einen ein Zugangsmittel zu Daten verloren gegangen ist, zum anderen personenbezogene Daten auf dem Zugangsmittel selbst (Transponder) betroffenen sind. Unbefugte können sich mittels des Transponders Zugang zu personenbezogenen Daten verschaffen. Bei den Daten, die eingesehen werden könnten, handelt es sich unter anderen um besondere Kategorien personenbezogener Daten gem. Art. 9 Abs. 1 DS-GVO. Eine Kenntnisnahme von Gesundheitsdaten kann für Betroffene grundsätzlich schwerwiegende Folgen haben. Allerdings fehlen in diesem Fall Anhaltspunkte für einen Verlust von Dokumentationen oder für einen unbefugten Zugriff hierauf.

Aus Sicht des Datenschutzes wäre zunächst eine sorgfältige Analyse eines möglichen Dokumentenverlustes oder einer -einsichtnahme geboten. Hierbei ist zu bedenken, dass Ablichtungen vor Ort erstellt werden können (z.B. über ein Smartphone),

was für die verantwortliche Stelle im Nachhinein nicht nachvollziehbar wäre. Fehlen dem Verantwortlichen nach sorgfältiger Prüfung Hinweise auf einen Verlust oder eine unbefugte Kenntnisnahme, wäre eine rein interne Dokumentation des Vorfalls in diesem Fall grundsätzlich vertretbar. Hierbei wird jedoch auch zu berücksichtigen sein, wie lange der Verlust des Zugangsmittels angedauert hat. Dies ergibt sich aus dem Sachverhalt nicht.

Meldepflicht gem. Art. 33/34 DS-GVO		
Interne Dokumentation gemäß Art. 33 Abs. 5 DS-GVO	Meldung an die Aufsichtsbehörde	Benachrichtigung Betroffene
X		

Fall 2: Unerkanntes GPS-Tracking

Sachverhalt

Bei einem Unternehmen werden 15 Dienstwagen mit GPS-Trackern ausgestattet. Hierdurch ist es der Fuhrparkleitung möglich, Fahrtzeiten und Routen von Beschäftigten während und außerhalb der Arbeitszeit nachzuverfolgen. Beschäftigte haben grundsätzlich die Möglichkeit, das GPS-Tracking abzuschalten, sind jedoch über die vorzunehmenden Einstellungen nicht hinreichend informiert.

Risikoanalyse

Im konkreten Fall können über das GPS-Tracking Fahrerprofile von Beschäftigten innerhalb und außerhalb des Beschäftigungsverhältnisses erstellt werden. Eine Profilbildung ist noch nicht automatisch mit einer Datenschutzverletzung verbunden. Im konkreten Fall ist jedoch der Umstand des Vorliegens eines Beschäftigungsverhältnisses und einer Datenerhebung von Aktivitäten aus dem Privatbereich von Bedeutung. Es droht das Risiko einer Diskriminierung im Beschäftigungsverhältnis sowie eine unbefugte Nachverfolgung privater Fahrten mit dem Dienstwagen. Dass die Maßnahme des Arbeitgebers bewusst herbeigeführt wurde und Zugriffsberechtigungen nicht verletzt wurden, bedarf einer besonderen Würdigung. Ausweislich der gesetzlichen Definition der Datenschutzverletzung, muss zunächst überhaupt eine Sicherheitsverletzung gegeben sein. Ausgangspunkt hierfür bilden die Anforderungen an die IT-Sicherheit aus Art. 32 DS-GVO, wobei in diesem Fall ein Verlust der Vertraulichkeit zu prüfen ist. Personenbezogene Daten von Beschäftigten wurden hier unrechtmäßig verarbeitet, jedoch gemäß intern vorgesehener Zugriffsberechtigungen eingesehen. Ob eine Verletzung unbefugt oder unabsichtlich herbeigeführt wurde, ist für das Vorliegen einer Datenschutzverletzung grundsätzlich irrelevant[4]. Dies führt zum Ergebnis, dass trotz einer planmäßigen Maßnahme des Verantwortlichen eine Meldepflicht gegenüber der Aufsichtsbehörde und der betroffenen Personen anzunehmen ist. Insbesondere der Umstand der Erfassung privater Lebensumstände führt zu einem hohen Risiko für Rechte und Freiheiten Betroffener.

Meldepflicht gem. Art. 33/34 DS-GVO		
Interne Dokumentation gemäß Art. 33 Abs. 5 DS-GVO	Meldung an Aufsichtsbehörde	Benachrichtigung Betroffene
X	X	X

Fall 3: Systemfehler im Schulungstool

Sachverhalt

Ein Unternehmen unterhält ein Schulungstool, das jedem Beschäftigten die Möglichkeit gibt, an Schulungen teilzunehmen und diese zu verwalten. Im Rahmen eines Softwareupdates erhält ein Beschäftigter Zugriff auf die Schulungsdaten eines anderen Mitarbeiters. Zu den Informationen zählen die

4 Vgl. Artikel-29-Datenschutzgruppe, WP 250 S. 7.

teilgenommenen Kurse, geplante Kurse, verschobene Termine sowie der Status der jeweiligen Kurse (erfolgreich teilgenommen bzw. nicht erfolgreich teilgenommen).

Risikoanalyse

Eine Verletzung des Schutzes personenbezogener Daten liegt hier unstreitig vor. Personenbezogene Daten waren durch Unbefugte einsehbar. Damit liegt ein Bruch der Vertraulichkeit vor.

Bei den Daten, die durch einen anderen Beschäftigten einsehbar waren, handelt es sich um keine besonderen Kategorien personenbezogener Daten. Die Daten entstammen aus dem Beschäftigungskontext und geben unter anderem Auskunft über die Leistung eines Beschäftigten im Bereich der Mitarbeiterschulungen. Allerdings sind hier nicht konkrete Punktzahlen offenbart worden, sondern der Umstand einer erfolgreichen oder nicht erfolgreichen Teilnahme. Auch die Information über teilgenommene Kurse ist für Betroffene nicht automatisch mit einem Risiko verbunden. Anhaltspunkte für eine Diskriminierung oder sonstige Benachteiligung am Arbeitsplatz bestehen nicht.

Meldepflicht gem. Art. 33/34 DS-GVO		
Interne Dokumentation gemäß Art. 33 Abs. 5 DS-GVO	Meldung an Aufsichtsbehörde	Benachrichtigung Betroffene
X		

Fall 4: Fehlgeleitete Zielvereinbarungen

Sachverhalt

Aufgrund einer fehlerhaften Berechtigungsvergabe konnten Mitarbeiter eines Teams Zielvereinbarungen, die eine Führungskraft mit Mitarbeitern des Teams geschlossen hatten, einsehen. Die Informationen konnten durch das Aufrufen einer Historie sichtbar gemacht werden.

Risikoanalyse

Die Zielvereinbarungen stellen Abreden zwischen dem Mitarbeiter und jeweiligen Vorgesetzten dar. Diese Vertraulichkeit war durch die Einsichtsmöglichkeit anderer Beschäftigten nicht länger gewahrt. Bei Zielvereinbarungen werden zwischen dem Mitarbeiter und der Führungskraft Ziele individuell vereinbart. Werden Informationen hierzu Beschäftigten desselben Teams offenbart, besteht grundsätzlich das Risiko einer Diskriminierung oder anderer sozialer Nachteile. Gerade weil Ziele und damit verbundene Leistungen von Beschäftigten verglichen bzw. gegenübergestellt werden können, kann in diesem Fall von einem Risiko für Betroffene ausgegangen werden. Durch den Aspekt eines möglichen Leistungsvergleichs im Beschäftigungsverhältnis liegt die Annahme eines hohen Risikos für Freiheiten und Rechte Betroffener nahe.

Meldepflicht gem. Art. 33/34 DS-GVO		
Interne Dokumentation gemäß Art. 33 Abs. 5 DS-GVO	Meldung an Aufsichtsbehörde	Benachrichtigung Betroffene
X	X	X

Fall 5: Der Berechtigungsexzess

Sachverhalt

Personenbezogene Daten zu Beschäftigten eines Unternehmens wurden in einem Netzlaufwerk gespeichert. Bei den Daten handelte es sich, unter anderem, um Protokolle zu Einzelgesprächen mit Mitarbeitern, Listen mit an Corona-Erkrankten einschließlich Kontaktpersonen, Urlaubslisten sowie personenbezogene Krankmeldungen. Die genaue Anzahl der Datensätze sowie ein tatsächlicher Zugriff auf Daten sind nicht bekannt.

Die Zugriffssteuerung auf den Netzwerkordner wurde auf Anweisung geändert und der Zugriff auf die

Daten einem definierten Kreis von Vorgesetzten erlaubt.

Risikoanalyse

Auch wenn konkrete Angaben zu dem erweiterten Kreis der zugriffsberechtigten Personen fehlen, ist das Vorliegen einer Sicherheitsverletzung naheliegend, da personenbezogene Daten nicht mehr für einen ursprünglich vorgesehen Nutzerkreis einsehbar sind und eine Vertraulichkeit der Daten nicht mehr gewahrt ist. Hierbei ist es wiederum unerheblich, ob die Verletzung der Vertraulichkeit unbefugt - wie in diesem Fall - oder unbeabsichtigt erfolgt. Zu den von einer unbefugten Preisgabe betroffenen Daten zählen solche einer besonderen Kategorie gem. Art. 9 Abs. 1 DS-GVO. Die unbefugte Kenntnisnahme dieser Daten kann zu einer Diskriminierung oder anderweitigen Benachteiligung im Beschäftigungsverhältnis führen. Gerade bei Informationen zu Erkrankungen sind z.B. Ächtungen durch Kolleginnen oder Kollegen möglich. Daher ist vorliegend von einem Risiko für Rechte und Freiheiten Betroffener auszugehen, das als hoch einzustufen ist.

Meldepflicht gem. Art. 33/34 DS-GVO		
Interne Dokumentation gemäß Art. 33 Abs. 5 DS-GVO	Meldung an Aufsichtsbehörde	Benachrichtigung Betroffene
X	X	X

Fazit

Verletzungen des Schutzes personenbezogener Daten treten in sehr unterschiedlichen Ausprägungen auf, was hinsichtlich ihres Erkennens und einer sich daran anschließenden Risikobewertung eine vertiefte Kenntnis der rechtlichen Anforderungen voraussetzt. Auf Grundlage der Ergebnisses der GDD-Umfrage bestehen starke Anhaltspunkte, dass sich Verantwortliche für den Datenschutz oder Datenschutzbeauftragte mit einer möglichen Meldepflicht auseinandergesetzt haben. Unklar ist, inwieweit Beschäftigte, als wichtige interne Meldestelle für Datenschutzverletzungen ausreichend geschult und in die unternehmerischen Prozesse eingebunden sind. Dies wird einen wichtigen Teil eines richtigen Umgangs mit den „Datenpannen“ ebenso ausmachen wie die eigentliche Prüfung eines Sachverhalts durch fachkundige Stellen. Die GDD ist weiter bemüht, einen wichtigen Beitrag bei der Rechtsanwendung zu leisten. Sie wird ihren Mitgliedern den Ratgeber zu den Datenpannen in der aktualisierten 3. Auflage im Mai 2021 zur Verfügung stellen.

Gesellschaft für Datenschutz
und Datensicherheit e.V.

Mitglied werden? Mehr Informationen?

https://www.gdd.de/service/mitglied-werden oder eine E-Mail an: info@gdd.de

Eine Mitgliedschaft bietet wesentliche Vorteile:

>> Mitglieder-Nachrichten mit aktuellen Fachinformationen
>> Bezug der Fachzeitschrift RDV (Recht der Datenverarbeitung)
>> Beratung bei konkreten Einzelfragen
>> Zugriff auf Rechtsprechungs- und Literaturarchiv
>> Online-Service „Dataagenda Plus“ (Muster, Checklisten, RDV ONLINE Archiv, Arbeitspapiere etc.)
>> Mitarbeit in Erfahrungsaustausch- und Arbeitskreisen
>> Teilnahme an den kostenfreien GDD-Informationstagen sowie Vergünstigungen bei Seminaren u.v.m.

Schließen Sie sich unseren mehr als 3.800 Mitgliedern an. Eine Mitgliedschaft erhalten Sie schon ab 150,- EUR/Jahr für Privatpersonen und ab 300,- EUR/Jahr für Firmen.

Herausgeber:
Gesellschaft für Datenschutz und Datensicherheit (GDD e.V.)
Heinrich-Böll-Ring 10
53119 Bonn
Tel.: +49 0228 96 96 75-00
Fax: +49 0228 96 96 75-25
www.gdd.de
info@gdd.de
Ansprechpartner: RA Steffen Weiß, LL.M.
Satz: C. Wengenroth, GDD-Geschäftsstelle, Bonn

Stand:
Version 1.0 (April 2021)