konzept17
Datensicherheit trifft Vertraulichkeit

Datenschutz im Arbeitsalltag – Pflichten, Risiken, Praxis

Ihr Datenschutz-Info-Blatt

Ausgabe 06/2026

Liebe Leserin, lieber Leser,

Datenschutz betrifft uns alle – im Arbeitsalltag genauso wie privat. Wer sorgfältig mit personenbezogenen Daten umgeht, schützt nicht nur das Unternehmen, sondern auch Kolleginnen, Kollegen und sich selbst.

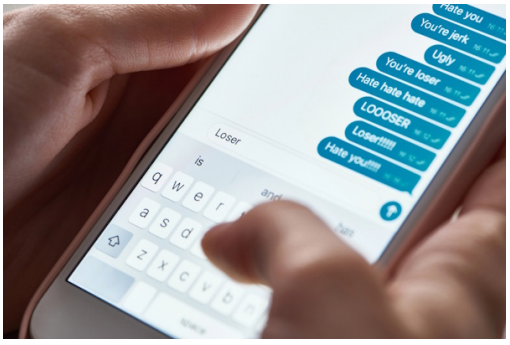
In dieser Ausgabe erfahren Sie, warum Datenschutzvorfälle schnell gemeldet werden müssen und welche Risiken entstehen, wenn Dateien in unzureichend geschützten Ablagen gespeichert werden. Schon kleine Unachtsamkeiten können zu unbefugten Zugriffen oder einer unbeabsichtigten Weitergabe von Daten führen.

Auch das Löschen personenbezogener Daten erfordert Aufmerksamkeit. Fehler kommen in der Praxis häufiger vor, als man denkt – mit möglichen rechtlichen Folgen. Der Beitrag zeigt, worauf es bei datenschutzkonformen Löschungen ankommt.

Außerdem lesen Sie, wie Datenschutzrechte Sie persönlich schützen können – etwa bei digitaler Belästigung im beruflichen oder privaten Umfeld. Datenschutz schafft Sicherheit: für jede und jeden Einzelnen sowie für uns alle.

Ihr Frank Berns, Datenschutzbeauftragter

Warum Datenschutz vor digitaler Belästigung schützen kann



Täglich werden Menschen im Internet beleidigt, belästigt und bedroht. Täter greifen dabei häufig auf konkrete Informationen über ihre Opfer zurück. Wer verantwortungsvoll mit seinen personenbezogenen Daten umgeht, stärkt daher auch den eigenen Schutz vor Cybermobbing und Online-Belästigung.

Persönliche Beleidigungen und gezielte Angriffe

Stellen Sie sich vor, Sie nehmen an einer beruflichen Schulung teil und berichten anschließend in sozialen

Netzwerken darüber. Kurze Zeit später informiert Sie die Plattform über einen neuen Kommentar zu Ihrem Beitrag. Neugierig öffnen Sie die Nachricht – und sind entsetzt: Statt einer harmlosen Reaktion wie „Schön, dass wir uns dort getroffen haben“ oder „Spannende Schulung“ lesen Sie eine persönliche Beleidigung.

Leider handelt es sich nicht um einen Einzelfall. Dieselbe Person hat Sie bereits mehrfach mit bösartigen Kommentaren beleidigt und belästigt. Dennoch erfüllen nicht alle Formen der Online-Belästigung den Tatbestand einer Straftat – auch wenn sie für den Betroffenen äußerst verletzend sind.

Täter missbrauchen Daten für ihre Angriffe

Manche denken, der einfachste Weg bestehe darin, sich vollständig aus dem Internet zurückzuziehen. Doch selbst wer privat nur wenige Informationen preisgibt, muss aus beruflichen Gründen häufig online präsent sein.

Gerade bei beruflichen Online-Profilen sollten Sie daher stets im Blick behalten, dass personenbezogene Daten missbraucht werden können – etwa, um Sie gezielt im Internet zu verfolgen oder bei jeder passenden Gelegenheit zu beleidigen und zu belästigen.

Datenschutz als Mittel gegen digitale Belästigung

Die Landesbeauftragte für den Datenschutz Sachsen-Anhalt hat darauf hingewiesen, dass Datenschutz auch ein wirksames Instrument gegen digitale Belästigungen sein kann. Täter nutzen häufig personenbezogene Daten der Betroffenen ohne deren Einwilligung, um ihre Angriffe persönlicher und damit verletzender zu gestalten.

Datenschutzverstöße liegen beispielsweise vor, wenn jemand ohne rechtliche Grundlage Namen, Adressen oder Bilder einer Person verbreitet oder veröffentlicht. Gleiches gilt, wenn Täter Social-Media-Accounts oder Telefonnummern missbrauchen, um belästigende Nachrichten, Bilder oder Texte zu versenden.

Datenminimierung reduziert die „Angriffsfläche“

Wenn Sie digital belästigt werden und Täter dabei Ihre Daten unzulässig nutzen, können Sie sich an die zuständige Datenschutzaufsichtsbehörde wenden. Gleichzeitig greift im Datenschutz derselbe Grundgedanke wie in der modernen IT-Sicherheit: Die Angriffsfläche sollte so klein wie möglich bleiben.

In der IT-Sicherheit bedeutet dies, ungeschützte Systeme nicht mit dem Internet zu verbinden. Im Datenschutz heißt es, potenziellen Tätern möglichst wenige personenbezogene Daten preiszugeben, die sie für Beleidigungen, Bedrohungen oder andere Angriffe missbrauchen könnten.

Fordert der Datenschutz Datenminimierung, dient dies daher auch dem persönlichen Schutz vor zunehmenden Online-Belästigungen. Dazu gehört beispielsweise, auf mobilen Endgeräten unnötige Funktionen zu deaktivieren – etwa die Standortbestimmung, sofern sie nicht benötigt wird.

Andernfalls können Fotos, die Sie in sozialen Netzwerken veröffentlichen, Standortinformationen enthalten. Täter könnten so nachvollziehen, wo Sie sich aufgehalten haben – selbst dann, wenn Sie in Ihrem Beitrag keinen konkreten Ort genannt haben.

Meldung von Datenpannen – jetzt zählt jede Minute!

Sie haben versehentlich eine E-Mail mit sensiblen Daten an den falschen Empfänger geschickt? Oder bemerken, dass Unbefugte Zugriff auf personenbezogene Daten hatten? Dann gilt: Nicht zögern – sofort melden! Je schneller Sie reagieren, desto besser lassen

sich Schäden begrenzen. Abwarten oder Beschönigen kann aus einer kleinen Panne schnell ein großes Problem machen.

Was Sie sofort tun sollten

- **Melden Sie den Vorfall unverzüglich** an die dafür vorgesehenen Stellen in Ihrem Unternehmen (z.B. IT-Abteilung, Datenschutzkoordination oder Datenschutzbeauftragte).
- **Schildern Sie den Sachverhalt ehrlich und vollständig** , auch wenn es unangenehm ist.
- **Versuchen Sie nicht** , selbst zu beurteilen, ob es sich „nur“ um eine Kleinigkeit handelt.

Wenn Sie unsicher sind, wer zuständig ist: Klären Sie das am besten schon jetzt, nicht erst im Ernstfall. Der oder die Datenschutzbeauftragte hilft Ihnen dabei in jedem Fall weiter.

Warum Eile so wichtig ist

Bei Datenschutzverletzungen läuft die Zeit: Sobald ein Unternehmen eine Datenschutzverletzung erkennt, bleiben nur 72 Stunden für die Meldung an die zuständige Aufsichtsbehörde (Art. 33 Abs. 1 DSGVO). Wochenenden und Feiertage verlängern diese Frist nicht.

Wird diese Frist überschritten, drohen Geldbußen – allein wegen der Verspätung – selbst dann, wenn das Unternehmen insgesamt angemessen reagiert hat und der Schaden gering geblieben ist. Deshalb reagieren Vorgesetzte und Datenschutzbeauftragte in solchen Situationen oft sehr dringlich. Das liegt nicht an ihnen, sondern an der gesetzlichen Vorgabe

Die Fakten müssen vollständig auf den Tisch

Eine pauschale Meldung ohne konkrete Angaben genügt den Aufsichtsbehörden nicht. Sie erwarten die Informationen, die das Gesetz ausdrücklich vorsieht. Dazu zählt eine genaue Darstellung des Vorfalls:

- Was ist genau passiert?
- Wessen Daten wurden an welchen falschen Empfänger übermittelt?
- Wie viele Personen und Datensätze sind betroffen (gegebenenfalls geschätzt)?

Darüber hinaus verlangt die Aufsichtsbehörde eine detaillierte Beschreibung der Maßnahmen, mit denen das Unternehmen die Folgen der Datenpanne begrenzt hat oder begrenzen will.

Keine Sorge: Sie müssen das nicht alles perfekt formulieren. Wichtig ist, dass alle bekannten Fakten auf den Tisch kommen.

All das ist anspruchsvoll – insbesondere angesichts der kurzen 72-Stunden-Frist. Selbst wenn Sie eine Datenpanne sofort gemeldet haben, ist die Arbeit damit nicht erledigt. Erst dann beginnt häufig die detaillierte Aufarbeitung mit zahlenreichen Rückfragen. Das ist mühsam, aber notwendig: Nur so entsteht eine belastbare Grundlage für eine ordnungsgemäße Meldung.

Oft müssen auch betroffene Personen informiert werden

Neben der Meldung an die Datenschutzaufsichtsbehörde besteht oft auch eine Informationspflicht gegenüber den betroffenen Personen. Hat die Datenpanne voraussichtlich spürbare Folgen für die Betroffenen – etwa Risiken für Privatsphäre oder Sicherheit – muss das Unternehmen diese Personen informieren (Art. 34 Abs.1 DSGVO). Das ist keine Bloßstellung, sondern gehört zu einem fairen und verantwortungsvollen Umgang. Gerade kundenorientierte Unternehmen wissen, dass Offenheit Vertrauen schafft. Auch wenn Kunden zunächst verärgert reagieren, bleiben sie dem Unternehmen häufig dennoch treu.

Schnelle Information kann Schäden begrenzen

Datenpannen können Schadensersatzansprüche auslösen. So wurde etwa ein Finanzamt in Sachsen zu 1.000 € Schadensersatz verurteilt, weil es eine Steuererklärung mit zahlreichen sensiblen Angaben – unter anderem zu Krankheiten – versehentlich an eine falsche Person versandt hatte. Solche Risiken sind Unternehmen bewusst.

Entscheidend ist dabei: Wer frühzeitig und möglichst vollständig weiß, was passiert ist, kann angemessen reagieren. Viele betroffene Personen zeigen sich gesprächsbereit, wenn das Unternehmen offen kommuniziert. Eine ehrliche Entschuldigung, möglicherweise verbunden mit einer kleinen Wiedergutmachung, wirkt oft deeskalierend. All das kann Ärger, Vertrauensverlust und Folgekosten deutlich reduzieren.

Ganz anders stellt sich die Lage dar, wenn betroffene Personen den Eindruck gewinnen, das Unternehmen wolle etwas vertuschen. Wird eine Datenpanne der zuständigen Aufsichtsbehörde erst nach Monaten bekannt oder unvollständig gemeldet, schürt das Misstrauen. Gerade solche Situationen führen nicht selten zu Schadensersatzklagen, die andernfalls gar nicht erhoben worden wären.

Lieber einmal zu viel melden als einmal zu spät. Wer eine Datenpanne sofort meldet, handelt richtig – und schützt sich selbst, die betroffenen Personen und das Unternehmen.

Dateiablagen – bequem, aber auch ein Risiko!

„Leg mir das doch bitte auf Laufwerk XY!“ Solche Sätze hört man im Büroalltag häufig. Gemeinsame Dateiablagen erleichtern die Zusammenarbeit – keine Frage. Gleichzeitig bergen sie aber Risiken, die vielen nicht bewusst sind.

Viele haben Zugriff auf dieselben Daten

Ob Austauschverzeichnis, gemeinsames Laufwerk oder Dateiablage – die Bezeichnung variiert. Gemeint ist immer ein zentraler Speicherort im Unternehmen, auf den mehrere Personen zugreifen können. Teilweise gilt der Zugriff sogar für alle Beschäftigten, etwa bei Verzeichnissen mit Telefonnummern oder allgemeinen Informationen. Gerade diese breite Zugänglichkeit macht solche Laufwerke anfällig für Datenschutzprobleme.

Wer darf hier eigentlich was sehen?

Meist tragen gemeinsame Laufwerke schlichte Namen wie „Laufwerk Z“ oder „Laufwerk A“. Für die Technik mag das genügen, für Beschäftigte sagt der Name allerdings wenig aus:

- Welche Daten liegen dort?
- Wer darf sie lesen oder ändern?
- Wer eigentlich nicht?

Beschäftigte, die schon lange im Unternehmen arbeiten, kennen die internen Regeln oft aus Erfahrung. Beispiel: Angebotsentwürfe für ein Projekt werden auf einem bestimmten Laufwerk abgelegt, auf das zwei Teams Zugriff haben. So kann bei Urlaub oder Krankheit weitergearbeitet werden.

Für neue Kolleginnen und Kollegen hingegen bleiben solche Regeln oft undurchsichtig. Genau hier beginnt das Risiko.

Ein häufiger Ausgangspunkt für Datenpannen

Datenschutzaufsichtsbehörden berichten immer wieder, dass auffällig viele Datenpannen mit gemeinsamen Dateiablagen zusammenhängen. Die Gründe sind meist banal.

Ein typisches Beispiel: Für ein Projekt wird ein Laufwerk eingerichtet, Zugriff erhalten nur die Projektbeteiligten. Das Projekt endet – doch das Laufwerk bleibt bestehen. Später nutzt ein anderes Team dasselbe Laufwerk, ohne dass alte Daten gelöscht wurden. Plötzlich haben unbeteiligte Personen Zugriff auf Informationen, die sie gar nicht benötigen. Das stellt einen klaren Datenschutzverstoß dar.

Prüfen Sie die Zugriffsberechtigungen

Wenn Sie mit einem neuen Laufwerk arbeiten, lohnt sich ein kurzer Blick auf die Berechtigungen. Der Bayerische Landesbeauftragte für den Datenschutz hat dafür folgenden Tipp veröffentlicht. Mit ihm lassen sich Berechtigungen für Verzeichnisse (= „Ordner“) bei den meisten Versionen von Microsoft Windows wie folgt überprüfen:

- Öffnen Sie den Datei-Explorer.
- Klicken Sie mit der rechten Maustaste auf den Ordner.
- Wählen Sie „Eigenschaften“ aus (Abb. 1).
- Öffnen Sie den Reiter „Sicherheit“ (Abb. 2).
- Prüfen Sie, welche Gruppen oder Personen Zugriff haben.
- Markieren Sie einen Eintrag, um zu sehen, welche Rechte erlaubt oder verweigert sind.

Kommen Sie damit nicht weiter, sprechen Sie die IT-Abteilung an. Besser einmal zu viel fragen als eine Datenpanne verursachen.

Halten Sie sich auch selbst an die Spielregeln

Viele Unternehmen haben klare Vorgaben für den Umgang mit Dateiablagen – ihr Nutzen hängt davon ab, ob sich alle daran halten. Häufig gilt: Wer Dateien einstellt, ist auch für das rechtzeitige Löschen verantwortlich. Natürlich erst dann, wenn die Daten nicht mehr gebraucht werden. Das funktioniert nur, wenn alle mitdenken und mitarbeiten.

Deshalb gilt auch: Ärgern Sie sich nicht, wenn die IT regelmäßig prüft, welche Dateien seit Langem ungenutzt sind. Nutzen Sie entsprechende Rückfragen lieber als Anlass, selbst wieder einmal aufzuräumen. Gemeinsame Laufwerke sind praktisch – aber nur sicher, wenn Zugriff und Inhalte regelmäßig kontrolliert werden.

Was beim Löschen von Daten zu beachten ist

Das Recht auf Löschung gehört zu den wichtigsten Datenschutzrechten. Trotzdem zeigt die Praxis: Personenbezogene Daten werden oft zu spät, falsch oder gar nicht gelöscht. Eine gemeinsame Prüfaktion der Datenschutzaufsichtsbehörden hat deutlich gemacht, wo die typischen Probleme liegen – und was Beschäftigte dagegen tun können.

Löschen ist wichtig – aber nicht immer einfach

Wer personenbezogene Daten nicht mehr benötigt, muss sie grundsätzlich löschen. So einfach klingt das. In der Realität ist es jedoch komplizierter.

Neben der Pflicht zum Löschen kann es auch eine Pflicht zur Aufbewahrung geben. Typische Beispiele sind Rechnungen oder steuerrelevante Unterlagen, die selbst nach der Zahlung noch mehrere Jahre gespeichert bleiben müssen.

Ein Blick in die Datenschutz-Grundverordnung (Art. 17 DSGVO – „Recht auf Vergessenwerden“) zeigt: Es gibt zahlreiche Gründe, warum Daten nicht sofort nach Zweckerfüllung gelöscht werden dürfen oder müssen. Genau das führt im Arbeitsalltag häufig zu Unsicherheit: Muss ich jetzt schon löschen? Darf ich überhaupt löschen? Und wie lösche ich richtig?

Wissen Sie’s genau, wann personenbezogene Daten gelöscht werden müssen?

Die Antworten finden Sie am Ende des Beitrags.

Frage 1: Werden personenbezogene Daten für den ursprünglichen Zweck nicht mehr benötigt, müssen sie immer sofort gelöscht werden, stimmt das?

1. Nein, die DSGVO nennt mehrere Gründe, wann personenbezogene Daten nicht direkt nach Zweckerfüllung gelöscht werden müssen.
2. Ja, nicht mehr benötigte Daten müssen ohne Ausnahme sofort gelöscht werden.

Frage 2: Es reicht es, Daten über die normale Löschfunktion von Windows oder einer Anwendung zu löschen, ist das richtig?

1. Nein, oft landen die Daten nur im Papierkorb oder bleiben technisch wiederherstellbar.
2. Ja, Betriebssysteme löschen Daten automatisch sicher und endgültig.

Prüfaktion zeigt typische Schwachstellen

Datenschutzaufsichtsbehörden in vielen EU-Staaten haben untersucht, wo es bei der Umsetzung des Löschrechts hakt. Auch in Deutschland zeigten sich immer wieder dieselben Problemstellen:

- Es fehlen **klare interne Regeln**, wann und wie gelöscht wird.
- Beschäftigte kennen diese Regeln oft **nicht oder nur unvollständig**.
- Unsicherheiten bestehen bei **Aufbewahrungsfristen** und **Ausnahmen von der Löschplicht**.
- Schulungen zum Thema Löschen finden **zu selten oder gar nicht** statt.

Wenn Sie beim Lesen denken „Ja, das kenne ich“, behalten Sie diesen Eindruck nicht für sich. Fragen Sie nach. Häufig existieren im Unternehmen bereits Prozesse – nur sind sie nicht allen bekannt.

Richtig Löschen: eine Aufgabe für alle

Damit Datenschutz im Alltag funktioniert, müssen alle im Unternehmen wissen, welche Daten sie löschen dürfen, wann gelöscht werden soll und wie gelöscht werden muss.

Andernfalls passieren typische Fehler: Daten werden zu früh gelöscht, obwohl sie noch aufbewahrt werden müssten. Es wird zwar gelöscht, aber technisch nicht sicher – die Daten bleiben wiederherstellbar. Oder Daten bleiben aus Unsicherheit einfach dauerhaft gespeichert.

Haben Sie Fragen zum Löschen? Zögern Sie nicht und stellen Sie sie. Sie sind damit keineswegs allein. Die Prüfaktion der Aufsichtsbehörden hat gezeigt, dass viele Beschäftigte genau an diesem Punkt unsicher sind.

Richtig löschen heißt: rechtzeitig, begründet und technisch sicher. Nachfragen ist dabei kein Fehler, sondern ein wichtiger Beitrag zum Datenschutz.

Und hier die Auslösung unserer Quizfragen:

Lösung Frage 1: Antwort 1 ist richtig. Die Datenschutz-Grundverordnung nennt mehrere Gründe, die einer sofortigen Löschung entgegenstehen können, zum Beispiel gesetzliche Aufbewahrungspflichten, Archivzwecke im öffentlichen Interesse, wissenschaftliche oder statistische Zwecke. Deshalb gehört zu jedem Löschprozess auch die Prüfung, ob und warum Daten noch aufbewahrt werden dürfen oder müssen.

Lösung Frage 2: Die Antwort 1 ist richtig. Bei vielen Systemen bedeutet „Löschen“ nur, dass der Speicherplatz freigegeben wird. Die Daten sind technisch oft noch vorhanden und mit Spezialsoftware wiederherstellbar. Für sensible personenbezogene Daten sind daher geeignete, sichere Löschverfahren oder -programme erforderlich, die eine Wiederherstellung ausschließen.

Impressum
Redaktion:
Frank Berns, Datenschutzbeauftragter, Geschäftsführer
Anschrift:
Konzept 17 GmbH
Westring 3
24850 Schuby
Amtsgericht Flensburg: HRB 12329
Telefon: +49 4621 5 30 40 50
E-Mail: mail@konzept17.de