www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

Rechtssicher | vollständig | dauerhaft

Februar 2025

Bild: iStock.com/da-kuk

**Der Europäische Datenschutzausschuss legt bei der Definition berechtigter Interessen strenge Maßstäbe an. Dies soll vermeiden, dass die Formulierung zum Auffangbecken für Datenverarbeitungen ohne konkrete Rechtsgrundlage gerät.**

Neue Leitlinien des Europäischen Datenschutzausschusses

# Verarbeitung auf Grundlage berechtigter Interessen

**Mit seinen neuen Leitlinien 1/2024 zur Verarbeitung personenbezogener Daten auf Basis von Art. 6 Abs. 1 Buchst. f DSGVO gibt der EDSA ein Prüfkonzept vor. Damit lässt sich feststellen, ob „berechtigte Interessen" als Rechtsgrundlage für eine Datenverarbeitung in Betracht kommen.**

„Berechtigte Interessen" nach Art. 6 Abs. 1 Buchst. f Datenschutz-Grundverordnung (DSGVO) dienen in der Praxis häufig als Rechtsgrundlage, um personenbezogene Daten zu verarbeiten. Der Europäische Datenschutzausschuss (EDSA) warnt jedoch in den neuen Leitlinien davor, „berechtigte Interessen" als letzte Möglichkeit zu nutzen, um eine Verarbeitung irgendwie zu rechtfertigen, wenn alle anderen Rechtsgrundlagen von Art. 6 DSGVO nicht greifen.

## Umfassende Prüfung erforderlich

Nach Auffassung des EDSA ist Art. 6 Abs. 1 Buchst. f DSGVO weder eine einfach anzuwendende Verarbeitungsgrundlage noch als Auffangbecken gedacht. Vielmehr müssen Verantwortliche eine umfassende Prüfung durchführen, um „berechtigte Interessen" als Rechtsgrundlage nutzen zu können.

Dafür sind nach den Leitlinien drei Prüfschritte erforderlich:

1. rechtmäßiges Interesse des Verantwortlichen
2. Notwendigkeit der Verarbeitung für die legitimen Interessen des Verantwortlichen
3. Interessenabwägung im eigentlichen Sinne


Verarbeiten öffentliche Stellen in Ausübung ihrer zugewiesenen Aufgaben personenbezogene Daten, so ist Art. 6 Abs. 1 Buchst. f DSGVO nach Auffassung des EDSA nicht als Rechtsgrundlage für die Verarbeitung anwendbar. →

Editorial

**Ricarda Veidt, Chefredakteurin**

# 100 € Schadensersatz – nicht viel, oder??

Liebe Leserin, lieber Leser! Haben Sie auch schon des Öfteren den Versuch gewagt, bei Verantwortlichen mit dem Thema „Schadensersatz" für mehr Datenschutz zu werben? Leider ist das eher selten von Erfolg gekrönt. Das Urteil des Bundesgerichtshofs zum Schadensersatz bei Scraping dürfte Ihnen in diesem Punkt für das neue Jahr erheblichen Schub verleihen (S. 6–7).

Dass die Datenschutzaufsicht eine Kontrolle vor Ort durchführen könnte, taugt dagegen kaum noch als Argument, um Überzeugungsarbeit für den Datenschutz zu leisten. Doch trotzdem sollten alle beteiligten Personen wissen, was im Fall der Fälle zu tun ist. Tipps aus der Praxis lesen Sie auf den Seiten 8 bis 11.

Einen guten Ansatzpunkt für Kontrollen würden die Behörden bei vielen Verantwortlichen vermutlich im Hinblick auf die Auskunftspflicht gegenüber Beschäftigten finden. Hand hoch: Wer hat eine spezielle Datenschutzinformation für die Belegschaft? Alle anderen mögen ihren Verantwortlichen die Seiten 14 bis 15 ans Herz legen.

Viel Erfolg im neuen Jahr
Ihre Ricarda Veidt

## Drei Prüfschritte durchführen

Verantwortliche müssen vor der jeweiligen Verarbeitung prüfen, ob „berechtigte Interessen" als Rechtsgrundlage für die beabsichtigte Verarbeitung tragfähig sind. Falls es im Unternehmen einen Datenschutzbeauftragten (DSB) gibt, sollte die verantwortliche Person ihn in die Durchführung der Prüfung einbeziehen.

### Prüfschritt 1: Rechtmäßiges Interesse

Liegt ein rechtmäßiges Interesse vor? Verantwortliche müssen zunächst zwischen dem Interesse und dem Verarbeitungszweck entscheiden. „Interesse" ist dabei der weiter gefasste Begriff. Ein Beispiel zur Verdeutlichung: Der Verantwortliche hat ein Interesse daran, die Produkte, die sein Unternehmen herstellt, zu bewerben. Dieses Interesse setzt das Unternehmen durch den Verarbeitungszweck „Direktmarketing" um.

Damit ein Interesse rechtmäßig ist, muss es folgende Voraussetzungen erfüllen:

- Das Interesse muss **gesetzmäßig** sein. Das heißt, es muss dem Recht der EU oder des Mitgliedstaats entsprechen. Es ist nicht erforderlich, dass das Interesse selbst in einem Gesetz geregelt ist. Es darf nur nicht den vorhandenen Regelungen widersprechen. Ein Negativbeispiel: Geplante Direktwerbung für Tabakprodukte wäre nicht gesetzmäßig, da die entsprechende Richtlinie der EU (2014/40/EU) bzw. die Regelungen der Mitgliedstaaten zur Umsetzung der Richtlinie solche Direktwerbung untersagen.
- Das Interesse muss **klar und eindeutig identifiziert** sein. Ein Negativbeispiel: die Installation einer Videoüberwachung „für Zwecke der Gemeinschaft" im Rahmen einer Nachbarschaftsinitiative. Hier liegt nach Auffassung des EDSA kein klares und eindeutiges Interesse vor.
- Das Interesse muss **echt und bestehend** sein. Rein hypothetische Interessen oder zukünftig mögliche Interessen erfüllen nicht die Anforderungen. Ein Negativbeispiel: Ein Zeitungsverlag möchte Daten früherer Abonnenten zusammenstellen, um für ein neues Magazin auf diese Daten zurückgreifen zu können. Da im Beispiel kein Plan besteht, tatsächlich ein neues Magazin zu veröffentlichen, liegt nach den Leitlinien noch kein echtes und bestehendes Interesse vor.
- Das rechtmäßige Interesse muss **für den Verantwortlichen oder einen Dritten bestehen**. Es muss mit den aktuellen Aktivitäten oder Tätigkeiten zusammenhängen.

### Prüfschritt 2: Notwendigkeit der Verarbeitung

Ist Prüfschritt 1 erfolgreich abgeschlossen, müssen Verantwortliche überprüfen, ob die Verarbeitung personenbezogener Daten notwendig ist, um das gesetzmäßige Interesse zu erreichen. Dabei sind folgende Überlegungen einzubeziehen:

- Rechte und Freiheiten der betroffenen Personen: Lässt sich das gesetzmäßige Interesse mit weniger Eingriffen in Rechte der betroffenen Personen erzielen? Falls ja, besteht keine Notwendigkeit der Verarbeitung!
- DSGVO-Vorgaben: Verantwortliche müssen dabei auch die Prinzipien der DSGVO mit einbeziehen, z.B. das Prinzip der Datenminimierung. Der EuGH

verlangt eine „strenge Notwendigkeit" („strictly necessary") der Verarbeitung, um das identifizierte Interesse zu erreichen (Az. C-26/22 und C-64/22 – Schufa Holding sowie C-252/21 – Meta/Bundeskartellamt). Diese strenge Notwendigkeit lässt sich auch aus Erwägungsgrund Nr. 47 zur DSGVO herauslesen.

Liegt eine solche Notwendigkeit der Verarbeitung vor, müssen Verantwortliche in Schritt 3 die eigentliche Interessenabwägung vornehmen.

**Prüfschritt 3: Interessenabwägung**

In diesem Schritt müssen Verantwortliche im Einzelfall die eigenen Interessen den Interessen der Personen gegenüberstellen, die von der Verarbeitung betroffen sind. Dies dient dazu, letztlich festzustellen, wessen Interesse schwerer wiegt.


Die EDSA-Leitlinien stellen klar: Es geht nicht darum, jegliche Einwirkung auf die Rechte der Betroffenen zu verhindern. Ziel ist es, übermäßige Eingriffe abzuwenden und die Interessen der Beteiligten zueinander in Verhältnis zu setzen.

Die Durchführung der Interessenabwägung lässt sich in mehrere Einzelschritte gliedern. Diese Schritte sind in der Tabelle unten im Überblick dargestellt.

Bei Schritt 2 „Die Einwirkung der beabsichtigten Verarbeitung auf die Betroffenen feststellen" müssen Verantwortliche zusätzlich die folgenden Punkte berücksichtigen.

Wichtig ist zunächst die Art der zu verarbeitenden personenbezogenen Daten. Bei der Verarbeitung besonderer Kategorien personenbezogener Daten sind zum einen die Voraussetzungen von Art. 9 Abs. 2 DSGVO zu beachten. Der EDSA weist darauf hin, dass Daten bereits dann als besonders sensibel zu werten sind, wenn in größeren Datensätzen, die sich nicht aufteilen lassen, ein Datum unter Art. 9 DSGVO fällt. Als Faustregel gilt in diesem Kontext: Je sensibler oder privater Daten sind, desto eher hat die Verarbeitung negative Auswirkungen auf die betroffene Person und desto mehr Gewicht erhalten diese Daten im Rahmen der Interessenabwägung.

## Beispiele für rechtmäßige Interessen

- **Betrug verhindern**
- **einen Onlinezugang zu Informationen erhalten**
- **das dauerhafte Funktionieren einer öffentlich zugänglichen Website sicherstellen**
- **zur Rechtsverfolgung Informationen über eine Person erhalten, die z.B. eine Sachbeschädigung begangen hat**
- **Eigentum, Leben und Gesundheit der Miteigentümer eines Gebäudes schützen**
- **wirtschaftliche Interessen verfolgen**
- **die Kreditwürdigkeit einer Person überprüfen**
- **ein Produkt verbessern**
- **Direktmarketing betreiben**
- **Sicherheit der IT gewährleisten/verbessern**

**Die Beispiele für rechtmäßige Interessen ergeben sich jeweils aus Einzelfällen, über die z.B. der Europäische Gerichtshof (EuGH) zu entscheiden hatte. Es empfiehlt sich für Verantwortliche unbedingt, diese Rechtsprechung im Auge zu behalten.**

| Teilschritt | Erläuterung |
|---|---|
| 1. Die grundlegenden Rechte und Freiheiten der Betroffenen sowie deren Interessen identifizieren. | Zu den Rechten und Freiheiten gehören z.B. Meinungsfreiheit, Eigentumsrechte, Verbot der Diskriminierung sowie das Recht auf Datenschutz. Zu den Interessen der betroffenen Personen, die der Verantwortliche in die Abwägung einbeziehen muss, zählen z.B. finanzielle Interessen und soziale oder persönliche Interessen. Es gehört zu den Aufgaben des Verantwortlichen, die von der beabsichtigten Verarbeitung betroffenen Rechte/Freiheiten und Interessen der betroffenen Personen zu identifizieren. |
| 2. Die Einwirkung der beabsichtigten Verarbeitung auf die Betroffenen feststellen. | Hierbei sind alle Möglichkeiten einer Einwirkung zu berücksichtigen: positive oder negative Auswirkungen, aktuelle oder potenzielle Auswirkungen. |
| 3. Die vernünftigen Erwartungen der Betroffenen einbeziehen. | Das ergibt sich aus Erwägungsgrund Nr. 47 DSGVO. Verantwortliche müssen zunächst die vernünftigen Erwartungen der betroffenen Personen unterscheiden von der üblichen Praxis in bestimmten Wirtschaftsbereichen. |
| 4. Interessen der Beteiligten gewichten. | Die Frage lautet hier: Wessen Interessen wiegen schwerer – die schutzwürdigen Interessen der betroffenen Person oder die Verarbeitungsinteressen des Verantwortlichen? Besondere Vorsicht ist hier geboten, wenn es um personenbezogene Daten von Kindern oder Jugendlichen geht. Da diese als besonders schutzwürdig gelten, wird in vielen Fällen die eigentliche Interessenabwägung zu ihren Gunsten ausfallen. Das bedeutet aber nicht, dass Verantwortliche Daten von Kindern überhaupt nicht verarbeiten können. |

**Die vier Teilschritte der eigentlichen Interessenabwägung**

→

In welchem Zusammenhang die Verarbeitung stattfinden soll, kann ebenfalls Folgen für die Einwirkung haben. Verantwortliche müssen deshalb diese Aspekte einbeziehen:

- Wie groß sind das Maß der Verarbeitung, die Menge der personenbezogenen Daten, z.B. die Datenmengen pro betroffener Person, die Anzahl betroffener Personen?
- In welcher Beziehung steht der Verantwortliche zu den betroffenen Personen? Handelt es sich um z.B. eine Lieferanten-Kunden-Beziehung oder um ein Arbeitgeber-Beschäftigten-Verhältnis?
- Findet eine Zusammenführung der personenbezogenen Daten mit anderen Datensätzen statt?
- Sind die zu verarbeitenden Daten bereits öffentlich verfügbar oder einfach zugänglich?
- Wie steht es um den Status der Betroffenen? Sind Betroffene z.B. besonders schützenswert, wie Kinder oder Jugendliche?

Verantwortliche müssen zudem weitere Konsequenzen der beabsichtigten Verarbeitung berücksichtigen. Zu den möglichen Konsequenzen gehören:

- Gibt es Entscheidungen Dritter, die auf den zu verarbeitenden Daten basieren?
- Entstehen irgendwelche rechtlichen Auswirkungen auf den Betroffenen infolge der Verarbeitung?
- Droht eine Diskriminierung der Betroffenen?
- Könnten Reputation oder Autonomie der Betroffenen leiden?
- Könnten den Betroffenen finanzielle Verluste infolge der Verarbeitung drohen?
- Könnten Betroffene infolge der Verarbeitung von Dienstleistungen, für die es keine Alternative gibt, ausgeschlossen werden?
- Bestehen Risiken für Freiheit, Sicherheit, Gesundheit oder Leben der betroffenen Personen infolge der Verarbeitung?
- Besonders zu berücksichtigen sind Gefühle der betroffenen Personen: Ist der Kontrollverlust über die eigenen Daten zu befürchten oder das Gefühl, dauerhaft unter Beobachtung zu stehen?

**WICHTIG**

***Verantwortliche dürfen hierbei nicht davon ausgehen, dass alle Betroffenen die gleichen Interessen haben. Außerdem müssen sie eine Datenschutz-Folgenabschätzung (DFSA) nach Art. 35 DSGVO durchführen, wenn sie in diesem Prüfschritt hohe Risiken identifizieren.***

Zu Schritt 3 „Vernünftige Erwartungen der betroffenen Personen in die Interessenabwägung einbeziehen" gehört es, folgende Punkte zu bedenken:

- Welchen Charakter haben die Beziehungen zwischen den konkret Betroffenen und dem Verantwortlichen? Handelt es sich z.B. um Kunden oder Nicht-Kunden? Ist der Kunde ein regelmäßiger Käufer der Produkte oder hat eine betroffene Person nur einen Newsletter abonniert? An welchem Ort und in welchem Zusammenhang sollen personenbezogene Daten erhoben werden? Beispiel: Eine betroffene Person wird eine Videoüberwachung eher in einer Bank erwarten als im Fitnessstudio.
- Welche rechtlichen Anforderungen bestehen in der konkreten Situation?
- Welche Erwartungen hätte der oder die durchschnittliche Betroffene? Hier sind das Alter der betroffenen Person, ihre Stellung in der Öffentlichkeit sowie ihr Wissen und Verständnis einzubeziehen.


Eine Druckerei verwendet Fotos, die Betroffene veröffentlicht haben. Mit diesen Bildern gestaltet sie Marketing-Flyer. Trotz der Veröffentlichung der Fotos wird eine betroffene Person vernünftigerweise nicht davon ausgehen, dass Dritte diese Bilder einfach so für geschäftliche Zwecke verwenden.

## Zurück auf „Los"

Es kann sein, dass während des beschriebenen Prüfverfahrens Unklarheiten bestehen, oder dass der Verantwortliche vorsieht, Schutzmaßnahmen einzuführen, die die Verarbeitung begrenzen. Dann sollte dieser den jeweils letzten Prüfschritt, der positiv für den Verantwortlichen ausgefallen ist, wiederholen.

Begrenzende Schutzmaßnahmen sind jedoch keine Maßnahmen, die die DSGVO sowieso vorschreibt. Vielmehr gehen sie darüber hinaus.

## Dokumentationspflichten einhalten

Verantwortliche müssen die Durchführung der einzelnen Prüfschritte und die jeweiligen Ergebnisse der Interessenabwägung entsprechend Art. 5 Abs. 2 DSGVO umfassend dokumentieren. Im Fall eines Falles müssen sie diese der zuständigen Aufsichtsbehörde vorlegen können.

Dabei hilft die Dokumentation aber auch, eine Selbstkontrolle durchzuführen. So lässt sich sicherstellen, dass die Verantwortlichen die Prüfschritte umfassend abgearbeitet haben, die in den Leitlinien vorgegeben sind.

## Zusätzlich gilt: Betroffenenrechte beachten

Selbstverständlich müssen Verantwortliche alle in der Datenschutz-Grundverordnung geregelten Betroffenenrechte beachten. Das gilt auch für die Informationspflichten nach Art. 13, 14 DSGVO.

Diese Pflichten umfassen u.a. die Information über die Rechtsgrundlage der Verarbeitung, d.h. eine Verarbeitung auf Basis berechtigter Interessen nach Art. 6 Abs. 1 Buchst. f DSGVO. Nach Ansicht des Europäischen Datenschutzausschusses können die Verantwortlichen dabei die Ergebnisse der notwendigen Interessenabwägung mitteilen.

Auf jeden Fall sind Verantwortliche in der Pflicht, die Ergebnisse der Interessenabwägung auf Anfrage der betroffenen Person mitzuteilen. Hierzu bietet sich ein entsprechender Hinweis im Rahmen der Informationspflichten an.

## Fazit: EDSA-Leitlinien bieten umfangreiche Hilfestellung

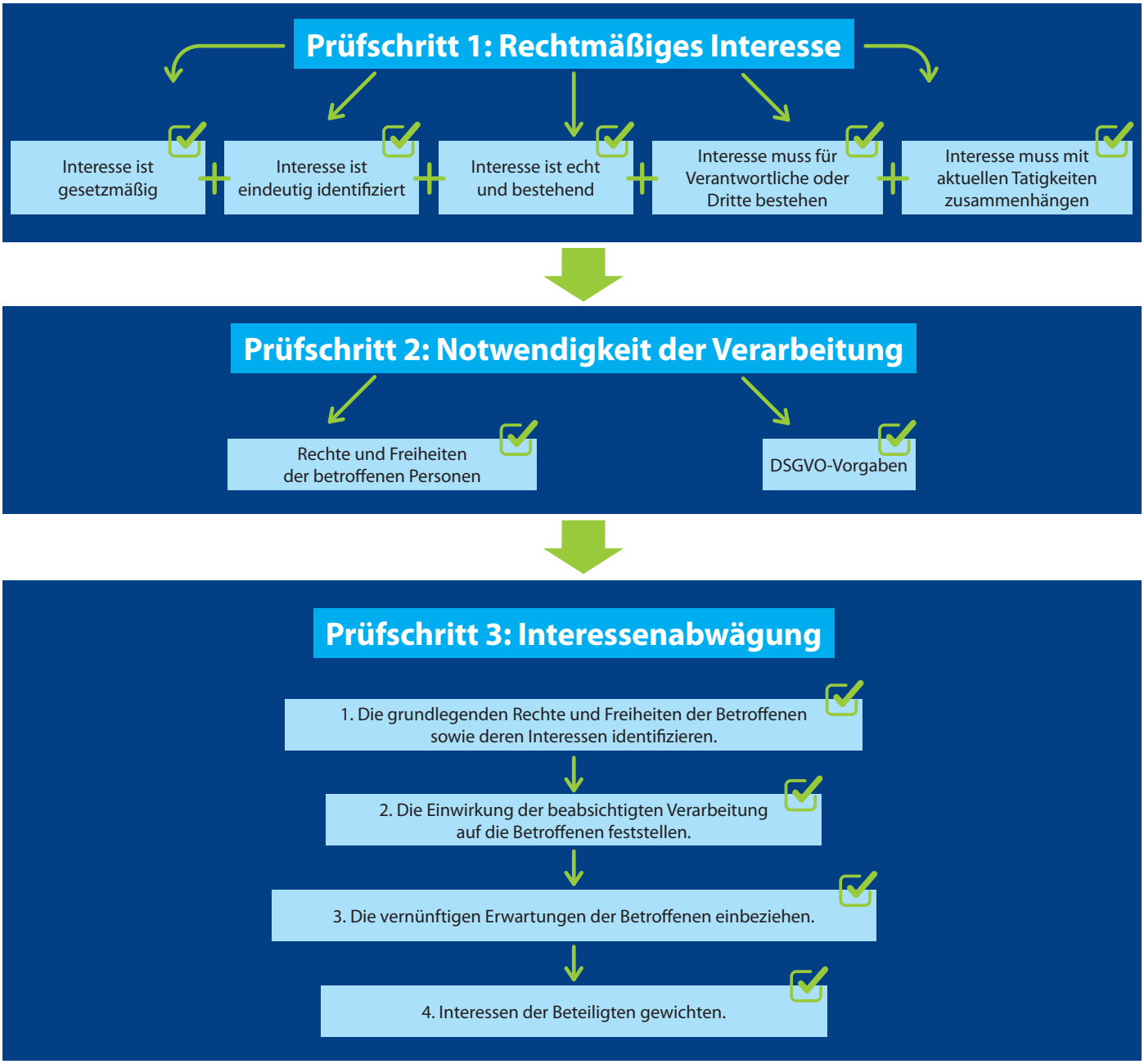
Mit den neuen Leitlinien zur Verarbeitung auf der Rechtsgrundlage berechtigter Interessen gibt der EDSA Verantwortlichen und Datenschutzbeauftragten eine umfangreiche Hilfestellung an die Hand, welche Aspekte besonders zu beachten sind. Die Leitlinien sorgen damit für mehr Rechtsklarheit, da der entsprechende Artikel der DSGVO sehr auslegungsbedürftig ist.

Die Leitlinien befinden sich aktuell noch im Stadium der öffentlichen Konsultation, d.h. der Text ist noch nicht endgültig. Es ist aber davon auszugehen, dass sich die dargestellten Prüfschritte nicht wesentlich ändern werden.

**ONLINE-TIPP**

***Der gesamte Text der neuen Leitlinien 1/2024 des Europäischen Datenschutzausschusses zur Verarbeitung personenbezogener Daten vom 08.10.24 ist – derzeit leider nur auf Englisch – verfügbar unter: https.//ogy.de/7n5b.***

Andrea Gailus ist Rechtsanwältin in eigener Kanzlei mit Schwerpunkt Datenschutz- und Telekommunikationsrecht.




**Übersicht über die drei Hauptprüfschritte**

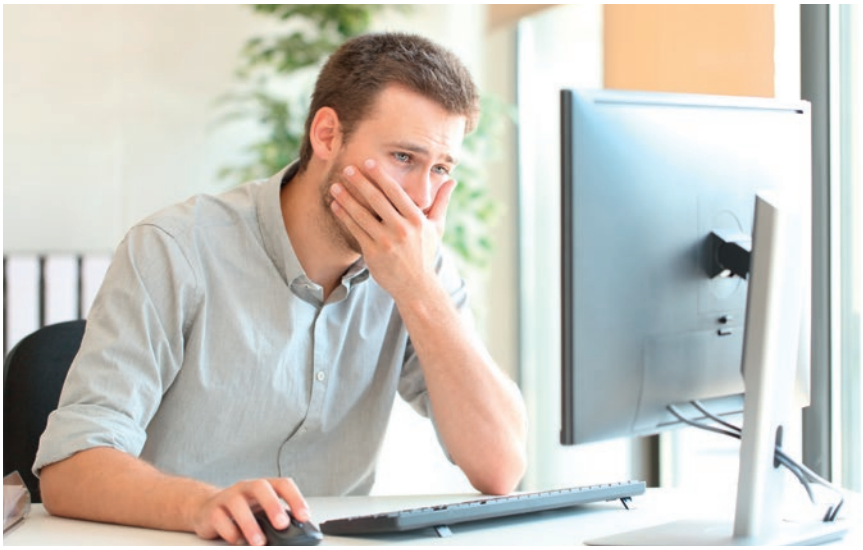


Bild: iStock.com/AntonioGuillem

**Über eine halbe Milliarde Facebook-Datensätze landeten ohne Zustimmung der Betroffenen im öffentlichen Internet. Für diese stellt das laut BGH einen immateriellen Schaden dar. Ein solcher Schaden droht auch bei Ransomware-Angriffen.**

DSGVO-Schadensersatz

# Kontrollverlust als Schaden

**Der Begriff des Schadens ist laut EuGH weit auszulegen. Bei einem Datenschutzvorfall, der 533 Millionen Facebook-Nutzerkonten betraf, zog der BGH daraus jetzt die Konsequenzen: Schon der bloße Verlust der Kontrolle über die eigenen Daten stellt einen Schaden dar. Die Folgen dieser Auslegung reichen weit über den konkreten Fall hinaus.**

Der Ausgangsfall betraf Facebook. Bis September 2019 gab es bei Facebook eine Kontakt-Import-Funktion. Damit konnte jeder Facebook-Nutzer das Facebook-Profil eines anderen Nutzers finden, wenn er dessen Mobilfunknummer in die Anwendung eingab. Das funktionierte unter zwei Voraussetzungen:

- Zum einen musste die Mobilfunknummer Verwendung finden, die im gesuchten Facebook-Profil hinterlegt war.
- Zum anderen durfte der gesuchte Facebook-Nutzer die Voreinstellungen nicht verändert haben, die Facebook für die Suche über die Kontakt-Import-Funktion vorgegeben hatte.

Im „gefundenen" Profil waren Daten sichtbar, die als Pflichtangaben in allen Facebook-Profilen öffentlich einsehbar sind, etwa Vorname und Familienname, aber darüber hinaus weitere Daten, die der Facebook-Nutzer als „öffentlich" gekennzeichnet hatte.

## Tückische Datenschutz-Voreinstellungen

Viele Facebook-Nutzerinnen und -Nutzer glaubten, die Kontakt-Import-Funktion durch die Datenschutzeinstellung für ihre Mobilfunknummer ausbremsen zu können. Zu diesem Zweck stellten sie die Sichtbarkeit der Mobilfunknummer in ihrem Profil auf „nur ich" ein.

Das wirkte sich jedoch zu ihrer Überraschung nicht auf die Kontakt-Import-Funktion aus. Die dort vorhandene standardmäßige Voreinstellung, dass „alle" diese Suchmöglichkeit hatten, blieb trotzdem bestehen.

Nur wer auch diese Voreinstellung gezielt von „alle" auf „Freunde von Freunden" oder „Freunde" veränderte, war von anderen Personen nicht mehr mittels der Mobilfunknummer aufzufinden.

## Unbekannte nutzten die Schwachstelle aus

Die Struktur von Mobilfunknummern folgt bestimmten Regeln. Dies nutzten Unbekannte, um auf der Basis dieser Regeln zufällige Ziffernfolgen zu erzeugen und diese potenziell existierenden Mobilfunknummern dann über die Kontakt-Import-Funktion bei Facebook einzugeben.

Sofern die entsprechende Ziffernfolge tatsächlich als Mobilfunknummer in Facebook hinterlegt war, konnten sie auf das Profil zugreifen, das zu dieser Nummer gehörte. Dort kopierten sie dann so viele Daten wie möglich. Dieses Vorgehen, das sog. „Scraping", gelang zwischen Januar 2018 und September 2019 nicht weniger als 533 Millionen Mal. Die dabei erbeuteten Daten stellten die Täter im April 2021 öffentlich ins Internet.

## Ein Betroffener fordert Schadensersatz

Der Kläger des Verfahrens, das bis zum Bundesgerichtshof (BGH) kam, war vom Scraping betroffen. Er forderte von Facebook Schadensersatz. Sein Argument: Die beschriebene Voreinstellung habe gegen die Datenschutz-Grundverordnung (DSGVO) verstoßen. Daraus sei ihm ein Schaden entstanden, denn er habe gegen seinen Willen die Kontrolle über seine Daten verloren.

Das zuständige Landgericht sprach ihm Schadensersatz in Höhe von 250 Euro zu. Dagegen ging Facebook in die Berufung. Das Oberlandesgericht lehnte jeglichen Schadensersatz ab. Deshalb trieb der Kläger das Verfahren bis zum Bundesgerichtshof als letzter Instanz.

## DSGVO-Schadensersatz hat vier Voraussetzungen

Folgende drei Voraussetzungen für einen Anspruch auf Schadensersatz gemäß Art. 82 DSGVO muss derjenige beweisen, der Schadensersatz fordert:

- Es muss ein Verstoß gegen die DSGVO vorliegen.
- Es muss ein Schaden entstanden sein.
- Zwischen dem Verstoß gegen die DSGVO und dem Schaden muss ein ursächlicher Zusammenhang bestehen.

Hinzu kommt als vierte Voraussetzung, dass den Verantwortlichen ein Verschulden hinsichtlich des DSGVO-Verstoßes trifft. Besonderheit dabei: Ein solches Verschulden wird kraft Gesetzes vermutet. Diese Vermutung kann der Verantwortliche nur widerlegen, „wenn er nachweist, dass er in keinerlei Hinsicht für den Umstand, durch den der Schaden eingetreten ist, verantwortlich ist“ (Art. 82 Abs. 3 DSGVO).

## Die DSGVO sagt wenig zum Thema „Schaden“

Art. 82 Abs. 1 DSGVO stellt klar, dass der Schaden materieller oder immaterieller Art sein kann. Es kann sich also etwa um die Beschädigung einer Sache handeln („materieller Schaden“), aber auch um einen Schaden, der sich nicht unmittelbar in Geld beziffern lässt, wie eine Verletzung des Rufs („immaterieller Schaden“).

Erwägungsgrund 146 Satz 3 zur DSGVO hält außerdem fest, der Begriff des Schadens solle „auf eine Art und Weise ausgelegt werden, die den Zielen dieser Verordnung in vollem Umfang entspricht.“

## Immaterielle Schäden können gravierend sein

Erwägungsgrund 85 Satz 1 zur DSGVO zählt Beispiele für immaterielle Schäden auf. Er erwähnt etwa den „Verlust der Kontrolle über […] personenbezogene Daten“, aber auch Diskriminierung und Rufschädigung. Daraus leitet der BGH unter Bezug auf die Rechtsprechung des Europäischen Gerichtshofs (EuGH) folgende Grundsätze ab (Rn 30 des Urteils):

- Schon der bloße Verlust der Kontrolle über die eigenen Daten stellt einen Schaden dar.
- Das gilt auch ohne eine missbräuchliche Verwendung dieser Daten.
- Die betroffene Person muss keine Befürchtungen und Ängste hinsichtlich des Missbrauchs ihrer Daten nachweisen.
- Wenn die betroffene Person besondere Befürchtungen oder Ängste nachweisen kann, können sie den immateriellen Schaden vertiefen oder vergrößern. Sie bilden aber keine Voraussetzung dafür, dass überhaupt ein Schaden vorliegt.

## Begründungen mit Textbausteinen reichen oft aus

Betroffene Personen müssen begründen, warum sie durch Scraping einen Schaden erlitten haben. Dabei will der BGH die Anforderungen nicht überspannen (Rn 35–41 des Urteils):

- Die Daten seien stets in vergleichbarer Weise abgegriffen und ins Internet gestellt worden. Deshalb liege es auf der Hand, dass die Argumentation „jedenfalls im Ausgangspunkt notwendig vergleichbare Züge trägt“.
- Der Scraping-Vorfall als solcher stehe ebenso fest wie die anschließende Veröffentlichung der Daten.
- Daher genüge bezüglich des Kontrollverlusts die Darlegung, dass der Kläger seine Telefonnummer stets nur bewusst und zielgerichtet weitergebe und nicht allgemein im Internet zugänglich mache.
- Er muss nicht im Einzelnen ausführen, welchen anderen Personen er seine Telefonnummer offengelegt hat.

## 100 Euro Schadensersatz als Basiswert

Welcher Geldbetrag angemessen ist, um einen immateriellen Schaden auszugleichen, hängt von den Umständen des Einzelfalls ab. Der BGH nennt jedoch eine Faustregel, an der sich die anderen Gerichte orientieren können: Als Ausgleich „für den eingetretenen Kontrollverlust als solchem“ erscheint eine Größenordnung von 100 Euro angemessen (Rn 100 des Urteils).

## Höhere Beträge sind denkbar

100 Euro bilden nur eine Richtschnur. Der BGH nennt eine Reihe von Faktoren, auf die es im Einzelfall bei der Ermittlung des konkreten Betrags ankommt. Die folgenden Faktoren dürften besonders häufig relevant sein (Rn 99 des Urteils):

- Sensibilität der betroffenen Daten: Wenn es etwa um Gesundheitsdaten geht (siehe Art. 9 Abs. 1 DSGVO), ist der Kontrollverlust als gravierender einzuschätzen.
- Ausmaß des Kontrollverlusts: Wenn die Daten einem unbegrenzten Empfängerkreis offenstehen, wiegt dies mehr, als wenn es um einen begrenzten Empfängerkreis geht.
- Dauer des Kontrollverlusts: Ein vorübergehender Kontrollverlust ist weniger bedeutsam als ein dauerhafter Kontrollverlust.

## Die Folgen des Urteils sind erheblich

Das Urteil des BGH vom 18.11.2024 mit dem Aktenzeichen VI ZR 10/24 ist zu finden unter https://ogy.de/gwvh. Es wird v.a. nach Cyberattacken erhebliche praktische Auswirkungen haben. So ist bei erfolgreichen Ransomware-Attacken der Zugriff auf die Betroffenendaten nicht mehr möglich. Das stellt einen dauerhaften Kontrollverlust dar. Sehr schnell wird es Standard sein, dass betroffene Personen versuchen, dafür Schadensersatz geltend zu machen. Selbst wenn es dabei je Person nur um einen kleinen Betrag geht, können sich die einzelnen Ansprüche angesichts der meist zahlreichen Betroffenen zu einer beträchtlichen Summe aufaddieren.

Dr. Eugen Ehmann, Jurist und bis vor Kurzem Regierungspräsident von Unterfranken, verfügt über langjährige Erfahrung mit dem Datenschutz in Behörden und Unternehmen.

**Ein Besuch der Datenschutzaufsicht ist für viele Betroffene Neuland. Da hilft es, im Vorfeld zu wissen, welche Informationen dafür bereitzustellen sind.**

Bild: iStock.com/Bobex-73

Vor-Ort-Prüfungen: Ablauf und Empfehlungen

# Wenn die Datenschutzaufsicht zu Besuch kommt

**Was tun, wenn die Behördenvertreter eine Prüfung vor Ort ankündigen oder unangekündigt vor der Tür stehen? Lesen Sie, wie diese Kontrollen im datenschutzrechtlichen Aufsichtsverfahren einzuordnen sind und ablaufen, was die Aufsicht darf und welche Pflichten Verantwortliche bzw. Auftragsverarbeiter haben.**

Eine Prüfung durch die Datenschutzaufsichtsbehörde führt regelmäßig zu Unsicherheiten im Unternehmen, selbst wenn sie anlassunabhängig erfolgt.

## Wie alles beginnt

Erfährt eine Datenschutzaufsichtsbehörde von einem möglichen Datenschutzverstoß, z.B. durch Beschwerden betroffener Personen, Veröffentlichungen in der Presse, Meldungen gemäß Art. 33 der Datenschutz-Grundverordnung (DSGVO) oder bei anlassunabhängigen Prüfungen, muss sie tätig werden.

Hierzu leitet die Behörde entweder ein verwaltungsrechtliches Aufsichtsverfahren, ein sanktionsrechtliches Ordnungswidrigkeitenverfahren oder beide Verfahren parallel ein. (Zu den Unterschieden zwischen den Verfahren siehe die Erläuterungen links.)

Der überwiegende Schwerpunkt der behördlichen Praxis ist das Aufsichtsverfahren. Es bildet auch den Ausgangspunkt dieses Beitrags.

**WICHTIG**

*Ein Aufsichtsverfahren ist auch anlasslos von Amts wegen möglich. Deshalb können Vor-Ort-Prüfungen nicht nur dann stattfinden, wenn ein Datenschutzverstoß vorliegt oder vorliegen könnte. Aufsichts- und Bußgeldverfahren sind getrennt zu führen und separat zu betrachten. Sie können aber parallel laufen und das Aufsichtsverfahren kann in ein Bußgeldverfahren „übergehen".*

## Warum die Datenschutzaufsicht vorbeischaut

Die Aufsichtsbehörden ziehen eine Vor-Ort-Prüfung insbesondere in Betracht, wenn andere Untersuchungsmaßnahmen nicht geeignet oder unergiebig sind, um einen Sachverhalt zweifelsfrei feststellen oder überprüfen zu können. Das ist in der Praxis der Fall, wenn Verantwortliche bzw. Auftragsverarbeiter mehrfach nicht auf eine schriftliche oder fernmündliche Kontaktaufnahme reagieren.

## Aufsichts- und Ordnungswidrigkeitenverfahren

Das verwaltungsrechtliche Aufsichtsverfahren („Aufsichtsverfahren") und das sanktionsrechtliche Ordnungswidrigkeitenverfahren („Bußgeldverfahren") haben unterschiedliche Zielrichtungen, Verfahrensregelungen und Befugnisse für die Behörde. Eine Vor-Ort-Prüfung ist im Rahmen beider Verfahren möglich. Das Bußgeldverfahren zielt auf die Verhängung einer Geldbuße gem. Art. 83 DSGVO, kann aber auch mit einer Einstellung des Verfahrens enden. Es ist im Gesetz über Ordnungswidrigkeiten und in der Strafprozessordnung geregelt. Das Aufsichtsverfahren ist in der DSGVO, dem Bundesdatenschutzgesetz (BDSG), den Landesdatenschutzgesetzen sowie den Verwaltungsverfahrensgesetzen des Bundes und der Länder geregelt. Es zielt auf die Beseitigung eines etwaigen Datenschutzverstoßes sowie die Überwachung und Durchsetzung der DSGVO (Art. 58 Abs. 2 Buchst. a bis h und j, Art. 57 Abs. 1 Buchst. a DSGVO).

Ein Vor-Ort-Termin erfolgt auch bei sehr komplexen Sachverhalten und in zeitkritischen Fällen der Klärung von Sachverhalten und Beweissicherung. Ein Vor-Ort-Termin findet zudem häufig statt, die Umsetzung von Abhilfemaßnahmen zu prüfen.

Schließlich kann es im Rahmen von anlasslosen Prüfungen – abhängig vom Ansatz der jeweiligen Aufsichtsbehörde – weitere Gründe geben. Die Brandenburgische Datenschutzbeauftragte (LDA Bbg) prüfte z.B. Autohäuser wie folgt: Sie schaute sich zunächst vor Ort einzelne Prozesse und Datenschutzmaßnahmen an, um diese anschließend einer vertieften Prüfung zu unterziehen (LDA Bbg, TB 2022, Abschn. III 1, https://ogy.de/LDA_Bbg).

## Wie eine Vor-Ort-Prüfung typischerweise abläuft

Der Ablauf einer Vor-Ort-Prüfung lässt sich grundsätzlich in drei Teile gliedern:

- organisatorischer Teil
- inhaltlicher Gesprächsteil
- Begehung (tatsächlicher Zugang zu Unterlagen etc.)

### Belehrung über Rechte

Eine Vor-Ort-Prüfung beginnt nach Eintreffen der Vertreter der Aufsichtsbehörde mit einer Belehrung gemäß § 40 Abs. 4 BDSG: Es besteht eine Auskunftspflicht gegenüber der Datenschutzaufsicht; eine Ausnahme bilden solche Fragen, deren Beantwortung sich oder einen Angehörigen gem. § 383 Abs. 1 Nr. 1 bis 3 Zivilprozessordnung der Gefahr einer strafgerichtlichen Verfolgung oder eines Ordnungswidrigkeitenverfahrens aussetzen würde.

### Vorstellungsrunde

Die Teilnehmer stellen sich vor, um ihre Funktionen und thematische Zuordnung zu klären, ebenso die Identität noch nicht bekannter Personen und ggf. deren Bevollmächtigung, z.B. bei Externen. Anschließend erörtern die Beteiligten Anlass, Gegenstand, Zweck und Ziel des Vor-Ort-Termins.

### Inhaltlicher Gesprächsteil

Danach erläutert die Behörde, wie sich der Sachverhalt aus ihrer Sicht bislang darstellt. Nun haben Verantwortliche bzw. Auftragsverarbeiter die Gelegenheit, ihre zuvor erfolgte schriftliche Darlegung klarzustellen, zu ergänzen und etwaige Missverständnisse auszuräumen. Diese Möglichkeit sollten Sie nutzen.

Anschließend stellt die Aufsichtsbehörde Fragen. Deren Inhalt hängt ab vom Prüfungsgegenstand und vom Stand der regelmäßig zuvor erfolgten schriftlichen Klärung. Regelmäßig wird die Aufsicht an ggf. zuvor angeforderte und schriftlich bereitgestellte Informationen und Unterlagen anknüpfen.

Es ist schwer vorhersehbar, in welche Richtung sich das Gespräch entwickeln kann. Das ist letztlich abhängig vom konkreten Einzelfall und dem Inhalt sowie der Art und Weise der Kommunikation, die vor dem Vor-Ort-Termin stattfand.

Ein Fokus liegt häufig auf organisatorischen und prozessualen Aspekten. Rechtlich relevante Punkte können ebenfalls Gegenstand der Fragen sein. Allerdings ist der Zweck eines Vor-Ort-Termins nur, den Sachverhalt zu ermitteln, und nicht die rechtliche Würdigung durch die Aufsicht.

Am Ende des Gesprächsteils hält die Aufsichtsbehörde fest, welche Informationen und Dokumente die Beteiligten im Vor-Ort-Termin nicht zur Verfügung stellen konnten und daher nachzureichen sind (siehe dazu die Randspalte auf der nächsten Seite). Eine etwaige Aushändigung während des Termins vor Ort wird die Behörde in der Regel nur durchsetzen, wenn sie befürchtet, dass andernfalls jemand den Status quo verändern könnte.

### Vor-Ort-Begehung (tatsächlicher Zugang zu Unterlagen etc.)

Der Umfang und Verlauf der eigentlichen Begehung vor Ort hängen stark vom Einzelfall ab. Stehen bestimmte Daten oder Datenbestände infrage, wird die Behörde Zugang zu diesen Daten via Monitor und mithilfe entsprechender Anwendungen verlangen. Ist der Prüfungsgegenstand eine Videoüberwachung von Beschäftigten, wird die Aufsicht Teile der betroffenen Bereiche oder im Zweifel das gesamte Betriebsgelände einschließlich der Außenumgrenzung begehen wollen. So kann sie die Kameras einschließlich deren Ausrichtung, aber auch Kontrollräume und Kontrollmonitore sowie die Speichertechnik in Augenschein nehmen. →

## Fragen der Aufsicht: Beispiel Betroffenenrechte

**Folgende organisatorische und prozessuale Fragen werden regelmäßig im Mittelpunkt stehen, wenn der Prüfungsgegenstand die Rechte der betroffenen Person sind:**

- **Wer macht bei Anfragen von betroffenen Personen was und wie?**
- **Wie sehen die Maßnahmen und Abläufe aus, damit Anfragen an die intern zuständige Stelle gelangen?**
- **Wie steht es um die Einbindung von Dienstleistern, Vereinbarungen und Vorgaben?**
- **Welche internen Vorgaben bestehen in Form von Richtlinien etc., wie Anfragen zu bearbeiten sind, eine Auskunft zu erteilen ist usw.?**
- **Wie gestalten sich interne Kontrollprozesse?**
- **Wann und wie werden Daten gelöscht und betroffene Personen darüber informiert?**

## Beispiele für die Bereitstellung von Informationen

- gespeicherte personenbezogene Daten (in erster Linie in Zusammenhang mit dem Prüfungsgegenstand)
- Leistungs- und Systembeschreibungen
- interne Handlungsanweisungen und Richtlinien
- sonstige interne und externe Kommunikation
- Verzeichnisse von Verarbeitungstätigkeiten (s. auch spezielle Regelung in Art. 30 Abs. 4 DSGVO)
- Verfahrensdokumentationen inkl. Datenschutz- und Sicherheitskonzepte sowie Details der technischen und organisatorischen Maßnahmen wie Zugriffsbeschränkungen, Rollenkonzepte etc.
- Dokumentation interner und externer Audits
- Vereinbarungen mit Auftragsverarbeitern einschließlich Weisungen (Art. 28 Abs. 3 Satz 2 Buchst. a DSGVO)
- sonstige vertragliche Vereinbarungen
- Dokumentation von „Datenschutzpannen" gem. Art. 33 Abs. 5 DSGVO
- Datenschutz-Folgenabschätzungen
- Qualifikation von Datenschutzbeauftragten

**BEISPIEL**

*Ein Klassiker der Vor-Ort-Prüfung sind auch in der heutigen Zeit „analoge" technische und organisatorische Maßnahmen. Insofern kann das gesamte Betriebsgelände inkl. Büros etc. betroffen sein, wenn die Aufsichtsbehörde „analoge" Maßnahmen prüft wie z.B. die Einhaltung einer „Clean-Desk-Policy", die Einsehbarkeit von Monitoren oder die Standorte von Druckern und „Datenschutztonnen".*

Im schlechtesten Fall findet die Aufsicht einen Server-Schrank in einer Gästetoilette, der ein defektes Schloss hat und zugleich als Wickeltisch dient (so geschehen bei einer Prüfung der niedersächsischen Datenschutzaufsicht, siehe LfD Nds, 27. TB 2021, S. 89, https://ogy.de/LfD_Nds).

### Was die Aufsichtsbehörde alles darf

Den rechtlichen Rahmen einer Vor-Ort-Prüfung ziehen die Befugnisse der Aufsicht und die Pflichten der Verantwortlichen bzw. Auftragsverarbeiter. Rechtsgrundlage für das Handeln der Aufsicht sind die Untersuchungsbefugnisse gem. Art. 58 Abs. 1 Buchst. a DSGVO, die eine Vor-Ort-Prüfung insgesamt abdecken. Sie werden ergänzt durch § 40 BDSG.

Bei öffentlichen Stellen gelten zudem die Regelungen von § 16 BDSG bzw. der Landesdatenschutzgesetze. Soll eine der Maßnahmen im Wege eines Verwaltungsakts erlassen und durchgesetzt werden, besteht gemäß Verwaltungsverfahrensgesetz insbesondere eine Anhörungspflicht gegenüber den Beteiligten (§ 28 VwVfG).

#### Anweisung, Informationen bereitzustellen

Die Datenschutzaufsichtsbehörde kann im Rahmen der Vor-Ort-Prüfung die Anweisung erteilen, Informationen bereitzustellen (Art. 58 Abs. 1 Buchst. a DSGVO). Sie darf alle Informationen verlangen, die für die Erfüllung der behördlichen Aufgaben erforderlich sind. Das ist der Fall, wenn es für die Aufgabenerfüllung förderlich ist und nicht gleich wirksam, aber weniger eingriffsintensiv erfolgen kann.

Damit sind sämtliche Informationen rund um den Untersuchungsgegenstand erfasst. Die Informationen können technischer, organisatorischer und rechtlicher Art sowie mit und ohne Personenbezug sein. Eine Auswahl praxisrelevanter Beispiele, welche Informationen das sein können, findet sich in der links nebenstehenden Übersicht. In der Regel fragen Aufsichtsbehörden die Informationen vor dem Vor-Ort-Termin in Schriftform an. Die Aufsicht kann vor Ort anweisen, weitere Informationen bereitzustellen, um offene Punkte zu vertiefen oder zu klären, sowie zu sonstigen Prüfungszwecken, z.B. zum Nachweis einer Umsetzung.

Die Art und Weise, wie die Informationen bereitzustellen sind, ist gesetzlich nicht konkret geregelt. Die Möglichkeiten sind mündlich wie schriftlich in Papierform oder digital und insofern auch in keinem bestimmten Dateiformat. Allerdings gilt: Die Art und Weise der Bereitstellung muss den Aufsichtsbehörden ihre Aufgabenerfüllung erleichtern und darf sie nicht erschweren.

#### Zugang zu personenbezogenen Daten, Informationen und Räumlichkeiten

Die Datenschutzaufsichtsbehörde kann im Rahmen der Vor-Ort-Prüfung Zugang zu allen personenbezogenen Daten und Informationen verlangen (Art. 58 Abs. 1 Buchst. e DSGVO). Es gilt derselbe Umfang wie bei der Bereitstellungspflicht gemäß Art. 58 Abs. 1 Buchst. a DSGVO. Einschränkungen können sich aus Geheimhaltungspflichten ergeben (§ 29 Abs. 3 BDSG).

Die Datenschutzaufsichtsbehörde kann außerdem Zugang zu den Räumlichkeiten einschließlich aller Datenverarbeitungsanlagen verlangen. Hierbei muss sie sich an das Verfahrensrecht halten (Art. 58 Abs. 1 Buchst. f DSGVO).

Der Umfang dieses Zugangsrechts hängt davon ab, was erforderlich ist, um die behördlichen Aufgaben zu erfüllen. Daher muss die betroffene Organisation der Aufsicht regelmäßig nur Zugang zu Räumen mit geschäftlicher Funktion und nur zu üblichen Betriebs-/Geschäftszeiten einräumen (§§ 40 Abs. 5 Satz 3, 16 Abs. 4 BDSG).

#### Duldungs- und Mitwirkungspflicht

Die Verweigerung oder unvollständige Gewährung des Zugangs ist bußgeldbewehrt (Art. 83 Abs. 5 Buchst. e DSGVO). Beachten Sie, dass Verantwortliche bzw. Auftragsverarbeiter nicht nur eine Duldungspflicht gemäß § 40 Abs. 5 Satz 2

BDSG haben, sondern auch eine gewisse Mitwirkungs- und Unterstützungspflicht (Art. 31 DSGVO). Hierzu zählen z.B., Hard- und Software zu starten und Daten sichtbar zu machen. Ein Verstoß gegen diese Mitwirkungs- und Unterstützungspflicht ist ebenfalls bußgeldbewehrt (Art. 83 Abs. 4 Buchst. a DSGVO).

**Was ist mit personenbezogenen Daten und Geschäfts-/Betriebsgeheimnissen?**

Eine Kenntnisnahme und Verarbeitung personenbezogener Daten sowie von Geschäfts- und Betriebsgeheimnissen durch die Aufsicht ist zulässig, soweit es zu deren Aufgabenerfüllung erforderlich ist. Da bei einem Zugriff auf das System häufig nicht absehbar ist, ob und welche Informationen betroffen sind, müssen Verantwortliche bzw. Auftragsverarbeiter (mit)klären, in welchem Umfang der Zugang zu eröffnen ist.

Eine Prüfung technischer und organisatorischer Maßnahmen erfordert z.B. häufig keine Kenntnisnahme personenbezogener Daten oder nur in einem reduzierten Umfang. In solchen Fällen sollten Sie eine Prüfung anhand von Beispiel-Datensätzen oder einer Demonstration statt eines Lesezugriffs ermöglichen.

## Empfehlungen für die Praxis

Bereiten Sie einen Vor-Ort-Termin sowohl organisatorisch als auch inhaltlich umfassend vor. Legen Sie inhaltlich den Fokus nicht ausschließlich auf den Prüfungsgegenstand, sondern lassen Sie dabei auch die Datenschutzorganisation und das Datenschutzmanagement insgesamt nicht außer Acht.

Bereiten Sie die relevanten Unterlagen vor und halten Sie diese griffbereit. Das sind zum einen alle Dokumente und Informationen, die im Zusammenhang mit dem Untersuchungsgegenstand stehen oder auch nur stehen könnten. Relevant ist aber auch alles, was unabhängig vom konkreten Prüfungsgegenstand zu einer ordnungsgemäßen Datenschutzorganisation und einem Datenschutzmanagement zählt und sich unter die Rechenschaftspflicht gemäß Art. 5 Abs. 2 DSGVO fassen lässt. Zu den Unterlagen, die in diesem Zusammenhang relevant sind, zählen insbesondere:

- Verzeichnis der Verarbeitungstätigkeiten
- Löschkonzept
- Datenschutzanweisungen und Vorgaben für die Beschäftigten wie Richtlinien etc.
- Dokumentation der Prozesse zu Betroffenenrechten wie Auskunft etc.
- Dokumentation der Auftragsverarbeitungen (inkl. Kontrollen)
- Dokumentation der Datenschutzschulung der Beschäftigen
- Dokumentation der technischen und organisatorischen Maßnahmen
- Bestellungsurkunde und Berichte des/der betrieblichen/behördlichen Datenschutzbeauftragten

Wählen Sie die „richtigen“ Ansprechpartner als mitwirkende Personen für den Termin aus und bereiten Sie diese eingehend vor. Ein kurzes „Briefing“ reicht gerade auch für die Geschäftsführung und Führungskräfte in der Praxis häufig nicht aus. Lassen Sie hierbei auch die strategischen Aspekte nicht außer Acht.

## Was „die richtige Strategie“ ist

Nutzen Sie die Möglichkeiten, den Terminverlauf zu gestalten: Fragen Sie zeitliche Unterbrechungen an, wenn es für interne Rücksprachen erforderlich ist. Solche Unterbrechungen gewährt die Aufsicht regelmäßig, wenn kein Anlass zu der Annahme besteht, dass die Sicherung von Beweismaterial gefährdet ist. Nehmen Sie Ihre Rechte wahr, z.B. Auskunftsverweigerung, und fordern Sie von der Behörde Erläuterungen, Begründungen oder eine Anhörung ein, sofern es angezeigt und zielführend ist.

Sie sollten grundsätzlich eine ausgewogene „Strategie zwischen Kooperation und strikter Rechtewahrnehmung“ verfolgen und je nach Verlauf des Termins anpassen. Vermindern Sie die Gefahr neuer Angriffsflächen, indem Sie sich bei Ihren Ausführungen auf das Notwendigste beschränken. Und vermeiden Sie wenn möglich rechtliche Erörterungen, soweit sie Ihre „Verteidigungsstrategie“ betreffen.

Auf dieser Grundlage einer guten inhaltlichen und organisatorischen Vorbereitung werden Sie die Herausforderungen einer Vor-Ort-Prüfung meistern können.

Dr. Markus Lang ist Rechtsanwalt in Düsseldorf (Datenschutzrecht-Praxis) und berät Unternehmen zu allen Fragen des Datenschutz- und IT-Rechts.

**PRAXIS-TIPP**

***Dokumentieren Sie den Termin umfassend. Das ist wichtig für den weiteren Austausch mit der Behörde. Außerdem sollten Sie Hinweise der Aufsicht während des Vor-Ort-Termins beachten, einen etwaigen Handlungsbedarf prüfen und Prozesse, Dokumente etc. anpassen, sofern die Hinweise der Sache nach und rechtlich zutreffend sind. Die behördlichen Hinweise im Vor-Ort-Termin haben zwar keine Regelungskraft und Bindungswirkung, bilden aber regelmäßig die Vorstufe zu Abhilfemaßnahmen nach Art. 58 Abs. 2 DSGVO, z.B. in Form von entsprechenden Anweisungen. Gab es solche – zutreffenden – Hinweise bereits im Vorfeld, sollten Sie die Anpassungen vor dem Vor-Ort-Termin umsetzen oder zumindest anstoßen und dies beim Termin hervorheben.***

Tipps zur Vermeidung

# Excel-Datenpannen

Bild: iStock.com/win10-mc

Microsoft Excel kommt in nahezu jedem Büro zum Einsatz. Viele unterschätzen den Funktionsumfang dieses Tabellenkalkulationsprogramms. Öfter fehlt es auch an der erforderlichen Schulung und Übung. Diese Faktoren führen immer wieder zu Datenpannen, die eine Meldepflicht gemäß Art. 33 DSGVO auslösen. Vielfach wären sie leicht zu vermeiden.

Welche Leistungsfähigkeit Microsoft Excel hat, zeigt sich schon daran, wie viele „Zellen" ein Arbeitsblatt enthalten kann. Möglich sind in der aktuellen Version 1.048.576 Zeilen und 16.384 Spalten. Das ergibt maximal 17.179.869.184 (gut 17 Milliarden) Zellen auf einem einzigen Arbeitsblatt.

## Datenpannen drohen an typischen Stellen

Der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) hat eine Reihe häufiger Konstellationen zusammengestellt, bei denen unvorsichtiges Verhalten zu einer unbeabsichtigten Offenlegung personenbezogener Daten führt. In einem Dreischritt stellt er dabei jeweils zunächst das Programmfeature vor, um das es geht. Im zweiten Schritt wird geschildert, wie es bei diesem Feature zu Datenpannen kommen kann. Den dritten Schritt bilden anschließend Hinweise dazu, wie sich diese Datenpannen vermeiden ließen.

Diese Vorgehensweise lässt sich an folgendem Beispiel zeigen: Immer wieder gerät aus dem Blick, dass eine Arbeitsmappe – solange der Platz im Arbeitsspeicher ausreicht – beliebig viele Arbeitsblätter enthalten kann. Sichtbar ist jedoch beim Öffnen einer Excel-Datei zunächst nur das erste Arbeitsblatt. Das kann dazu führen, dass personenbezogene Daten, die in weiteren Arbeitsblättern enthalten sind, bei der Bearbeitung der Excel-Datei schlicht übersehen werden. Wird die Datei dann weitergegeben, sind in ihr auch diese Daten enthalten.

## Die Tipps sind direkt umsetzbar

Der BayLfD gibt eine ganze Reihe von Ratschlägen, wie eine solche Panne zu vermeiden wäre. So rät er:

- Überlegen Sie vor der Neuanlage einer Arbeitsmappe mit mehreren Arbeitsblättern, ob Sie die Aufgabe auch mit mehreren Ein-Arbeitsblatt-Arbeitsmappen erledigen können.
- Überlegen Sie, ob Sie für die zu erledigende Aufgabe Excel benötigen oder ob auch ein „einfacheres" Betriebsmittel (etwa ein Textverarbeitungsprogramm) ausreichen würde.
- Löschen Sie aus bestehenden Excel-Arbeitsmappen nach Möglichkeit konsequent die nicht (mehr) benötigten Arbeitsblätter.
- Überlegen Sie, ob die Datei beim Empfänger noch weiterbearbeitet werden soll. Falls nein, ist die Zuleitung einer PDF-Version vorzugswürdig. Denn sie lässt sich vor dem Versand leicht auf versteckte Daten kontrollieren.

Ausdrücklich betont der BayLfD, dass es bei seinen Hinweisen nicht um strukturelle Schwächen von Microsoft Excel geht. Vielmehr betreffen sie Aspekte, die in der Hektik des Büroalltags hin und wieder schlicht untergehen.

## Manchmal ginge es auch ohne Excel

Generell vertritt der BayLfD die Auffassung, dass nicht jede Arbeit, bei der das möglich ist, mit einem Tabellenprogramm wie Excel erledigt werden muss. Oft gebe es Alternativen. Auch müsse nicht jeder PC-Arbeitsplatz mit dieser Anwendung ausgestattet sein.

Wenn Excel aber zum Einsatz komme, sei auf eine hinreichende Sensibilisierung der Mitarbeiterschaft zu achten. Ohne entsprechende Schulungen geht es seines Erachtens nicht.

Quelle: Bayerischer Landesbeauftragter für den Datenschutz, 33. Tätigkeitsbericht für das Jahr 2023, Ziffer 2.5 („Datenpannen mit Microsoft Excel verursachen und vermeiden"), S. 44-50. Der Bericht ist abrufbar unter https://datenschutzarchiv.org/detailansicht/Dokumente/2023/TB_Bayern_LfD_33_2023_de.pdf

**Sprachaufzeichnungen**

## Auskunftsrecht nach DSGVO

Der Auskunftsanspruch nach Art. 15 DSGVO erstreckt sich auch auf Sprachaufzeichnungen von Kundengesprächen. Dass solche Aufzeichnungen – wie in manchen Bereichen der Kreditwirtschaft – gesetzlich vorgeschrieben sind, ändert daran nichts. Im Regelfall hat die betroffene Person einen Anspruch darauf, die Audiodatei des Gesprächs als Kopie zu erhalten (Rechtliche Grundlage hierfür ist Art. 15 Abs. 3 DSGVO). Nur wenn sie damit einverstanden ist, genügt eine Abschrift („Transkription") des Gesprächs.

Quelle: Datenschutzaufsicht Rheinland-Pfalz, Tätigkeitsbericht 2023, Kapitel 4.2 (S. 30/31). Der Tätigkeitsbericht ist abrufbar unter https://datenschutzarchiv.org/detailansicht/Dokumente/2023/TB_Rheinland-Pfalz_LfD_32_2023_de.pdf.

**Vorstellungsgespräche**

## Gruppengespräche zulässig?

Sehr zurückhaltend äußert sich der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) zu Vorstellungsgesprächen, die in Form von Gruppengesprächen stattfinden. Zwar bestünden gewisse Spielräume dafür, wie Verantwortliche Vorstellungsgespräche ausgestalten können. Die Datenschutzrechte betroffener Personen müssten jedoch auch in Bewerbungsverfahren im Blick behalten werden:

„Aus datenschutzrechtlicher Sicht sind solche Gruppengespräche bedenklich, weil hier nicht nur der potenzielle Beschäftigungsgeber, sondern gegebenenfalls auch andere Bewerberinnen und Bewerber Einzelheiten zu persönlichen und beruflichen Verhältnissen ihrer Mitbewerbenden erfahren können. Schon die Tatsache, dass sich eine Person auf eine bestimmte Stelle beworben hat, geht Dritte eigentlich nichts an."

Folgende Aspekte sind aus Sicht des BayLfD besonders zu beachten:

- Einzelgespräche sind in Auswahlverfahren grundsätzlich vorzugswürdig.
- Jedenfalls müssten alle sensiblen und persönlichen Daten in Einzelgesprächen geklärt werden. Dazu gehört seines Erachtens auch die Erörterung des Lebenslaufs.
- Beim Testen von Softskills wie dem Kommunikations- und dem Informationsverhalten sowie dem Interagieren in einer Gruppe liegen fachliche Gründe vor, die Gruppengespräche rechtfertigen. Sie müssen dann aber auf diese Aspekte beschränkt sein.

Quelle: Bayerischer Landesbeauftragter für den Datenschutz, 33. Tätigkeitsbericht für das Jahr 2023, Ziffer 7.3 („Vorstellungsgespräche in Gruppen"), S. 118/119. Der Bericht ist abrufbar unter https://datenschutzarchiv.org/detailansicht/Dokumente/2023/TB_Bayern_LfD_33_2023_de.pdf .

**Ungeklärtes Verhältnis**

## DSGVO und DSA/DMA

Auf Wunsch eines Mitglieds des Deutschen Bundestags haben dessen wissenschaftliche Dienste eine Ausarbeitung mit dem Titel „Zum Verhältnis des Digital Services Act (DSA) und des Digital Markets Act (DMA) zur EU-Datenschutzgrundverordnung" erstellt. Da es dazu bisher keine Rechtsprechung des Europäischen Gerichtshofs (EuGH) gibt, werden teils entgegengesetzte Auffassungen vertreten (s. S. 7–8 des Papiers).

Der DSA enthält insbesondere Sorgfaltspflichten für die Anbieter von „Vermittlungsdiensten". Solche Anbieter sorgen etwa für die Durchleitung elektronischer Informationen oder stellen Hosting-Dienste zur Verfügung. Ohne derartige Vermittlungsdienste würden Online-Märkte nicht funktionieren. Die Dienste beziehen sich in beträchtlichem Ausmaß auf personenbezogene Daten.

Die Vorgaben des DMA sollen für das reibungslose Funktionieren von Märkten sorgen, auf denen „Torwächter" tätig sind. Darunter sind Unternehmen zu verstehen, die „zentrale Plattformdienste" bereitstellen. Zu Plattformdiensten dieser Art gehören gemäß Art. 2 Nr. 2 DMA etwa Online-Suchmaschinen und Cloud-Computing-Dienste. Dass sie in großem Umfang personenbezogene Daten verarbeiten, liegt auf der Hand. Ziel des DMA ist es insbesondere, die „Datenmacht der Torwächter" zu reduzieren (s. S. 14 des Papiers).

Manche Juristen betrachten die Regelungen des DSA und des DMA als bereichsspezifische Regelungen, die der DSGVO vorgehen. Ihr Hauptargument: Die DSGVO sei inzwischen durch ein völlig neues EU-Plattform- und Datenwettbewerbsrecht ergänzt worden, zu dem der DMA und DSA zählten. Die hierdurch bewirkte intensive Regulierung von marktmächtigen Plattformen diene auch der wirksamen Absicherung des Datenschutzgrundrechts.

Andere Stimmen in der Rechtsliteratur sind dagegen der Auffassung, die DSGVO bleibe von den Regelungen des DSA und des DMA „völlig unangetastet" (s. S. 8 des Papiers). Für betriebliche Datenschutzbeauftragte (DSB) ist das Verhältnis der Regelungen schon deshalb bedeutsam, weil es mit darüber entscheidet, was zu ihren gesetzlichen Aufgaben gehört.

Sollten DSA und DMA bereichsspezifische Regelungen zur DSGVO darstellen, würde die Befassung mit diesen Regelungen unmittelbar zu den Aufgaben der Datenschutzbeauftragten gehören. Denn dann wären sie als „andere Datenschutzvorschriften der Union" anzusehen. Um die Pflichten aus solchen Datenschutzvorschriften müssen sich DSB genauso kümmern wie um die Pflichten aus der Datenschutz-Grundverordnung (s. Art. 39 Abs. 1 Buchst. a DSGVO).

Quelle: Deutscher Bundestag, Wissenschaftliche Dienste, Unterabteilung Europa, Fachbereich Europa, Titel: Zum Verhältnis des Digital Services Act und des Digital Markets Act zur EU-Datenschutzgrundverordnung, Stand: 29.8.2024; Umfang: 19 Seiten. Die Ausarbeitung ist bei Eingabe ihres Titels in einer Suchmaschine unmittelbar zu finden.

Dr. Eugen Ehmann verfügt über langjährige Erfahrung mit dem Datenschutz in Behörden und Unternehmen. Derzeit bereitet er bereits den Datenschutzkongress IDACON 2025 vor. Unter www.idacon.de finden Sie jeweils den aktuellen Stand.

Bild: iStock.com/Maxime Horlaville

**Unternehmen müssen ihre Beschäftigten über den Umgang mit deren personenbezogenen Daten informieren. Diese Pflicht beginnt schon beim Bewerbungsprozess.**

### Auskunftspflicht gemäß DSGVO gilt auch hausintern

# Datenschutzerklärung für Beschäftigte

**Viele Verantwortliche nehmen die Auskunftspflicht sehr ernst und haben Prozesse eingeführt, um Externe über die Datenverarbeitung zu informieren. Doch es lohnt sich (und ist sogar verpflichtend), den gleichen Aufwand in die Information der eigenen Beschäftigten zu stecken.**

Eine Datenschutzerklärung auf der Website oder in Formularen eines Unternehmens gehört, sofern personenbezogene Daten verarbeitet werden, zum Standard. Es sollte bekannt sein, was sie enthalten muss, nämlich:

- den Namen und die Kontaktdaten des oder der Verantwortlichen
- die Kontaktdaten des oder der Datenschutzbeauftragten (DSB)
- die Zwecke der Datenverarbeitung
- die berechtigten Interessen der Datenverarbeitung, falls diese auf Art. 6 Abs. 1 Buchst. f der Datenschutz-Grundverordnung (DSGVO) beruht
- die Empfänger der personenbezogenen Daten
- eine etwaige Datenübermittlung in ein Drittland
- die Dauer der Datenverarbeitung
- Informationen über die Rechte, die der betroffenen Person zustehen, wie z.B. Löschung, Berichtigung und Auskunft
- Informationen zu einem etwaigen Widerrufsrecht
- Informationen bzgl. Beschwerderecht bei einer Aufsichtsbehörde

## Kein Unterschied zwischen Externen und Beschäftigten

Grundsätzlich sollten Sie als DSB die Verantwortlichen zu folgendem Punkt beraten: Die gleichen Mühen, die ein Unternehmen in eine Datenschutzinformation für „Externe“ gesteckt hat, sollte es auch für die eigenen Beschäftigten aufwenden. Warum? Weil die DSGVO bei Art. 15 DSGVO nicht unterscheidet, ob die betroffene Person jemand innerhalb oder außerhalb des Unternehmens ist.

Vielmehr spricht Art. 15 DSGVO vom „Auskunftsrecht der betroffenen Person“. Solche betroffenen Personen können gleichermaßen Kundinnen und Kunden, Lieferanten, (Website-)Besucher oder eben auch die eigene Belegschaft sein.

Es häufen sich Fälle, in denen Beschäftigte den Datenschutz „missbrauchen“: Sie ziehen bei Streitigkeiten mit dem (ehemaligen) Arbeitgeber die „Datenschutzkarte“. Das bedeutet, dass gerade in arbeitsgerichtlichen Streitigkeiten gern vom Auskunftsrecht standardmäßig Gebrauch gemacht wird.

Sich erst in diesem Stadium mit dem Thema Beschäftigtendatenschutz vertraut zu machen, ist zu spät. Das Beste ist, erst gar keine Angriffsfläche zu bieten und direkt die Beschäftigten in das ganzheitliche Datenschutzkonzept einzubeziehen. Und das fängt am besten mit einer gut durchdachten Datenschutzerklärung für Beschäftigte an.

## Inhalt der Datenschutzerklärung

Grundsätzlich gehören in eine Datenschutzerklärung für die Belegschaft dieselben Informationen wie in eine Datenschutzerklärung, die das Unternehmen z.B. für seine Kundschaft angefertigt hat. Selbstverständlich muss sich die Erklärung auf die personenbezogenen Daten beziehen, die das Unternehmen zu seinen Beschäftigten verarbeitet. Dabei sind die Verarbeitungen insbesondere im Hinblick auf folgende Punkte zu untersuchen:

- Welche personenbezogenen Daten der Beschäftigten werden verarbeitet?
- Welche Zugriffsberechtigungen bestehen auf diese Daten?
- Wie sieht es mit den Aufbewahrungsfristen aus?

Zur Gegenprobe – und zwar auch zur Kontrolle, ob das Verzeichnis von Verarbeitungstätigkeiten vollständig ist –

**PRAXIS-TIPP**

*Es ist zu empfehlen, eine Datenschutzerklärung für Beschäftigte analog zur „normalen" Datenschutzerklärung aufzubauen. Sollten Sie ein gepflegtes, aktuelles Verzeichnis von Verarbeitungstätigkeiten haben, ist es sinnvoll, die Datenverarbeitungen dort durchzugehen. So können Sie die Datenschutzerklärung für Beschäftigte leichter erstellen.*

sollten Sie die folgenden Bereiche der Datenverarbeitung in einer Mitarbeiter-Datenschutzerklärung prüfen:

- Datenverarbeitung im Rahmen des regulären Bewerbungsprozesses
- eines internen Bewerbungsprozesses
- des Beschäftigungsverhältnisses
- des Austritts aus dem Unternehmen (z.B. durch Kündigung, Erreichen des Renteneintritts)
- von Personalgesprächen (z.B. Gehaltsgesprächen, Bonuszahlungen, Mitarbeiter-Performance-Gesprächen o.Ä.)
- des Themas „Mitarbeiter werben Mitarbeiter"
- unternehmensinterner Veranstaltungen (z.B. Weihnachtsfeiern, Aufsichtsratssitzungen, Firmenevents wie z.B. Firmenläufe o.Ä.)
- von Mitarbeiterrabatten (z.B. Gewährung von vergünstigten Konditionen in Fitnessstudios, Restaurants etc.)
- des hybriden Arbeitens (sofern hier andere Regelungen wie z.B. Betriebsvereinbarungen o.Ä. vorhanden sind, sollte die Datenschutzerklärung auf diese – ggf. zusätzlich – verweisen)
- der Arbeitszeiterfassung
- der Nutzung von Fotos und Videoaufnahmen der Belegschaft (allgemein z.B. auf der Website und konkret z.B. bei Firmenevents)

## Richtig kommunizieren ist die halbe Miete

Im besten Fall haben Sie eine Datenschutzerklärung geschaffen, die alle möglichen Datenverarbeitungsszenarien der Beschäftigten abbildet. Diese Information müssen Sie an die Arbeitskräfte kommunizieren. Gemäß Art. 13 DSGVO ist die betroffene Person über die Datenverarbeitung zum Zeitpunkt der Erhebung der personenbezogenen Daten zu informieren.

Im Rahmen eines neuen Bewerbungsverfahrens (d.h. der zukünftige Mitarbeiter ist noch im Bewerbungsprozess) muss die Information z.B. durch Verlinkung auf eine Seite in der Stellenbeschreibung bereitstehen. Für alle anderen Verfahren können Sie z.B. auf eine Seite im unternehmenseigenen Intranet verlinken. Wichtig ist nur, dass alle Beschäftigten, die zu informieren sind, auf diese Seite Zugriff haben.

**Beispiel Firmenjubiläum**

Ein Beispiel: Sie haben eine umfassende Datenschutzerklärung für Beschäftigte erstellt, die u.a. die Datenverarbeitung bzgl. Firmenevents beschreibt. Die Erklärung verweist insbesondere auf das Anfertigen von Fotoaufnahmen sowie die Verarbeitung der unternehmenseigenen E-Mail-Adressen der Beschäftigten zum Einladungsversand. Eventuell fragt das Unternehmen auch Gesundheitsdaten ab, z.B. im Hinblick auf Lebensmittelunverträglichkeiten.

Das Unternehmen lädt die Beschäftigten nun zum zehnjährigen Firmenjubiläum ein. Es mietet Räumlichkeiten an, sorgt für die Verpflegung und lässt Fotos von diesem Jubiläum anfertigen.

Streng genommen muss der oder die Verantwortliche den Beschäftigten nun eine Datenschutzinformation der Einladung zur Verfügung stellen. In den seltensten Fällen soll jedoch der Datenschutz in einer solchen Einladung den meisten Platz in Anspruch nehmen.

Sie können der Verpflichtung zur Information Betroffener nach Art. 15 DSGVO z.B. durch einen Link auf eine Intranetseite nachkommen – nach dem Motto: „Im Rahmen dieses Firmenjubiläums verarbeiten wir Ihre personenbezogenen Daten. Informationen dazu finden Sie unter XXXXX."

**Beispiel interne Bewerbung**

Ein weiteres Beispiel: Sie unterhalten ein internes Stellenportal, bei dem sich die Beschäftigten informieren können, welche Stellen derzeit innerhalb des Unternehmens zu besetzen sind. Doch Sie wollen die Stellenanzeige selbst nicht überfrachten. Deshalb verlinken Sie wieder auf die Datenschutzerklärung für Beschäftigte, die sich diese im Intranet jederzeit ansehen können.

**PRAXIS-TIPP**

*Selbstverständlich sollten Sie die Datenverarbeitung im Rahmen des internen Bewerbungsprozesses mit aufführen. Im internen Stellenportal reicht ein kurzer Hinweis: „Im Rahmen Ihrer Bewerbung verarbeiten wir Ihre personenbezogenen Daten. Weitere Informationen finden Sie unter XXXXX."*

## Wer suchet, der findet

Wichtig ist, dass Angestellte wissen, wo sie Informationen zum Datenschutz im Rahmen ihres Beschäftigungsverhältnisses abrufen können. Viele Unternehmen thematisieren das Thema direkt bei der Einstellung im Onboarding-Prozess und machen die Neuzugänge auf den besagten Link aufmerksam.

Auch bietet es sich an, an geeigneter Stelle im Intranet den Link für die Datenschutzerklärung für Beschäftigte zu platzieren. Geeignete Stellen können sein: die Personalseite, die Seite für den Datenschutz, die Seite für alle neuen Mitarbeitenden.

Und: Halten Sie die Datenschutzerklärung für Beschäftigte immer aktuell! Dann sind Sie gut aufgestellt und die Belegschaft hat ein gutes Gefühl, dass der Schutz ihrer Daten einen hohen Stellenwert hat.

Doris Kiefer ist Rechtsanwältin und leitet als Head of Data Protection das Datenschutzteam eines E-Commerce-Unternehmens für ganz Europa.

Bild: iStock.com/alxpin

**Die Bewertungen des Angemessenheitsbeschlusses EU–USA fallen je nach Sichtweise unterschiedlich aus**

Datenschutzrahmen EU-USA

# Erste Evaluierung des Angemessenheitsbeschlusses

**Am 10.07.2023 erließ die Europäische Kommission einen Angemessenheitsbeschluss für die Übermittlung personenbezogener Daten in die USA. Ein Jahr später fand eine Evaluierung dieses Beschlusses statt. Die Ergebnisse sind für alle Unternehmen relevant, die Daten in die USA übermitteln.**

Der Angemessenheitsbeschluss für die USA legt fest, dass die USA ein angemessenes Datenschutzniveau für personenbezogene Daten gewährleisten. Bedingung ist, dass man bei der Übermittlung von Daten aus der EU an Unternehmen in den USA die in dem Beschluss enthaltenen Vorgaben einhält (Art. 1 des Beschlusses). Der korrekten Umsetzung dieser Vorgaben kommt somit eine zentrale Bedeutung zu.

## Vorgesehene Evaluierungen

Der Angemessenheitsbeschluss verpflichtet die EU-Kommission dazu, ihn ein Jahr nach seiner Bekanntgabe zu evaluieren. Es geht dabei darum, „ob die Feststellungen zur Angemessenheit des von den Vereinigten Staaten gewährleisteten Schutzniveaus im Rahmen des Datenschutzrahmens EU-USA noch sachlich und rechtlich gerechtfertigt sind". So erläutert Erwägungsgrund 211 des Beschlusses die Evaluierungspflicht. Sie ist in Art. 3 Abs. 4 des Beschlusses förmlich verankert.

Zu künftigen Evaluierungen ist die EU-Kommission in einer Häufigkeit verpflichtet, die mit dem Europäischen Datenschutzausschuss (EDSA) abzustimmen ist (Art. 3 Abs. 4 des Beschlusses). Ein fester zeitlicher Abstand ist nicht vorgegeben.

Die EU-Kommission hält es für zweckdienlich, dass die nächste Evaluierung in drei Jahren stattfindet. Der EDSA hat erklärt, er halte einen Zeitraum von „drei Jahren oder weniger" für angemessen (Rn 70 seines Berichts). Eine Überschreitung des Dreijahreszeitraums würde er demnach wohl nicht akzeptieren.

## Grundlage für die Evaluierung

Der Angemessenheitsbeschluss fordert, dass jede Evaluierung „auf der Grundlage aller verfügbaren Informationen, einschließlich Informationen, die bei der gemeinsam mit den zuständigen Behörden der Vereinigten Staaten durchgeführten Überprüfung gewonnen wurden", zu erfolgen hat (Art. 3 Abs. 4 des Beschlusses).

Die EU-Kommission hebt hervor, dass sie sich bei ihrer Evaluierung um eine umfassende Informationsbasis bemüht hat (näher dazu Ziffer 1 ihres Berichts). Sie wertete öffentlich zugängliches Material aus, holte aber auch Stellungnahmen sachkundiger Verbände ein. Alle Interessierten hatten zudem Gelegenheit, Stellungnahmen auf einem Internetportal abzugeben.

Ein Gremium offizieller Repräsentanten aus der EU und den USA war verantwortlich dafür, die Evaluierung durchzuführen. Auf europäischer Seite war die EU-Kommission federführend. Der EDSA war mit fünf Personen vertreten. Auf US-Seite waren alle relevanten Regierungsbehörden eingebunden, so etwa das Department of Commerce (DoC) und die Federal Trade Commission (FTC).

## Unterschiedliche Bewertungen

Das Kernstück der Beurteilung ist rechtlich gesehen der Evaluierungsbericht der EU-Kommission. Der Bericht des EDSA über die Evaluierung ergänzt ihn. Er setzt teilweise andere Akzente als der Bericht der EU-Kommission und beleuchtet zusätzliche Hintergründe. Dem EDSA lag der Bericht der EU-Kommission vor, als er

sein Dokument erstellte (siehe Rn 5/6 des EDSA-Berichts).

Seit der aktuelle Angemessenheitsbeschluss gilt, haben innerhalb eines Jahres 2.800 Unternehmen den Zertifizierungsprozess beim Department of Commerce (DoC) durchlaufen. Dagegen hatten im ersten Jahr des vom EuGH für nichtig erklärten Vorgängerbeschlusses zum Privacy Shield lediglich 2.400 Unternehmen die Zertifizierung nach den damaligen Regeln abgeschlossen. Diesen Unterschied wertet die EU-Kommission als Erfolg (Ziffer 2.1.1. ihres Berichts).

Der EDSA hebt dagegen hervor, dass über 1.100 Unternehmen ihre noch unter dem Privacy Shield erfolgte Registrierung aktiv zurückgezogen hätten. Bei 2.600 Unternehmen seien solche Registrierungen durch Zeitablauf erloschen (Rn 9 des EDSA-Berichts). Das relativiert den Erfolg der neuen Regelungen.

## Beschwerdemöglichkeiten bleiben ungenutzt

Der Datenschutzrahmen EU-USA sieht nach Anhang I des Angemessenheitsbeschlusses umfassende Beschwerdemöglichkeiten für betroffene Personen vor. Kaum jemand macht jedoch davon Gebrauch. So sind bisher weder bei den Datenschutzaufsichtsbehörden in der EU noch beim DoC solche Beschwerden eingegangen (Rn 12 des EDSA-Berichts).

**WICHTIG**

*Der Datenschutzrahmen EU-USA enthält in Ziffer I.6. folgende Regelung: „Eine Organisation, die sich für eine Ausdehnung der Vorteile des Datenschutzrahmens EU-USA auf Personaldaten entscheidet, die im Rahmen eines Beschäftigungsverhältnisses aus der EU übermittelt werden, muss darauf hinweisen, wenn sie sich dem Ministerium gegenüber auf die Grundsätze verpflichtet, und sie muss die in den Zusatzgrundsätzen zur Selbstzertifizierung beschriebenen Anforderungen erfüllen."*

Die EU-Kommission vermutet, dass diese Möglichkeiten noch zu wenig bekannt sind, und setzt daher auf verstärkte Öffentlichkeitsarbeit (Ziffer 2.1.4 zweiter Absatz ihres Berichts). Nach Auffassung des EDSA wäre es geboten, dass die zuständigen US-Behörden, also unter anderem das DoC und die FTC, auch ohne besonderen Anlass Überprüfungen von Amts wegen durchführen (Rn 8 des EDSA-Berichts).

## Umstrittene Regelung für Personaldaten

Nach Auffassung der US-Behörden betrifft die Regelung für Personaldaten nur Situationen, in denen eine Unternehmensgruppe Daten von Beschäftigten „atlantikübergreifend" verarbeitet. Demgegenüber meint der EDSA, die Regelung betreffe schlicht alle Fälle, bei denen Daten von Beschäftigten aus der EU in die USA gelangen. Es ist nicht gelungen, diese Differenzen auszuräumen (ausführlich dazu Rn 17 des EDSA-Berichts).

Die US-Behörden führen die Zertifizierungen durch. Daher ist ihre Interpretation in der Praxis maßgeblich.

Die Zusatzgrundsätze gemäß Ziffer III.9 des Datenschutzrahmens EU-USA enthalten einschneidende Vorgaben. Daraus ergibt sich etwa die Pflicht, „bei Untersuchungen der in der EU jeweils zuständigen Behörden mitzuwirken und deren Empfehlungen zu befolgen", siehe Ziffer III.9 Buchst. d. Die Auswirkungen sind erheblich. Die Frage, für welche Verarbeitungssituationen die Sonderregelung für Personaldaten gilt, entscheidet nämlich darüber, wann solche erheblichen Pflichten zu beachten sind.

## Datenschutzgesetze der US-Bundesstaaten

20 der 50 US-Bundesstaaten haben inzwischen allgemeine Datenschutzgesetze verabschiedet. Acht dieser Gesetze sind bereits in Kraft getreten (Rn 20 des EDSA-Berichts).

Dies ist wichtig, weil sich die Existenz solcher Gesetze darauf auswirken kann, wie das US-Datenschutzniveau zu bewerten ist. Auf der anderen Seite erscheint die Wahrscheinlichkeit sehr gering, dass die US-Bundesebene ein allgemeines Datenschutzgesetz verabschiedet. Dort spielen vielmehr insbesondere im Sicherheitsbereich die „Executive Orders" des US-Präsidenten eine erhebliche Rolle (Nr. 2.1.5 des Berichts der EU-Kommission).

## Überwachungsbefugnisse der US-Geheimdienste bleiben

Sehr ausführlich stellen beide Berichte dar, dass die Überwachungsbefugnisse von US-Geheimdiensten im Evaluierungszeitraum uneingeschränkt fortbestehen. Dies gilt ungeachtet zahlreicher Änderungen von Details, die die Berichte ausführlich beschreiben (Ziffer 2.2 des Berichts der EU-Kommission sowie Rn 23-63 des EDSA-Berichts).

Hier könnte ein Knackpunkt bei einer etwaigen Überprüfung des Angemessenheitsbeschlusses durch den Europäischen Gerichtshof (EuGH) liegen.

**ONLINE-TIPP**

*Die im Artikel erwähnten Schriftstücke lassen sich auf folgenden Webseiten nachlesen:*

- *Gegenstand der Evaluierung ist der Durchführungsbeschluss (EU) 2023/1795 der Kommission vom 10.7.2023. Die deutsche Sprachfassung ist zu finden unter https://ogy.de/rttu.*
- *Beim Evaluierungsbericht der EU-Kommission handelt es sich um das Dokument COM (2024) 451 final vom 9.10.2024. Er befindet sich auch auf Deutsch unter https://ogy.de/upc7.*
- *Der Bericht des EDSA zu diesem Evaluierungsbericht (Version 1.1, angenommen am 4.11.2024) liegt nur auf Englisch vor auf der Webseite https://ogy.de/cgp2.*

Dr. Eugen Ehmann ist seit vielen Jahren umfassend aktiv als Autor, Referent und Moderator für Datenschutz in Behörden und Unternehmen.


Bild: iStock.com/bymuratdeniz

**Moderne CRM-Systeme arbeiten häufig KI-gestützt. Hier ist zu hinterfragen: Deckt die bestehende IT-Sicherheitsinfrastruktur alle Datensicherheitsrisiken ab, die dadurch entstehen können?**

### Neue Anwendungsfälle für die Datensicherheit

# Wenn sich KI im CRM versteckt

**Führt ein Unternehmen ein neues CRM-System ein, ist in vielen Fällen KI an Bord. Für die Datensicherheit des CRM bringt dies neue Fragestellungen mit sich. DSB müssen daher ihre Prüfkataloge erweitern.**

Für den Einsatz künstlicher Intelligenz (KI) im Customer Relationship Management (CRM) spricht eine Vielzahl von Vorteilen in einer ganzen Reihe von Anwendungsfällen:

- personalisierte E-Mails und Newsletter erstellen
- kundenspezifische Skripte für Akquise-Anrufe generieren
- passgenaue Antworten für Kunden in Chatbots
- sprachbasierte Suche nach Kundeninformationen im CRM-System
- Kundenhistorie automatisiert zusammenfassen
- KI-gestützte Bewertung von Leads
- Optimierung der Sales-Pipeline
- individuelle Vorschläge für das Upselling und Cross-Selling, also den Verkauf von Zusatzprodukten

Offensichtlich verarbeitet die KI dabei personenbezogene Daten der Kunden und Interessenten. Eine solche Datenverarbeitung war schon in klassischen CRM-Systemen der Fall (https://ogy.de/94ss). Doch durch KI kommen neue Risiken hinzu, auf die auch die Datensicherheit reagieren muss.

## Neue Datenrisiken bei CRM nicht vergessen

Datenschutzbeauftragte (DSB) sollten bei ihrer Risikobewertung eines neuen CRM-Systems auf die wahrscheinliche KI-Integration achten und entsprechend die folgenden Datenrisiken zusätzlich berücksichtigen:

- Grundsätzlich ist die Frage zu klären, wo die Daten gespeichert und verarbeitet werden. Viele KI-Dienste sind cloudbasiert und arbeiten nicht lokal. Selbst wenn das CRM-System intern auf eigenen Servern läuft, könnten die KI-Funktionen zusätzlich aus der Cloud kommen.
- Stammt das CRM-System aus der Cloud, ist die Wahrscheinlichkeit sehr hoch, dass auch die KI aus der Cloud kommt. Dabei ist es aber nicht sicher, dass es sich in beiden Fällen um die gleiche Cloud handelt. Das CRM-System könnte aus einer EU-Cloud stammen, während die KI getrennt davon in einer Cloud in einem Drittland läuft und sich als separater Dienst dazugesellt. Hier stellt sich die Frage nach dem Datenschutzniveau der KI-Cloud.
- Neben den Berechtigungen und Rollen der menschlichen Nutzer des CRM-Systems gilt es auch, die Zugriffsmöglichkeiten der KI-Dienste zu hinterfragen.
- Neben den Kundendaten sind auch die personenbezogenen Ergebnisse der KI-Dienste zu schützten. Es stellt sich hierbei die Frage, wo diese gespeichert sind und wer auf die Ergebnisse zugreifen kann.

**WICHTIG**

***Datenschutzbeauftragte sollten sich bewusst sein, dass die Einführung neuer CRM-Lösungen zu neuen Risiken und zusätzlich erforderlichen Schutzmaßnahmen führen kann, die über jene klassischer CRM-Lösungen hinausgehen. Es muss das Bewusstsein vorhanden sein, dass die Einführung eines CRM auch den Einzug von KI ins Unternehmen mit sich bringen kann. Hierzu gilt es auch den Einkauf, die IT-Abteilung, den Vertrieb und das Management zu sensibilisieren, nicht nur die CRM-Nutzerinnen und -Nutzer. Zusammen mit der Security-Abteilung ist zu klären, ob die vorhandene Security auch Zugriffe von und auf KI überwachen und Anomalien in diesem Bereich erkennen und beantworten kann. Oftmals besteht konkreter Handlungsbedarf, um neue KI-Funktionen in das Security-Konzept einzufügen.***

## KI-Einsatz erfordert erweiterte Sicherheitsfunktionen

Um die zusätzlichen Risiken durch die KI-Unterstützung in den CRM-Systemen zu minimieren, geht es darum, möglichst viel Transparenz in die Aktivitäten der KI zu bekommen. Ebenso muss klar zu erkennen sein, wie die KI-Dienste zum Einsatz kommen, also zu welchen Zwecken und Zielen die Analyse der Daten erfolgt.

Doch nicht nur die vorgesehenen KI-Aktionen und der geplante KI-Einsatz durch die Mitarbeitenden müssen im Security-Konzept für die CRM-Einführung abgebildet sein. Auch ungewollte oder bösartige Zugriffe auf die KI und Aktivitäten mit der KI stellen große Risiken dar. Deshalb gilt es, Anomalien wie z.B. ungewöhnliche Aktivitäten rund um die KI im CRM-System aufzuspüren und darauf zu reagieren.

## Integrierter oder zusätzlicher Schutz für die KI

Bei modernen, KI-basierten CRM-Lösungen sollte man zum einen Maßnahmen der Datensicherheit wie Security-Schulungen für die Nutzenden erweitern, um dort auf die KI-Risiken hinzuweisen. Ebenso sind umfassende Informationen über die KI-Dienste im CRM einzuholen: mit welchen KI-Modellen von welchem Anbieter zu welchem Zweck auf welche personenbezogenen Daten Zugriff erfolgt.

## Neue Prüfungen bei KI-unterstützten CRM-Systemen

| Prüfpunkt | Ja | Nein |
|---|---|---|
| Einholung von Informationen über die KI-Dienste im geplanten CRM | ☐ | ☐ |
| Berechtigungs- und Zugriffsmanagement: Berücksichtigt die Zugriffe auf die KI-Funktionen und durch die KI-Dienste im CRM | ☐ | ☐ |
| Monitoring-Lösungen: KI-Dienste im CRM abdecken und überwachen, Anomalien aufdecken | ☐ | ☐ |
| Funktionen zur Verschlüsselung, Anonymisierung, Maskierung und zum Löschen der Daten gelten sowohl für die Kundendaten als auch für die Resultate der KI-Dienste im CRM | ☐ | ☐ |
| Security-Schulungen für die Nutzenden des CRM erweitert um das Thema Risiken durch KI | ☐ | ☐ |
| Sensibilisierung auch des Managements über die Folgen einer KI-Unterstützung im CRM | ☐ | ☐ |

**Zusätzliche Datenschutzprüfungen bei KI-basierten CRM-Lösungen. Die Checkliste finden Sie online unter www.datenschutz-praxis.de/datenschutzbeauftragte/checkliste-crm-ki.**

Bestehende Lösungen für das Berechtigungs- und Zugriffsmanagement müssen auch Zugriffe auf die KI-Funktionen und durch die KI-Dienste selbst abbilden können. Monitoring-Lösungen müssen ebenfalls die KI-Dienste abdecken und überwachen, um Anomalien erkennen zu können.

Funktionen zur Verschlüsselung, Anonymisierung, Maskierung und für das Löschen der Daten müssen auch die Resultate der KI-Dienste berücksichtigen. Dies gilt also nicht nur die Kundendaten selbst, welche die KI verarbeitet.

Bevor man ein CRM-System implementiert, ist zu klären, welche Sicherheitsfunktionen es mitbringt und welche man zusätzlich benötigt. Mitunter erkennen z.B. vorhandene Lösungen für das Berechtigungsmanagement „KI-Agenten" nicht als Identität, deren Berechtigungen zu regeln sind. Es kann also sein, dass man für ein neues CRM bestehende Security-Lösungen erweitern oder gar ersetzen muss.

Oliver Schonschek, Dipl.-Phys., ist News Analyst mit Fokus auf IT-Sicherheit und Datenschutz und Co-Host von Datenschutz PRAXIS Der Podcast. Er wurde bereits mehrfach als Top 10 Global Thought Leader für Privacy, Security und Cybersecurity ausgezeichnet.

IMPRESSUM

**Verlag:**
WEKA Media GmbH & Co. KG
Römerstraße 4, 86438 Kissing
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
Website: www.weka.de

**Herausgeber:**
WEKA Media GmbH & Co. KG
Gesellschafter der WEKA Media GmbH & Co. KG sind als Kommanditistin: WEKA Business Information GmbH & Co. KG und als Komplementärin: WEKA Media Beteiligungs-GmbH

**Geschäftsführer:**
Jochen Hortschansky, Kurt Skupin

**Redaktion:**
Ricarda Veidt, M.A. (V.i.S.d.P.)
E-Mail: ricarda.veidt@weka.de
Natalie Ziebolz
Andreas Dumont, München
Dr. Wilhelm Greiner, Mitteilerei, Kinding

**Anzeigen:**
Jana Popp
Telefon: 0 82 33.23-72 62
Fax: 0 82 33.23-5 72 62
E-Mail: jana.popp@weka.de

**Erscheinungsweise:**
Zwölfmal pro Jahr

**Aboverwaltung:**
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
E-Mail: service@weka.de

**Abonnementpreis:**
12 Ausgaben Print + Online-Zugriff 289 € (zzgl. MwSt. und Versandkosten)
12 Ausgaben als PDF im Heftarchiv + Online-Zugriff 279 € (zzgl. MwSt.)

**Druck:**
Burscheid Medien GmbH
Leonhardstraße 23, 88471 Laupheim

**Layout & Satz:**
METAMEDIEN
Spitzstraße 31, 89331 Burgau

**Bestell-Nr.:**
09100-4133

**ISSN:**
1614-6867

**Bestellung unter:**
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
www.datenschutz-praxis.de

**Haftung:**
Die WEKA Media GmbH & Co. KG ist bemüht, ihre Produkte jeweils nach neuesten Erkenntnissen zu erstellen. Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert. Erfüllungsort und Gerichtsstand ist Kissing.


Maximale Datenunsicherheit

# Der Hausmeister als Sicherheits-Chef

**Ein Kunde legt großen Wert auf Datensicherheit. „Nur bei uns sind die Daten sicher", so die Devise vom Boss. „Unser Hausmeister sorgt dafür, dass die Daten bei uns sicherer sind als in irgendeiner Cloud." Auch wenn ich ihm verdeutliche, dass die betrieblichen Smartphones längst Daten in die Cloud schicken – die Überzeugung des Chefs ist nicht zu erschüttern.**

Es kommt der Tag der Begehung. Zuerst der nicht verschlossene Technikraum. Neben Hausechnik und IT stehen dort Putzmittel und Reinigungsgeräte. Der Hausmeister – gern auch „Facility Manager" genannt – klärt uns auf: „So können die Reinigungskräfte immer arbeiten." Das Schlüsselbrett an der Wand mit diversen Schlüsseln? „Die Reinigungstruppe braucht die", sagt der Meister aller Schlüssel beiläufig. Datenschutz? Ich notiere die Antwort für den Bericht.

Wir kommen zum Serverraum, laut Geschäftsleitung der Hochsicherheitstrakt des Unternehmens. Heute ist der IT-Leiter nicht da. „Der gibt den Schlüssel für den Serverraum niemals raus", erklärt der Datenschutzkoordinator.

Am Serverraum angekommen, fragt der Facility Manager: „Haben Sie den Schlüssel?" Der Datenschutzkoordinator schüttelt den Kopf. „Nein, der ITler ist krank." „Kein Problem", sagt der Facility Manager und verschwindet um die Ecke.

Gleich darauf ist er wieder da. „Hier ist der Schlüssel. Der hängt im Technikraum am Schlüsselbrett", berichtet er lapidar. „Die Reinigungskräfte müssen ja auch den Serverraum putzen." Ich staune. Der Serverraumschlüssel hängt frei zugänglich in einem unverschlossenen Raum? Gut, da ist ja noch der PIN-Code. „Den habe ich", äußert der Facility Manager selbstbewusst. „Ich bin ja verantwortlich für die Schließanlage." Und tippt an der Tastatur leicht sichtbar die PIN „6666" ein. Sehr schön, diese PIN vergisst man sicher nicht so leicht!

„Nur bei uns sind die Daten sicher" – in einer ganz eigenen Interpretation des pragmatischsten aller Hausmeister! Dennoch wird er mir mit seiner unerschütterlichen Selbstsicherheit fehlen, wenn er nächstes Jahr in Rente geht …

Eberhard Häcker ist seit vielen Jahren selbstständig und mit großer Leidenschaft sowie Kreativität externer Datenschutzbeauftragter.

## In der nächsten Ausgabe

### Auskunftsersuchen

Das Auskunftsrecht der DSGVO ist zentral, aber nicht unbegrenzt. Nutzen Sie die Begrenzungsmöglichkeiten!

### Einmalanmeldungen

Single Sign On vereinfacht die Authentifizierung. Integrierte Funktionen erfordern aber zusätzliche Datenschutzprüfungen.

### Auftragsverarbeitung

Welche Inhalte sind für einen Vertrag zur Auftragsverarbeitung zwingend erforderlich und welche optional? Ein Überblick.