DATENSCHUTZAKTUELL Professional
NOV I 2025
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

ALLES FAKE: SENSIBILISIEREN SIE FÜR PHISHING & CO.

IHRE TÄTIGKEIT
Ihr Job endet demnächst? So haben Sie einen guten Abgang 3

KONTROLLE
Organisatorisches Versagen: Prüfen Sie diese 7 Hotspots 6

Finden Sie Antworten gemeinsam

Liebe Leserin, lieber Leser,

Sie kennen das bestimmt: Man hat eine Frage zum Datenschutz und Sie sollen die perfekte Lösung liefern. Es mag zwar kein falsches Vorgehen sein, wenn Sie sich dementsprechend an die Erarbeitung der Lösung machen. Doch warum sollte das allein Ihr Ding sein? Ist es eben nicht!

Nehmen Sie andere für das Erarbeiten der Lösung mit ins Boot. Erklären Sie die relevanten Rahmenbedingungen im Datenschutz und lassen Sie die Kollegen zur Lösung beitragen. Das entlastet nicht nur Sie. Sie finden so Lösungen, über die sich später niemand beschweren kann. Schließlich hat man daran mitgearbeitet.

Viele Grüße

Andreas Würtz,
Rechtsanwalt und Chefredakteur

Ihr Experte für Datenschutz
Andreas Würtz verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz pragmatisch umsetzen lässt.

Inhalt

Datenschutz organisieren
Schutz Ihres Unternehmens: Machen Sie den Check
Seiten 1–2

Datenschutzbeauftragter
Ihr Job endet demnächst? So haben Sie einen guten Abgang
Seite 3

Sensibilisierung
Alles Fake: Sensibilisieren Sie für Phishing & Co.
Seiten 4–5

Kontrolle
Organisatorisches Versagen: Prüfen Sie diese 7 Hotspots
Seite 6

Fragen an die Redaktion
Wie geht man am besten mit unterschiedlichen Auffassungen um?
Seite 7

Genießt auch der Stellvertreter Kündigungsschutz?
Seite 7

Rechtsprechung
EuGH: Pseudonyme Daten können auch anonym sein
Seite 8

Zum neuen Onlinebereich!
www.privacyxperts.de/login

Expertensprechstunde:
https://t1p.de/andreas-wuertz

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Bonn

V.i.S.d.P.: Michael Jodda (Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | Anwesha Dey; Seite 1: Adobe Stock | brokglas

Erscheinungsweise: 26-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Sorgen Sie jetzt vor – mit unserem Sicherheits-Check.

Schutz Ihres Unternehmens: Machen Sie den Check

Aktuell sind wir schon mittendrin in der „dunklen Jahreszeit". Und damit ist Hochsaison für Einbrecher, Saboteure und Spione. Schließlich geht im Dunklen vieles einfach besser. Werden Technik, Computer oder Datenträger entwendet, sind regelmäßig auch personenbezogene Daten betroffen. Also liegt für Sie die Frage auf der Hand: Wie steht es um die Sicherheit?

Blinde Flecken darf es nicht geben

Klar ist: Das Risiko, Opfer von Cyberkriminellen zu werden, steigt für jedes Unternehmen zusehends. Kein Wunder also, dass man in vielen Unternehmen hier mit Gegenmaßnahmen besonders aktiv ist.

Aber wer sich nur auf dieses Risiko fokussiert, verliert schnell andere Risiken aus dem Blick. Und die gibt es natürlich zuhauf. Da wäre nicht nur der klassische Einbrecher, der es auf alles abgesehen hat, was sich leicht zu Geld machen lässt. Daneben gibt es auch diejenigen, die es auf Know-how oder Daten abgesehen haben oder als Saboteure einfach nur Schaden in Ihrem Unternehmen anrichten wollen. Auch hiergegen muss sich Ihr Unternehmen wappnen.

Machen Sie das Datenschutzrisiko klar

Wollen Sie sich einmal anschauen, wie es um grundlegende Schutzmaßnahmen rund um Grundstück, Gelände oder Gebäude steht, hören Sie vielleicht, dass Sie das gerne anderen überlassen können. Hier sollten Sie nicht gleich aufgeben. Zeigen Sie auf, dass grundlegende Schutzmaßnahmen wie eine Zutrittskontrolleinrichtung oder ein Einbruchmeldesystem auch Schutzmaßnahmen sind, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten.

Doch es geht nicht nur um risikoangemessenen Schutz im Sinne von Art. 32 Datenschutz-Grundverordnung (DSGVO). Passen die Schutzmaßnahmen nicht und kommt es zum Diebstahl von Computern oder Unterlagen, gibt es schnell ein größeres Problem: Es liegt eine Datenpanne vor, sprich eine Verletzung des Schutzes personenbezogener Daten. Und die muss unter Umständen der Datenschutzaufsichtsbehörde gemeldet werden (Art. 33 DSGVO). Bei einem hohen Risiko für die Betroffenen müssen diese zusätzlich informiert werden (Art. 34 DSGVO).

Prüfen Sie, was Sache ist

Als Profi wissen Sie: Es ist keine Option, einfach zu vermuten, dass ggf. andere sich um ein Thema kümmern werden oder irgendwie schon alles passen wird. Daher: Machen Sie als Datenschutzbeauftragter den Check. Dabei sollten Sie systematisch vorgehen:

- **Starten Sie mit einer Risikoanalyse:** Bewerten Sie mögliche Gefahren und leiten Sie daraus unter Betrachtung von möglichem Schaden und Eintrittswahrscheinlichkeit die Risiken ab.
- **Identifizieren Sie die notwendigen Maßnahmen**: Damit ist das Soll erfasst.
- **Bewerten Sie den Istzustand:** Erfassen Sie, was an Maßnahmen umgesetzt ist.
- **Stellen Sie Schwachstellen und Defizite fest:** Gleichen Sie das Ist mit dem Soll ab. Dokumentieren Sie die Abweichungen.
- **Leiten Sie nötige Maßnahmen ab:** Zeigen Sie auf, was zur Behebung der Defizite nötig ist.
- **Begleiten Sie die Umsetzung:** Beraten Sie im Rahmen Ihrer Aufgaben

Sie wollen sich ein Bild von der Situation machen? Für eine Kontrolle grundlegender Aspekte können Sie die folgende Checkliste einsetzen.

Checkliste: Prüfung grundlegender Sicherheitsmaßnahmen

Prüfschwerpunkte	Das ist wichtig	Okay?
Regelwerke	❯ Prüfen Sie, welche relevanten Festlegungen es zu sicherheitsrelevanten Aspekten gibt. Gemeint sind insbesondere Sicherheitskonzepte. Werfen Sie hier auch einen Blick auf die letzte Überarbeitung. Liegt diese lange zurück, kann das schon darauf hindeuten, dass manches veraltet ist, etwa Zuständigkeiten. ❯ Haben Sie auch ein Auge auf relevante Betriebsvereinbarungen, beispielsweise zur Zutrittskontrolle oder zur Videoüberwachung. Diese können umfassende Vorgaben zur Umsetzung und zum erlaubten Einsatz von Systemen machen. Prüfen Sie, inwieweit die Vorgaben aus Betriebsvereinbarungen zu den Regelwerken passen.	○ Ja ○ Nein
Dokumentation	❯ Für Sicherheitsmaßnahmen sind in der Regel Konzepte oder Betriebshandbücher unerlässlich. Diese enthalten oft auch Vorgaben zu Prozessen und einzubindenden Stellen. ❯ Prüfen Sie auch hier auf Aktualität und Vollständigkeit. ❯ Schauen Sie zudem ins Verzeichnis von Verarbeitungstätigkeiten. Sind personenbezogene Daten im Spiel, müssen auch bei Sicherheitsmaßnahmen entsprechende Verarbeitungstätigkeiten im Verzeichnis nach Art. 30 Abs. 1 DSGVO enthalten sein.	○ Ja ○ Nein
Vertragliche Regelungen	❯ Hier können Sie den Fokus auf (Sicherheits-)Dienstleister oder Auftragsverarbeiter legen. Schauen Sie, was zum Datenschutz vereinbart wurde. ❯ Bewerten Sie die Rollen der Beteiligten. Es kann passieren, dass man sich dazu keine Gedanken macht, weil man nur die Dienstleistung im Bereich Sicherheit sieht und das Verarbeiten personenbezogener Daten übersieht.	○ Ja ○ Nein
Qualifikation zuständiger Mitarbeiter	❯ Systeme müssen bedient werden. So z. B. die Videoüberwachung, ein Besuchermanagementsystem oder die Zutrittskontrolleinrichtung. Die zuständigen Mitarbeiter sollten über die nötige Qualifikation verfügen. ❯ Hinterfragen Sie die Qualifikation im Datenschutz. Die von den betreffenden Mitarbeitern verarbeiteten Daten unterliegen regelmäßig einer strengen Zweckbindung. Also sollten die Mitarbeiter über spezifische Grundlagenkenntnisse im Datenschutz verfügen.	○ Ja ○ Nein
Allgemeine Sensibilisierung	❯ Auch dem Otto-Normal-Mitarbeiter müssen Basics zur Sicherheit vermittelt werden. Die beste Zutrittskontrolle bringt nichts, wenn ein unvorsichtiger Mitarbeiter dem Unbefugten die Tür aufhält. ❯ Schauen Sie sich Materialien und Konzepte an. Klären Sie, wie man sicherstellt, dass kein Mitarbeiter durchrutscht.	○ Ja ○ Nein
Physische Absicherung von Grundstück, Gelände und Gebäuden	❯ Kontrollieren Sie Zäune, Tore, Außentüren und Fenster. Diese sollten zu einem angemessenen Sicherheitsniveau beitragen und nicht nur „Fassade" sein. ❯ Idealerweise machen Sie eine Begehung. Zudem bietet sich ein Check zu Zeiten an, bei denen eigentlich niemand mehr da ist. Testen Sie hier auch, inwieweit Türen und Fenster tatsächlich verschlossen sind oder Zutrittskarten außerhalb der Regelarbeitszeiten nicht mehr funktionieren.	○ Ja ○ Nein
Umgebungssicherheit	❯ Haben Sie auch ein Auge auf die Umgebung Ihres Unternehmens. Auch dort können Risiken lauern, die etwa unter dem Aspekt „Verfügbarkeit" ein Problem für den Datenschutz sein können. ❯ Schauen Sie insbesondere nach grundlegenden Risiken, etwa eine erhöhte Gefahr für Feuer oder Hochwasser. Ist der Server Ihres Unternehmens im Keller, kann der bei Hochwasser schlimmstenfalls auch unter Wasser stehen.	○ Ja ○ Nein
Zutrittskontrolleinrichtungen	❯ Bewerten Sie die Zugangsregelungen zu Grundstück, Gebäuden und kritischen Bereichen. ❯ Klären Sie insbesondere, inwieweit verlorene Zutrittsmittel (z. B. Chipkarten) gesperrt werden oder der Zutritt bei Beschäftigungsende schnell entzogen wird.	○ Ja ○ Nein
Einbruchmeldetechnik	❯ Prüfen Sie die Dokumentation. Besprechen Sie zudem, wann die Anlage zuletzt gewartet bzw. getestet wurde. ❯ Klären Sie auch die Prozesse. Eine Meldung darf nicht ins Leere laufen.	○ Ja ○ Nein
Videoüberwachung	❯ Diese muss funktionieren. Machen Sie die Sichtprüfung. Nicht selten ist die Funktion durch verschmutzte Linsen oder verstellte Kameras erheblich beeinträchtigt. ❯ Prüfen Sie das System auch unter Datenschutzaspekten. Klären Sie vor allem die Speicherdauer der aufgezeichneten Videos. Mehr als 72 Stunden sollte man gut begründen können. Lassen Sie sich auch schildern, in welchen Fällen auf Bildmaterial zugegriffen wird und wie hier die Zulässigkeit eines Zugriffs bzw. der Weitergabe geprüft wird.	○ Ja ○ Nein
Besondere Sicherung besonderer Bereiche	❯ Es gibt in jedem Unternehmen Bereiche, die nicht für jedermann gedacht sind. Typischerweise sind hier der Serverraum, ein Aktenarchiv oder die Aufbewahrung von Datensicherungen zu nennen. Lassen Sie sich erläutern, wie man dem besonderen Schutzbedarf nachkommt. ❯ Machen Sie die Probe aufs Exempel. Prüfen Sie, ob die Sicherheitsmaßnahmen das halten, was man Ihnen versprochen hat.	○ Ja ○ Nein
Aufbewahrung, Löschung und Entsorgung von Schutzwürdigem	❯ Das betrifft beispielsweise die Aufbewahrung von Zutrittsmitteln (insbesondere Schlüssel, Chipkarten) am Empfang. Schauen Sie sich an, wo man Entsprechendes sicher verwahrt. ❯ Auch im Unternehmen gibt es besonders Schutzwürdiges, etwa Akten oder Datenträger. Prüfen Sie hier die spezifischen Schutzmaßnahmen.	○ Ja ○ Nein

Ihr Job endet demnächst? So haben Sie einen guten Abgang

Vielleicht ist es demnächst bei Ihnen so weit: Sie gehen in den verdienten Ruhestand oder Sie übernehmen eine ganz andere Aufgabe im Unternehmen. Klar ist in beiden Fällen: Das Ende Ihrer Tätigkeit ist absehbar. Doch einfach alles stehen und liegen lassen ist für Sie keine Option. Stil und Professionalität sollten Sie auch am Ende Ihrer Tätigkeit beweisen.

Machen Sie es Ihrem Nachfolger leichter

Auf Ihren Nachfolger kommt viel Neues zu. Daher sollten Sie ihn tatkräftig unterstützen und ihm das Zurechtfinden erleichtern. Ihr Wissen, Ihre Erfahrungswerte und ganz speziellen Tipps sind Gold wert.

Damit Sie hier keine wichtige Erledigung, sprich kein To-do, vergessen, können Sie auf diese Checkliste setzen.

To-do	Wichtige Aspekte	Erledigt?
Wichtige Beratungen abschließen	› Bei wichtigen Vorhaben oder Beratungen sollten Sie dafür sorgen, dass die Kollegen durch den Wechsel nicht ausgebremst werden. Geben Sie ggf. eine schriftliche Einschätzung. › Ist eine abschließende Stellungnahme nicht möglich, sollten Sie den Zwischenstand festhalten.	○ Ja ○ Nein
Beratungs-dokumentation vervollständigen	› Dokumentieren Sie den Beratungsstand bei allen noch nicht abgeschlossenen Fragen oder Beratungen so, dass sich ein Nachfolger leicht zurechtfindet. › Nehmen Sie idealerweise bei den offenen Beratungen eine Priorisierung nach Wichtigkeit und Dringlichkeit vor.	○ Ja ○ Nein
Risikoübersicht zusammenstellen	› Machen Sie eine Analyse, wo Sie als bisheriger Datenschutzbeauftragter die Gefahren und Risiken im Datenschutz sehen. Schätzen Sie ein, wo aus Ihrer Sicht der größte Handlungsdruck besteht. › Vergessen Sie keine „Baustellen", auch nicht solche, die weniger mit den Kernaspekten des Datenschutzes zu tun haben. Das können auch organisatorische Themen sein.	○ Ja ○ Nein
Offene-Punkte-Liste erstellen	› Listen Sie alle Punkte auf, die unerledigt sind. Es gebietet die Fairness, dass Sie keine Problemfelder unter den Tisch fallen lassen. › Kategorisieren Sie die Einträge, beispielsweise nach typischen Überbegriffen wie „Organisatorisches", „Schulungen", „Beratung", „Unternehmensleitung".	○ Ja ○ Nein
Handbuch für den Nachfolger erarbeiten	› Stellen Sie alles Relevante und Wissenswerte für den Nachfolger in einer Art Handbuch zusammen. Das erleichtert es ihm erheblich, sich zurechtzufinden. › Führen Sie das Handbuch nach Möglichkeit elektronisch. Referenzen und Links funktionieren dann problemlos. › Denken Sie auch an eine Übersicht mit wichtigen Ansprechpartnern, Prozessen oder internen Festlegungen.	○ Ja ○ Nein
E-Mail-Postfach bereinigen	› Bereinigen Sie Ihr Postfach. Exportieren Sie alle relevanten E-Mails in eine Postfachdatei, die Sie Ihrem Nachfolger übergeben können. › Passen Sie zum Wechsel die Berechtigungen für Funktionspostfächer an.	○ Ja ○ Nein
Abschluss-gespräche führen	› Garantiert hatten Sie wichtige Ansprechpartner oder Unterstützer. Besprechen Sie rechtzeitig mit diesen, ob es im Vorfeld noch Themen gibt, die Sie in Angriff nehmen sollten. › Nutzen Sie die Gelegenheit, um sich bei Ihren Wegbegleitern zu bedanken. Persönlicher Dank ist am besten.	○ Ja ○ Nein
Nicht mehr Erforderliches bzw. Relevantes entsorgen	› Im Laufe Ihrer Tätigkeit hat sich garantiert viel angesammelt. So manches ist inzwischen veraltet oder ohne Relevanz. Ersparen Sie Ihrem Nachfolger, sich durch einen Berg an Informationen oder Unterlagen arbeiten zu müssen. Was weg kann, sollte auch weg. › Achten Sie auf eine sachgemäße Entsorgung. Bei Schützenswertem muss der Datenschutz gewahrt werden.	○ Ja ○ Nein
Arbeitsplatz und Archiv bereinigen	› Räumen Sie Ihren Arbeitsplatz auf und hinterlassen Sie diesen so, dass er eine gute Visitenkarte für Sie abgibt. Sieht es aus wie bei „Hempels unterm Sofa", wirft das kein gutes Licht auf Sie. › Prüfen Sie auch Aktenschränke oder Archivräume. Sortieren Sie dort aus, was keine Relevanz mehr hat.	○ Ja ○ Nein
Tätigkeitsbericht erstellen	› Damit können Sie einen guten Abschluss machen und zugleich das Ende Ihres Amts in ein positives Licht rücken. › Ziehen Sie Ihre Bilanz, idealerweise im positiven Sinn. Heben Sie hervor, was erreicht wurde und was Sie bewegt haben.	○ Ja ○ Nein
Abschied durchführen	› Das kann eine kleine Abschiedstour im Unternehmen genauso umfassen wie eine kleine Feier. Sparen Sie hier nicht zu sehr. Man wird Sie dann besser in Erinnerung halten. › Denken Sie unbedingt an eine Abschieds-E-Mail. Verschicken Sie diese nicht auf den letzten Drücker. Vielleicht will man Ihnen noch antworten.	○ Ja ○ Nein
Berechtigungen abgeben	› Prüfen Sie, welche Berechtigungen Sie nicht mehr benötigen bzw. welche der Nachfolger braucht. › Beantragen Sie rechtzeitig die Anpassung.	○ Ja ○ Nein

Alles Fake: Sensibilisieren Sie für Phishing & Co.

Künstliche Intelligenz (KI) ist als Trendthema Nummer eins in aller Munde. Kaum ein Unternehmen, das sich nicht damit beschäftigt. Doch wo viel Licht ist, ist auch viel Schatten. Cyberkriminelle setzen immer mehr auf die Möglichkeiten, die KI bietet. Phishing wird zunehmend perfekter. Damit Mitarbeiter gut gerüstet sind, sollten Sie sensibilisieren.

Know-how ist unerlässlich

Die Mitarbeiter werden schon Bescheid wissen – denkt Ihre Unternehmensleitung so, dann ist es nur eine Frage der Zeit, bis es zum großen Schaden kommt. Vielmehr ist eine solche Denke grob fahrlässig. Ihr Unternehmen muss alles daransetzen, die Beschäftigten mit dem relevanten Wissen auszustatten, das sie im Fall der Fälle brauchen.

Neue Herausforderungen durch KI

Natürlich versuchen Cyberkriminelle, ganz klassisch an sensible Informationen zu kommen oder Zahlungen zu veranlassen. Dementsprechend sind auch die klassischen Erkennungsmerkmale weiterhin relevant. So z. B.:

- unpersönliche, unpassende oder falsche Anrede
- gefälschte Absender- oder Linkadressen unter Verwendung von Buchstaben oder Zahlendrehern
- Aufbau von Handlungsdruck, nach dem Schema „Ihr Konto wird sofort gesperrt"

Allerdings bietet KI Cyberkriminellen ganz neue Möglichkeiten, Menschen und damit auch die Beschäftigten Ihres Unternehmens in die Falle zu locken. So wird KI eingesetzt, um

- täuschend echte Fälschungen von E-Mails, Schreiben oder Webseiten zu erstellen,
- das Opfer zu analysieren und typische Schwachpunkte zu finden,
- Stimmen und Nachrichten zu fälschen, um z. B. Forderungen des falschen Chefs echt wirken zu lassen,
- SMS und Messenger-Nachrichten so zu gestalten, dass diese tatsächlich vom echten Absender zu stammen scheinen.

Cyberkriminelle entdecken den Brief für sich

Die Leichtgläubigkeit und Täuschbarkeit von Menschen ausnutzen – darauf setzen Cyberkriminelle besonders. Und das klappt besonders gut mit Schreiben, die anscheinend von Behörden stammen oder die klassisch per Post verschickt werden. Wirkt das Schreiben oder etwa eine Rechnung echt, denkt mancher Mitarbeiter nicht lange nach. Das, was gefordert wird, wird ohne Umwege umgesetzt.

Mancher vertrauensselige Mensch macht das nicht anders, wenn es um QR-Codes geht. Die werden inzwischen ebenfalls gerne gefälscht und über die echten QR-Codes an Ladesäulen geklebt. Das Ziel: Die Opfer werden zur Eingabe von Kreditkartendaten auf gefälschten Seiten von Stromanbietern verleitet.

Sensibilisieren Sie auf die Schnelle

Sprechen Sie etwa mit der IT-Abteilung, dem Finanzbereich oder den zuständigen Kollegen im Bereich Cybersecurity, inwieweit sie aktuelle Beispiele für neue Vorgehensweisen von Cyberkriminellen haben. Passen Sie dann das nachfolgende Muster so an, dass dieses auf Ihr Unternehmen zugeschnitten ist und die spezifischen Vorfälle berücksichtigt.

Sorgen Sie für Abwechslung

Damit die Mitarbeiter mit dem nötigen Wissen versorgt werden, muss es nicht immer eine E-Mail sein. Denken Sie auch an einen Artikel im Intranet. Hier haben Sie meist viel mehr Platz, um etwa auch echte Beispiele aus dem Unternehmen unterzubringen. Alternativ können Sie auch eine kurze virtuelle Schulung oder Sprechstunde anbieten. Das kann im Ergebnis nachhaltiger wirken, gerade wenn individuelle Fragen beantwortet werden können.

Schauen Sie auch auf das Drumherum

Dass Cyberkriminelle sich immer wieder etwas Neues einfallen lassen und dass die Mitarbeiter sensibilisiert werden müssen, damit sie darauf nicht hereinfallen, ist eine Sache. Eine andere Sache ist, dass Ihr Unternehmen passende Anlaufstellen und Prozesse hat, um im Fall der Fälle schnell und professionell mit einem entsprechenden Vorfall umgehen zu können. Denn die beste Hotline bringt nichts, wenn dort ständig besetzt ist oder eine Bandansage läuft. Prüfen Sie daher im Rahmen Ihrer Aufgaben auch folgende Aspekte:

- **Regelungen:** Bestehen klar kommunizierte Anweisungen für die Mitarbeiter, wie diese bei einem Vorfall reagieren müssen? Nur wenn bekannt ist, was zu tun ist, besteht eine erhöhte Wahrscheinlichkeit, dass entsprechend gehandelt wird.
- **Meldewege:** Bestehen niederschwellige Möglichkeiten, Vorfälle zu melden oder speziellen Rat einzuholen, etwa bei der Hotline eines Cybersecurity-Teams? Es den Mitarbeitern leicht zu machen kann entscheidend sein. Komplizierte Formulare wirken eher abschreckend. Besser sind E-Mail, Telefon oder ein Chat mit direktem Kontakt zu den Spezialisten.
- **Erreichbarkeit:** Wenn etwas schiefgeht, muss schnell gehandelt werden. Sind die Kontaktmöglichkeiten oder Spezialisten auch zu Randzeiten oder am Wochenende verfügbar?

Muster: Phishing-Sensibilisierung für Mitarbeiter

Gehen Sie Cyberkriminellen nicht auf den Leim

Liebe Kolleginnen und Kollegen,

Cyberkriminelle haben es auf unser Unternehmen und auf Sie als Mitarbeiter abgesehen. Wichtig ist es also, dass Sie den Cyberkriminellen nicht auf den Leim gehen und nicht in die Phishing-Falle tappen. Das gelingt Ihnen, indem Sie vor allem die Hinweise in diesem Schreiben beachten.

Was mit Phishing gemeint ist, wissen Sie bestimmt. Das sind Versuche von Cyberkriminellen, mit gefälschten E-Mails, Nachrichten, SMS, Briefen oder Anrufen an sensible Daten zu gelangen. Oder: Man will Sie zu einem Verhalten oder Handeln veranlassen, das den Kriminellen ihre weiteren Machenschaften ermöglicht, etwa den Diebstahl oder das Verschlüsseln von Daten.

Auch Cyberkriminelle finden KI super

Künstliche Intelligenz (KI) macht nicht nur Ihr Leben leichter – das Potenzial von KI sehen und nutzen auch Cyberkriminelle. So setzen sie darauf, um täuschend echte E-Mails zu erstellen, die nicht nur personalisiert sind und ohne Rechtschreib- und Grammatikfehler daherkommen. Mit den entsprechenden Bild- und Audiogeneratoren werden Deepfakes erstellt, also Stimmen, Bilder oder Videos von Entscheidungsträgern oder Vertrauenspersonen nachgeahmt. Wer nicht genau hinschaut, merkt ggf. nicht, dass die Nachricht oder das Video gerade nicht vom Geschäftsführer oder Verhandlungspartner stammt.

KI hilft zudem dabei, Prozesse zu automatisieren, auch bei Cyberkriminellen. So werden echte Webseiten kopiert, um die Kopie so zu manipulieren, dass Opfer darauf hereinfallen und etwa sensible Anmeldedaten oder Kreditkarteninformationen eingeben.

Vorsicht vor derzeit aktuellen Maschen

Cyberkriminelle schlafen nicht und sie kommen immer wieder auf neue Ideen. So z. B.:

- **Behördenschreiben:** *Zwar ist die Masche nicht neu. Allerdings ist die Täuschung zunehmend perfekt. So passen nicht nur Aussehen und Inhalt auf den ersten Blick. Solche Fake-Behördenbriefe werden nicht nur per E-Mail, sondern auch per Briefpost verschickt. Seien Sie also auf der Hut, wenn Behörden (z. B. Statistikämter, Finanzämter, Bundeskriminalamt) etwas von unserem Unternehmen oder Ihnen wollen. Lassen Sie sich nicht irritieren, nur weil etwas amtlich daherkommt oder per Post verschickt wird. Auch wenn direkt mit einem Bußgeld gedroht wird, sollten Sie nichts überstürzen. Hinterfragen Sie das Anliegen und stimmen Sie sich mit Kollegen und Vorgesetzten ab.*
- **Geheimhaltung:** *Heißt es, dass man nur Sie ins Vertrauen zieht und Sie niemandem etwas erzählen dürfen, heißt es Stopp. Ignorieren Sie das. Sie können sich immer mit dem Vorgesetzten abstimmen.*
- **Anhänge von Fremden:** *Kennen Sie den Absender nicht und sind Anhänge enthalten, ist besondere Vorsicht geboten. Sprechen Sie im Zweifel vorab mit dem Vorgesetzten oder den Spezialisten der IT-Hotline. Öffnen Sie die Anhänge nicht, laden Sie nichts herunter und installieren Sie nichts. Auch bei bekannten Absendern ist Vorsicht angebracht, wenn Anhänge unüblich sind.*
- **Widersprüchliches Verhalten:** *Seien Sie besonders vorsichtig, wenn etwas nicht wie üblich abläuft oder nicht zum Bisherigen passt. Ändert sich plötzlich die Bankverbindung oder gab es noch nie eine Audionachricht vom Chef? Waren bislang andere Ansprechpartner zuständig oder war noch nie ein Behördenschreiben bei Ihnen gelandet? Dann heißt es Stopp. Machen Sie nicht das, was gefordert wird.*

Und ganz wichtig: *Hören Sie auf Ihr Bauchgefühl. Kommt Ihnen etwas seltsam oder komisch vor, heißt es immer: Vorsichtig sein. Machen Sie nicht gleich das, was von Ihnen gefordert wird. Behalten Sie die Nerven, bewahren Sie einen kühlen Kopf und reden Sie mit anderen darüber. So wird häufig klar, dass Sie mit Ihrem Bauchgefühl nicht falsch lagen.*

Das machen Sie bei Verdächtigem

Dann heißt es zunächst Ruhe bewahren und nicht unüberlegt handeln. Sie haben immer Zeit, die nächsten Schritte zu durchdenken. Fragen Sie bei Zweifeln nach, und zwar bei Kollegen, Vorgesetzten, der IT-Hotline oder beim Datenschutzbeauftragten. Melden Sie Verdächtiges. Und: Sind Sie jemandem auf den Leim gegangen, können Sie größeren Schaden vermeiden helfen. Melden Sie die Sache sofort Ihrem Vorgesetzten und der IT-Hotline.

Noch Fragen? Die Antworten bekommen Sie bei der IT-Hotline unter der Durchwahl -1234 oder beim Datenschutzbeauftragten. Wir beißen nicht und stehen Ihnen mit Rat und Tat zur Seite – immer und jederzeit!

Viele Grüße

Ingo Nesien
Datenschutzbeauftragter

Organisatorisches Versagen: Prüfen Sie diese 7 Hotspots

Als Datenschutzexperte wissen Sie: Datenschutz ist eine ziemlich große Herausforderung, und zwar für Ihr Unternehmen und Sie als Datenschutzbeauftragter. Und damit Datenschutz bei der Verarbeitung personenbezogener Daten funktioniert, kommt es nicht nur auf die technische Umsetzung an. Entscheidend ist auch das Organisatorische.

Organisatorisches kann zum Problem werden

Art. 24 Abs. 1 Datenschutz-Grundverordnung (DSGVO) und Art. 32 DSGVO machen unmissverständlich klar: Ihr Unternehmen muss risikoorientiert geeignete technische und organisatorische Maßnahmen umsetzen. Es muss so sicherstellen und nachweisen können, dass die Verarbeitung gemäß der DSGVO erfolgt bzw. sicher ist. Auch muss es fortlaufend prüfen, ob die Maßnahmen noch angemessen sind bzw. inwieweit diese angepasst werden müssen.

Dabei ist klar: Nicht nur technisch kann beim Verarbeiten von personenbezogenen Daten so einiges schiefgehen. Das ist auch möglich, wenn Sie den Blick auf das Organisatorische richten. Beispielsweise können

- fehlende Regeln und Vorschriften dazu führen, dass Beschäftigte Daten falsch verarbeiten und es zum Datenschutzverstoß kommt,
- unzureichendes Wissen und fehlende Sensibilität zu Fehlverhalten im Umgang mit personenbezogenen Daten führen,
- überhaupt nicht, falsch oder unzureichend erfüllte Betroffenenrechte für großen Ärger sorgen, etwa mit Betroffenen,
- wiederholte oder fortgesetzte Verstöße auf systemische Organisationsmängel hinweisen, die ein Bußgeld unumgänglich machen und diese ggf. höher ausfallen lassen,
- fehlende oder unzureichende Kontrollen die Risiken und Schäden größer machen.

Übrigens: Ihr Unternehmen und dessen Leitung sollten nie nur das Bußgeldrisiko im Blick behalten. Werden nicht die gebotenen Maßnahmen ergriffen, wird nicht angemessen mit Risiken umgegangen. Das kann auch das persönliche Haftungsrisiko erhöhen.

Halten Sie Ausschau nach diesen 7 Hotspots

Prüfen Sie, ob Sie diese Hotspots, sprich diese Schwachpunkte, in Ihrem Unternehmen wiederfinden. Ist dem so, sollten Sie zügig das Gespräch mit der Unternehmensleitung suchen. Diskutieren Sie Ihre Feststellung und suchen Sie gemeinsam nach Wegen, um die Situation zu verbessern.

Hotspot Nr. 1: Fehlende Vorgaben, Regelungen und Verträge

Schauen Sie zunächst ins Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 DSGVO. Darin sollten alle Verarbeitungsverfahren bzw. Verarbeitungsprozesse abgebildet und umfassend dokumentiert sein. Prüfen Sie zumindest stichprobenhaft für die risikobehafteten Verarbeitungstätigkeiten, inwieweit Regelungen, Arbeitsanweisungen und Festlegungen bestehen. Denken Sie in dem Zusammenhang auch an Verträge und Vereinbarungen mit Datenschutzrelevanz. Das sind nicht nur Datenschutzverträge, etwa zur Auftragsverarbeitung. Auch Betriebsvereinbarungen können Defizite aufweisen und nicht alles Relevante regeln bzw. schlichtweg veraltet sein.

Hotspot Nr. 2: Unzureichende Umsetzung von Festlegungen

Nur weil es Vorgaben oder Festlegungen gibt, sind diese nicht automatisch umgesetzt. Manchmal entwickeln oder etablieren sich auch Handhabungen, die dem Geregelten widersprechen. Kontrollieren Sie also die tatsächliche Umsetzung und machen Sie insofern einen Abgleich von Ist und Soll.

Hotspot Nr. 3: Fehlende oder nicht funktionierende Prozesse

Prozesse sind entscheidend. Denn sie geben Abläufe vor und stellen sicher, dass erforderliche Entscheidungen von den zuständigen und befugten Personen getroffen werden. Haben Sie hier zunächst ein Auge auf Prozesse, die direkten Datenschutzbezug haben bzw. der Umsetzung der Vorgaben der DSGVO dienen. Typisches Beispiel sind hier die Prozesse rund um die Umsetzung von Betroffenenrechten oder zum strukturierten Vorgehen bei Datenpannen.

Hotspot Nr. 4: Mangelndes Risikobewusstsein

In manchem Unternehmen wird nach dem Prinzip gehandelt, dass alles schon irgendwie gutgehen wird. So zu denken und zu arbeiten ist nicht nur riskant. Es ist geradezu grob fahrlässig. Dass irgendwann etwas schiefgehen wird, ist geradezu vorprogrammiert.

Hotspot Nr. 5: Unzureichende Awareness und Sensibilität

Hier liegt der Fokus auf Führungskräften und Mitarbeitern. Schätzen Sie ein, wie es um Sensibilität für die Anforderungen des Datenschutzes steht. Auch ist die positive Grundeinstellung zum Thema entscheidend. Kämpft man eher gegen den Datenschutz, wird es mit der Umsetzung schwierig.

Hotspot Nr. 6: Defizite bei der Datenschutzorganisation

Bewerten Sie kritisch, inwieweit die Organisation zu den bestehenden Herausforderungen passt. Verfügen Sie nicht über die nötigen Ressourcen oder verweigert man Ihnen die nötige Unterstützung, wird dem Datenschutz ein Bärendienst erwiesen.

Hotspot Nr. 7: Fehlende Kontrollen

Ob etwas funktioniert, sieht man erst, wenn man nachprüft, ob dem so ist. Dabei müssen es nicht immer Ihre Kontrollen sein, um ein Funktionieren oder Nichtfunktionieren auszumachen. Prozesse oder Regelungen können auch andere Stellen prüfen. Aber klar ist: Die Prüfungen müssen passen und Tiefgang haben. Oberflächliche Prüfungen bringen nichts und schützen erst recht nicht vor Schlimmerem.

Wie geht man am besten mit unterschiedlichen Auffassungen um?

FRAGE: Das von mir als Datenschutzbeauftragte betreute Unternehmen ist oft als IT-Dienstleister tätig. Dass hier Art. 28 Datenschutz-Grundverordnung (DSGVO) gilt und es einer Vereinbarung zur Auftragsverarbeitung bedarf, liegt auf der Hand. Unser Datenschutzkonzept ist Teil zahlreicher Verträge mit Auftraggebern. Die Datenschutzbeauftragte eines potenziellen Auftraggebers hat dieses Konzept als nicht ausreichend bewertet. Ich sehe das als Datenschutzbeauftragte ganz anders. Allerdings könnte nun das Geschäft mit dem neuen Auftraggeber platzen, wenn nicht dessen Anforderungen entsprochen wird. Wie geht man mit dieser kniffligen Situation am besten um?

ANTWORT: Wichtig ist zunächst, dass Ihr Unternehmen das Gespräch mit dem Auftraggeber sucht, um die Situation zu besprechen und Möglichkeiten auszuloten, wie man doch noch zusammenkommen kann. Dazu kann es eine gute Idee sein, wenn Sie sich mit der Datenschutzbeauftragten des Auftraggebers austauschen. Sie sollten verstehen und nachvollziehen können, welche Aspekte, Einschätzungen und Feststellungen zu ihrer Einschätzung führten. Unter Umständen sind die Gründe gerechtfertigt.

Daneben ist natürlich Folgendes wichtig: Auch bei der Festlegung der technischen und organisatorischen Schutzmaßnahmen herrscht quasi Vertragsfreiheit. Es ist also zwischen Verantwortlichem und Auftragsverarbeiter „verhandelbar", welche Maßnahmen im konkreten Fall umzusetzen sind.

Dabei gibt es auch für Ihr Unternehmen mehrere Optionen. Es kann die gewünschten Schutzmaßnahmen umsetzen und die anfallenden Kosten in seine Vergütung einpreisen. Alternativ kann Ihr Unternehmen die aus seiner Sicht angemessenen Schutzmaßnahmen anbieten und dem Vertragspartner die Entscheidung überlassen, ob diese für seine konkrete Verarbeitung ausreichend und risikoangemessen sind. Will dieser die angebotenen Maßnahmen nicht akzeptieren, kommt das Geschäft nicht zustande. Das kann für Ihr Unternehmen die vorzugswürdige Option sein, wenn es ein sehr starres Datenschutzkonzept verfolgt und für Kunden nur in sehr begrenztem Umfang davon abweichen kann. Denn jedes Abweichen kann die Dienstleistung verteuern, etwa durch Prozesse, die individuell gestaltet sind und nicht mehr von der Stange.

Tauschen Sie sich aus

Sprechen Sie mit der Datenschutzbeauftragten. Eventuell können Sie sie von Ihrer Auffassung überzeugen. Doch auch wenn Sie erkennen, dass Sie falsch lagen, wäre das kein Beinbruch. Machen Sie den zuständigen Kollegen klar, dass Sie in diesem Fall an Ihrer bisherigen Einschätzung nicht mehr festhalten können, und diskutieren Sie die Auswirkungen auf Ihr Unternehmen. Müssen Anpassungen vorgenommen werden, etwa am Datenschutzkonzept, ist das etwas, an dem kein Weg vorbeiführt. Schließlich müssen die Schutzmaßnahmen nach Art. 32 DSGVO passen.

Genießt auch der Stellvertreter Kündigungsschutz?

FRAGE: Ich bekomme als Datenschutzbeauftragter demnächst einen Stellvertreter. Es gab einen Termin mit dem für diesen Posten vorgesehenen Kollegen. In diesem Zusammenhang kam die Frage auf: Gelten für den Stellvertreter die gleichen besonderen Rechte, sprich, besteht für den stellvertretenden Datenschutzbeauftragten auch besonderer Kündigungsschutz?

ANTWORT: Es ist eine gute Sache, wenn Sie jemanden haben, der etwa während Ihres Urlaubs Ansprechpartner in Datenschutzfragen sein kann. Allerdings ist eine solche Rolle bzw. ein Stellvertreter für den Datenschutzbeauftragten weder nach Art. 37 ff. Datenschutz-Grundverordung noch nach § 38 Bundesdatenschutzgesetz vorgesehen. Grundsätzlich bedarf es eben nur eines Datenschutzbeauftragten, wenn auch im Einzelfall ein Stellvertreter sinnvoll sein kann. Gesetzlich gefordert ist er nicht, sodass für ihn auch nicht die besonderen Rechte gelten.

Betrachten Sie die Sache auch aus der Perspektive Ihres Unternehmens. Natürlich wäre es möglich, dass der besondere Kündigungsschutz auf arbeitsvertraglicher Ebene vereinbart und somit auch auf einen Stellvertreter angewendet wird. Realistischerweise dürfte das jedoch nicht im Interesse des Verantwortlichen sein, sprich des Arbeitgebers. Es wäre meist auch nicht sachgerecht, da ein Stellvertreter meist eben nicht die volle Verantwortung und das volle Aufgabenspektrum des Datenschutzbeauftragten übernimmt.

EuGH: Pseudonyme Daten können auch anonym sein

Wann und unter welchen Umständen Daten als personenbezogene Daten anzusehen sind, war auch schon vor der Datenschutz-Grundverordnung (DSGVO) umstritten. Dass es hier entscheidend auf die Perspektive des Verantwortlichen ankommt, zeigt eine Entscheidung des Europäischen Gerichtshofs (EuGH) vom 4.9.2025 (Rs. C-413/23 P).

Der Sachverhalt

Auf EU-Ebene gibt es den SRB, den „Einheitlicher Abwicklungsausschuss". Der ist zuständig, um im Zusammenhang mit der Abwicklung von Banken Ansprüche von Anteilseignern oder Gläubigern zu prüfen und darüber zu entscheiden. So war es auch im Fall einer spanischen Bank. Der SRB startete dazu ein Verfahren zur Vorbereitung seiner Entscheidung. Dazu mussten sich Anteilseigner und Gläubiger registrieren, um etwa an einem Anhörungsverfahren teilzunehmen.

Bei der Registrierung wurden personenbezogene Daten erfasst. Wer sich registriert hatte, sollte zur Vorbereitung der SRB-Entscheidung einen Fragebogen erhalten. Dazu wurde ein 33-stelliger zufälliger Code erzeugt, der den registrierten Personen zugeordnet wurde. Die zurückerhaltenen Fragebögen sollten vom Wirtschaftsprüfer Deloitte als unabhängigem Gutachter bewertet und aufbereitet werden. Dabei erhielt Deloitte keine Informationen, die einen Rückschluss auf eine konkrete Person zuließen. Deloitte verfügte also aus seiner Sicht nur über anonyme Informationen. Die Zuordnung war über den Code nur dem SRB möglich.

Unvollständige Datenschutzhinweise

Bei der Registrierung wurde über die stattfindende Datenverarbeitung informiert, und zwar nach Art. 15 der Verordnung 2018/1725, quasi der DSGVO für Stellen der EU. Nicht informiert wurde jedoch darüber, dass der SRB die pseudonymisierten Fragebögen zur Analyse an Deloitte weitergibt.

Das bemerkten einige Betroffene. Sie beschwerten sich beim Europäischen Datenschutzbeauftragten (EDSB). Dieser untersuchte die Sache und kam unter anderem zum Ergebnis, dass der SRB gegen die Informations- und Transparenzpflicht verstoßen hatte. Das wollte der SRB nicht akzeptieren. Er klagte vor dem Gericht der EU und bekam recht. Gegen diese Entscheidung ging der EDSB vor. Der zuständige EuGH entschied nun zugunsten des EDSB.

So urteilte der EuGH

Auf den Punkt gebracht: Pseudonymisierte Daten können bei einer Übermittlung an einen Dritten für diesen nicht personenbezogen sein. Entscheidend ist hier die Identifizierbarkeit des Betroffenen für den Dritten. Aber: Ein Verantwortlicher muss über die Übermittlung der pseudonymisierten Daten informieren. Das auch dann, wenn die Daten aus Sicht des Dritten wegen der Pseudonymisierung als nicht personenbezogene Daten gewertet werden können.

Im Gegensatz zur Vorinstanz geht der EuGH bei den in den Fragebögen enthaltenen Informationen eindeutig von personenbezogenen Daten aus. Es handelt sich um persönliche Meinungen und Sichtweisen, die zwangsläufig eng mit einer Person verknüpft sind.

Identifizierbarkeit ist entscheidend

Ob bei pseudonymen Daten für einen Dritten ein Personenbezug besteht, hängt insbesondere davon ab, ob im Hinblick auf die Daten eine Person identifizierbar ist. Kann nicht ausgeschlossen werden, dass ein Dritter mit den ihm zur Verfügung stehenden Mitteln, etwa einem Abgleich mit anderen Informationen, die Daten einer betroffenen Person zuordnen kann, muss von einer Identifizierbarkeit ausgegangen werden. Allerdings müssen entgegen der Ansicht des EDSB nicht immer und für jede Person pseudonymisierte Daten als personenbezogene Daten angesehen werden. Im Einzelfall kann eine Pseudonymisierung den Dritten tatsächlich an einer Identifizierung hindern.

Transparenz ist Pflicht

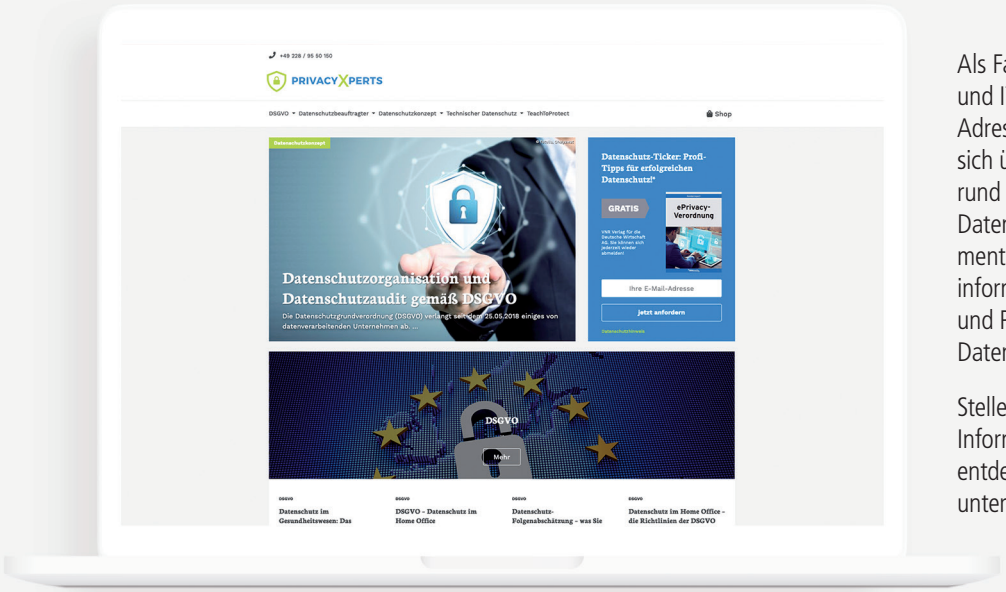
Der EDSB hat zu Recht beanstandet, dass der SRB gegen die ihm obliegende Informationspflicht nach Art. 15 der Verordnung 2018/1725 verstoßen hat. Deloitte war in der Datenschutzerklärung nicht als potenzieller Empfänger der Informationen genannt. Diese Information hätte zum Zeitpunkt der Erhebung der Daten zur Verfügung gestellt werden müssen. Die Grundsätze der fairen und transparenten Verarbeitung machen es erforderlich, dass ein Betroffener nicht nur über den Verarbeitungsvorgang und seine Zwecke an sich informiert wird. Auch die weiteren Informationen sind notwendig. Dem Betroffenen muss ermöglicht werden, in voller Kenntnis der Sachlage zu entscheiden, ob er die betreffenden Daten zur Verfügung stellen will. Die Informationspflicht bestand beim SRB als Verantwortlichem im Zeitpunkt der Erhebung der Daten. Es kommt also nicht darauf an, ob die Daten durch die Pseudonymisierung für einen Dritten noch personenbezogen waren oder nicht.

§

Fazit für Ihre Arbeit

Der EuGH stellt klar: Für den Personenbezug kommt es in erster Linie auf die tatsächliche Identifizierbarkeit des Betroffenen an. Ist eine Identifizierbarkeit ausgeschlossen, können aus Sicht des Verantwortlichen pseudonyme Daten für Dritte anonyme Daten darstellen. Aber: Der Verantwortliche muss immer auch über die Empfänger der pseudonymen Daten informieren, und zwar auch dann, wenn es sich aus Sicht des Empfängers um anonyme Daten handelt.

„Datenschutz aktuell“ ist ein Produkt der PrivacyXperts-Familie!



Als Fachverlag für Beratung im Bereich Datenschutz und IT-Security sind Sie bei uns genau an der richtigen Adresse, wenn es um Ihre Themen geht. Lassen Sie sich über unsere Fachinformationsdienste und Portale rund um neue EU-Verordnungen, aktuelle Urteile zum Datenschutzrecht oder über die umfangreichen Dokumentationspflichten für Datenschutzverantwortliche informieren. So erhalten Sie nützliche Informationen und Praxistipps für Ihre Arbeit und sind beim Thema Datenschutz bestens aufgestellt.

Stellen Sie eine direkte Verbindung zu verlässlichen Informationen und aktuellen Entwicklungen her und entdecken Sie viele weitere Datenschutz-Produkte unter **www.privacyxperts.de/shop**

MITARBEITERINFORMATION CYBERSICHERHEIT

- ✓ **zeitsparend und wirksam** für Cybergefahren und Informationssicherheit sensibilisieren
- ✓ die **wichtigsten Informationen griffbereit** und mit **praktischen Checklisten** direkt umsetzbar
- ✓ **perfekt für neue Mitarbeiterinnen und Mitarbeiter, um** schnell die relevantesten Themen zu schulen

JETZT STAFFELRABATT SICHERN

JETZT NEU

Bestellen Sie direkt hier: https://t1p.de/MitarbeiterinformationCybersicherheit

PRIVACYXPERTS

Telefon: 02 28 95 50 150
Fax: 02 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de

Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2–4
53177 Bonn