4/25

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER

PSEUDONYMISIERUNG

Wie Sie damit viele Datenschutzprobleme lösen können

DATENSICHERHEIT

8 typische Risiken für Ihre Daten – und wie Sie sie vermeiden

powered by
PRIVACYXPERTS

Liebe Leserin, lieber Leser,

Daten sind für Ihr Unternehmen Gold wert. Allerdings bergen sie auch viele Risiken, wenn sie in falsche Hände geraten, da sie hochsensibel und schutzwürdig sind. Ein Missgeschick bei der Verarbeitung oder ein Angriff durch Kriminelle kann zu einem meldepflichtigen Datenschutzvorfall führen.

Je nach Vorfall und Sensibilität kann dies auch Schadensersatzforderungen durch die betroffenen Personen nach sich ziehen. Hinzu kommt, dass die Verarbeitung der Daten im Rahmen der Möglichkeiten der Datenschutzvorschriften erfolgen muss. Viele dieser Probleme können Sie in Ihrem Unternehmen mit Pseudonymisierung und Anonymisierung lösen. Was es hiermit auf sich hat, lesen Sie ab Seite 3 in dieser Ausgabe.

Datenschutz muss nicht trocken sein – aber er muss ernst genommen werden. Mit ein wenig Achtsamkeit und gesundem Misstrauen machen Sie unser Unternehmen sicherer. Mit unseren Tipps in dieser Ausgabe ab Seite 5 vermeiden Sie 8 typische Risiken im Datenschutz.

Wir wünschen Ihnen einen schönen Frühling.

Mit freundlichen Grüßen

Ihr Redaktionsteam von „Privacy@Work“

SEBASTIAN TAUSCH

ARBEITET ALS SELBSTSTÄNDIGER IT-BERATER UND UNTERSTÜTZT KLEINE UND MITTLERE UNTERNEHMEN PRAXISNAH IM BEREICH DATENSCHUTZ. NACH EINER KAUFMÄNNISCHEN AUSBILDUNG SAMMELTE ER VIELE JAHRE PRAKTISCHE IT-ERFAHRUNG.

ANDREAS HESSEL

IST ALS CHIEF INFORMATION SECURITY OFFICER LANGJÄHRIGER LEITER DES BEREICHES INFORMATIONSSICHERHEIT UND RISIKOMANAGEMENT EINER LANDESBANK. DANEBEN ARBEITET ER ALS EXTERNER DATENSCHUTZBEAUFTRAGTER UND BERATER IM BEREICH CYBERSECURITY.

DATENSCHUTZPROBLEME LÖSEN MIT PSEUDO- UND ANONYMISIERUNG

Daten sind das neue Gold. Insbesondere die Auswertung von Daten ermöglicht es Unternehmen, aber auch anderen Organisationen, wie Forschungseinrichtungen, wichtige Erkenntnisse aus den Daten zu gewinnen. Doch diese Datensammlungen können auch im Jahr 2025 schnell zum Risiko werden. Ein Missgeschick bei der Verarbeitung oder ein Angriff durch Kriminelle kann zu einem meldepflichtigen Datenschutzvorfall führen. Je nach Vorfall und Sensibilität kann dies auch Schadensersatzforderungen durch die betroffenen Personen nach sich ziehen. Hinzu kommt, dass die Verarbeitung der Daten im Rahmen der Möglichkeiten der Datenschutzvorschriften erfolgen muss. Mit der Pseudonymisierung und Anonymisierung lassen sich viele dieser Probleme lösen.

Das ist der Unterschied

Die Begriffe werden immer wieder verwechselt, doch sie haben unterschiedliche Bedeutungen und auch Auswirkungen.

Pseudonymisierung: Personenbezogene Daten werden so verändert, dass sie ohne zusätzliche Informationen nicht mehr einer bestimmten Person zugeordnet werden können. Ein Beispiel aus dem Personalbereich: Anstelle eines Namens wird eine Mitarbeiter-ID, etwa aus der Personalsoftware, verwendet. Die Rückführung auf die ursprüngliche Person ist aber weiterhin möglich – etwa durch die Personen, welche auf die Personalsoftware zugreifen können. Daher unterliegen pseudonymisierte Daten weiterhin der Datenschutz-Grundverordnung (DSGVO)!

Anonymisierung: Hier werden personenbezogene Daten so verändert, dass eine Identifizierung der Person unmöglich ist – selbst mit zusätzlichen Informationen. Ein Beispiel wäre eine Analyse der Gehaltsstrukturen nach Abteilungen, bei der keine individuellen Mitarbeiterdaten mehr erkennbar sind. Damit entfällt die Anwendbarkeit der Datenschutzvorschriften für diese Daten. Aber Achtung: Die Anonymisierung muss richtig erfolgen! Das gelingt nicht immer, wie nachfolgend noch aufgezeigt wird.

Die Vorteile der Pseudonymisierung

Die Pseudonymisierung bietet mehrere Vorteile, insbesondere wenn personenbezogene Daten weiterhin verarbeitet werden müssen. Ein großer Vorteil ist, dass die Daten besser geschützt sind, da ohne den separaten Schlüssel keine direkte Identifikation möglich ist. Dadurch kann das Risiko eines Datenschutzverstoßes verringert werden. Zudem ermöglicht die Pseudonymisierung die Nutzung personenbezogener Daten für Analysen, ohne dass sofort Rückschlüsse auf einzelne Personen gezogen werden können. In vielen Fällen ist sie ein guter Kompromiss zwischen Datenschutzanforderungen und der Notwendigkeit, Daten weiterhin zu verwenden.

Beispiel: Ein Unternehmen möchte die Krankheitsquoten in den verschiedenen Abteilungen auswerten. Anstatt die Namen der erkrankten Mitarbeiter zu erfassen, werden pseudonymisierte Kennungen genutzt. So kann die Personalabteilung Trends erkennen, ohne sofort einzelne Personen identifizieren zu können. Falls im Nachhinein genauere Untersuchungen nötig sind, ist eine Identifikation über die separate Zuordnungsliste im Bedarfsfall weiterhin möglich.

Die Nachteile der Pseudonymisierung

Trotz der Vorteile gibt es auch einige Nachteile der Pseudonymisierung. Einer der größten Nachteile ist, dass die Daten unter die DSGVO fallen, da die Identifizierung der betroffenen Personen weiterhin möglich ist. Dadurch bleiben die gesetzlichen Anforderungen an Datenschutz und Datensicherheit bestehen. Zudem erfordert eine sichere Pseudonymisierung organisatorische und technische Maßnahmen, um zu verhindern, dass unbefugte Personen auf die Zuordnungsliste zugreifen können. Wird diese Liste kompromittiert, kann dies zu einem erheblichen Datenschutzrisiko führen. Wie bei den Vorteilen oben aber beschrieben, verringert sich das Risiko eines meldepflichtigen Datenschutzvorfalls bei der Arbeit mit pseudonymisierten Daten üblicherweise.

Beispiel: Ein Unternehmen speichert Gehaltsdaten mit pseudonymisierten IDs, um interne Gehaltsvergleiche durchzuführen. Falls jedoch ein Mitarbeiter Zugang zu der Zuordnungsliste erhält, könnte er genau

>

> nachvollziehen, welches Gehalt welcher Person zugeordnet ist. Ohne ausreichende Sicherheitsmaßnahmen könnte dies zu internen Konflikten oder Datenschutzverstößen führen.

Die Risiken einer schlechten Anonymisierung

Ein häufiger Fehler ist, dass Daten nur scheinbar anonymisiert werden. Doch durch Kombination verschiedener Datensätze oder externe Informationen kann eine Person oft doch wieder identifiziert werden. Dies nennt man Re-Identifikation. Beispiele hierfür sind:

Einzelne Merkmale reichen aus: Wenn nur wenige Merkmale bestehen bleiben, z. B. Alter, Geschlecht, kann eine Person oft eindeutig identifiziert werden. *Beispiel:* In einer Gehaltsauswertung werden Gehälter nach Geschlecht und Alter gruppiert. Wenn es nur eine Mitarbeiterin über 60 gibt, ist ihr Gehalt indirekt nachvollziehbar.

Kombination mit anderen Datenquellen: Wenn anonymisierte Daten mit öffentlich verfügbaren oder geleakten Datensätzen verknüpft werden, kann dies zur De-Anonymisierung führen.

Beispiel: Eine Firma veröffentlicht eine anonyme Gehaltsstatistik, in der unter anderem Abteilung und Standort genannt werden. Wenn in einer anderen öffentlich zugänglichen Angabe die Standorte der Teams und deren Teamgrößen erwähnt werden, kann unter Umständen ermittelt werden, wem bestimmte Gehaltswerte zuzuordnen sind.

Zu detaillierte Auswertungen: Werden Daten zu spezifisch gruppiert oder veröffentlicht, lassen sich Einzelpersonen oft wieder herausfiltern.

Beispiel: Eine Gehaltsübersicht listet die Durchschnittsgehälter nach Abteilungen auf. In der Abteilung arbeiten eine Person in Vollzeit und eine Person im Rahmen einer geringfügigen Beschäftigung (Minijob).

Die Vorteile einer echten Anonymisierung

Eine korrekte Anonymisierung bietet zahlreiche Vorteile:

Weniger Risiko und somit oft weniger Schutzbedarf: Sofern keine personenbezogenen Daten enthalten sind, sinkt das Risiko zumindest im Hinblick auf den Datenschutz, da keine Personen mehr betroffen sind. Enthält die Auswertung auch sonst keine sensiblen Daten, etwa Firmengeheimnisse, reduziert sich üblicherweise auch der mögliche Schaden, wenn unbefugte Personen diese einsehen können. Damit sinkt normalerweise auch der Schutzbedarf.

DSGVO kommt nicht mehr zur Anwendung: Werden keine Daten einer natürlichen Person verarbeitet und lässt sich auch kein Bezug zu einer natürlichen Person herstellen, findet die DSGVO keine Anwendung mehr.

Längere Speicherung und keine Zweckbindung: Da die DSGVO nicht mehr angewendet wird, entfallen die entsprechenden Vorgaben. Somit müssen etwa kein Zweck und keine Rechtsgrundlage für die Verarbeitung im Sinne der DSGVO vorhanden sein. Auch die Löschung nach Zweckentfall im Sinne der DSGVO greift nicht mehr.

Wann und wie anonymisieren?

Wer Daten sicher anonymisieren will, sollte folgende Maßnahmen beachten:

Maskierung: direkte Identifikatoren entfernen oder unkenntlich machen.

Beispiel: Personalnummer und Name werden aus der Gehaltsübersicht entfernt.

Aggregation: Daten zusammenfassen, sodass keine Rückschlüsse auf Einzelpersonen möglich sind.

Beispiel: Anstatt die Gehälter einzelner Mitarbeiter anzugeben, werden Durchschnittswerte pro Abteilung genutzt.

Differential Privacy: Methoden nutzen, die bewusst Zufallsrauschen in Daten einfügen, um Identifizierungen zu verhindern.

Beispiel: In einer Gehaltsauswertung wird jedem individuellen Gehalt ein zufälliger Betrag aus einem vorgegebenen Spielraum hinzugefügt oder abgezogen, bevor Durchschnittswerte berechnet werden. Dadurch bleibt die Gesamtstatistik aussagekräftig, aber einzelne Gehaltswerte sind nicht mehr genau zurückzuverfolgen.

k-Anonymität: sicherstellen, dass jede Kombination von Daten mindestens k-mal vorkommt, sodass keine Einzelperson hervorsticht.

Beispiel: Wenn in einer Abteilung nur eine Person arbeitet, sollten die Daten dieser Person nicht separat in Berichten erscheinen. Meistens wird dann die Ein-Per-

sonen-Abteilung einer anderen zugeordnet, also etwa die IT-Abteilung der Verwaltung.

In der Praxis werden diese Maßnahmen auch kombiniert, um eine möglichst robuste Anonymisierung zu gewährleisten.

Die Möglichkeiten nutzen

Pseudonymisierung und Anonymisierung sind wichtige Werkzeuge, um den Datenschutz zu gewährleisten. Während die Pseudonymisierung oft für den sicheren Umgang mit personenbezogenen Daten im Unternehmen genutzt wird, bietet eine echte Anonymisierung den Vorteil, dass Daten ohne DSGVO-Einschränkungen verarbeitet werden können. Unternehmen sollten sich daher frühzeitig mit diesen Konzepten befassen und geeignete Verfahren wählen, um langfristig datenschutzkonform und effizient zu arbeiten. Um die beschriebenen Risiken, etwa schlechter Anonymisierung, zu verhindern, sollten Sie Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten frühzeitig einbinden. (ST)

DATENSCHUTZ UND DATENSICHERHEIT IM UNTERNEHMEN: 8 TYPISCHE RISIKEN – UND WIE SIE SIE VERMEIDEN

1. Datenschutz-Fails im Büroalltag – sind Sie auch dabei?

Datenschutz im Büro ist wie eine gute Versicherung: Man merkt erst, dass man ihn braucht, wenn etwas schiefgeht. Und leider passieren kleine Pannen im Arbeitsalltag schneller, als man denkt:

- Ein falsch adressierter E-Mail-Anhang,
- ein offenes Dokument am Bildschirm oder
- ein vergessener Ausdruck auf dem Drucker – all das sind Momente, in denen Datenschutzverletzungen entstehen.

Doch keine Panik! Mit ein paar einfachen Verhaltensregeln lassen sich die schlimmsten Fails vermeiden.

Wie es schiefgehen kann:

- Das Passwort „123456“ – sicher wie ein Gartentor ohne Schloss.
- Der offene Aktenordner mit Gehaltslisten, damit jeder mal reinschauen kann.
- Der Ausdruck mit Kundeninfos, der als Notizzettel für die Einkaufsliste dient.

Besser machen:

- Nutzen Sie einen Passwort-Manager, um Ihre Passwörter sicher zu speichern.
- Räumen Sie den Schreibtisch auf und sperren Sie vertrauliche Dokumente weg.
- Vernichten Sie Papiere mit personenbezogenen oder sensiblen Daten und nehmen Sie keine Papiere mit nach Hause.

2. „Alexa, schick die Kundendaten an die Konkurrenz!“ – Sprachassistenten und Datenschutz

Technologie soll unser Leben erleichtern, aber manchmal sorgt sie für unerwartete Probleme – besonders wenn sie alles mithört. Sprachassistenten wie Alexa, Siri oder Google Assistant sind praktisch, aber sie haben eine Schwäche: Sie lauschen mit. Das mag im privaten Bereich im Wohnzimmer harmlos sein, aber im Büro oder Homeoffice kann es brisant werden. Möchten Sie wirklich, dass Ihre Kundenverträge, internen Besprechungen oder Finanzzahlen bei Amazon, Apple oder Google landen?

Warum das problematisch ist:

- Sprachassistenten speichern Gespräche – und das oft in der Cloud.
- Sie reagieren auf Schlüsselwörter und könnten versehentlich sensible Infos aufnehmen.
- Sie sind neugieriger als Ihr Kollege aus der Buchhaltung.

Besser machen:

- Schalten Sie Sprachassistenten im Büro aus oder verbannen Sie sie gleich ganz. Das gilt auch für Ihr privates Smartphone oder Ihre Smartwatch mit aktiviertem Sprachassistenten.
- Falls unverzichtbar, konfigurieren Sie die Datenschutz-Einstellungen so restriktiv wie möglich.
- Besprechen Sie sensible Themen lieber hinter verschlossenen Türen – ohne digitale Zuhörer.

>

3. Homeoffice und Datenschutz: die 3 größten Risiken und wie Sie sie vermeiden

Homeoffice ist großartig – keine langen Pendelstrecken, flexible Arbeitszeiten und das eigene Sofa als Bürostuhl. Doch während die Bequemlichkeit sich erhöht, steigt oft auch das Datenschutzrisiko. Wer im Café arbeitet oder im eigenen Wohnzimmer, offenbart Firmengeheimnisse für jeden Sitznachbarn und wer private Cloud-Dienste nutzt, könnte vertrauliche Daten ungewollt extern speichern.

Doch auch hier gilt: Mit ein paar einfachen Maßnahmen lassen sich diese Risiken minimieren.

Typische Datenschutz-Sünden:

1. Arbeiten im Café – gratis WLAN, gratis Datenspionage inklusive.
2. Familien-PC nutzen – „Mama, was ist eine Abmahnung?"
3. Private Cloud-Speicher für Unternehmensdokumente – weil's so bequem ist.

Wie Sie's besser machen:

1. Nutzen Sie eine VPN-Verbindung, wenn Sie außerhalb des Unternehmensnetzwerks arbeiten.
2. Erstellen Sie getrennte Benutzerkonten für Arbeits- und Privatnutzung.
3. Speichern Sie Unternehmensdaten ausschließlich auf genehmigten Systemen.

4. Smarte Drucker, dumme Fehler – wie Ihr Bürodrucker zur Datenfalle wird

Drucker sind wie stille Mitbewohner im Büro – sie stehen da, arbeiten fleißig und keiner denkt groß über sie nach. Doch genau das macht sie gefährlich. Moderne Drucker speichern Daten, lassen sich aus der Ferne ansteuern und sind oft schlecht gesichert.

Ein nicht gelöschter Druckerspeicher oder ein Netzwerkdrucker ohne Passwortschutz kann sensible Informationen preisgeben.

Wo die Gefahren lauern:

- Ausdrucke mit sensiblen Infos liegen stundenlang am Drucker.
- Alte Drucker werden entsorgt – mit Festplatten, auf denen weiterhin Daten gespeichert sind.
- Netzwerkfähige Drucker ohne Sicherheitsupdates sind ein gefundenes Fressen für Hacker.

Schutzmaßnahmen:

- Holen Sie Ausdrucke sofort ab, besonders wenn diese vertrauliche Infos enthalten.
- Löschen Sie Daten auf Druckerfestplatten, bevor Geräte entsorgt werden.
- Halten Sie Firmware und Sicherheitseinstellungen Ihrer Drucker aktuell. Schalten Sie ggf. Ihre IT-Abteilung oder Ihren Datenschutzbeauftragten ein.

5. Sauberer Schreibtisch, sicherer Datenschutz – warum Clean Desk mehr ist als nur eine Ordnungsmaßnahme

Ihr Schreibtisch ist Ihr persönlicher Arbeitsplatz – aber was liegt dort alles herum? Sensible Dokumente, Notizzettel mit Passwörtern oder sogar ein ungeschützter USB-Stick?

Chaos auf dem Schreibtisch kann schnell zu einem Datenschutzproblem werden.

Klassische Fehler:

- Offene Kundenakten auf dem Tisch.
- Notizzettel mit Passwörtern an der Pinnwand.
- Offene PCs, USB-Sticks mit Kundendaten, die wie Souvenirs herumliegen.

Bessere Strategie:

- Räumen Sie vor allem sensible Unterlagen weg, wenn diese nicht mehr benötigt werden.
- Verwenden Sie Passwort-Manager statt Zettelwirtschaft.
- Sperren Sie Laptops und PCs immer, wenn Sie den Platz verlassen, verschlüsseln Sie die Daten auf USB-Sticks und lassen Sie diese nicht offen auf Ihrem Schreibtisch liegen.

6. Die dunkle Seite der KI – wie KI Datenschutz und Datensicherheit beeinflusst

KI ist beeindruckend – aber auch eine Datenschutz-Herausforderung. Systeme, die Daten analysieren, verarbeiten oft riesige Mengen an persönlichen Informationen, manchmal ohne klare Kontrolle.

Wo KI problematisch ist:

- Gesichtserkennung speichert biometrische Daten ohne Einwilligung.
- Chatbots verarbeiten personenbezogene Daten unkontrolliert.
- Automatische Datenanalysen können Datenschutzgrenzen überschreiten.

Wie Sie sich schützen:

- Prüfen Sie, ob KI-Tools datenschutzkonform sind. Fragen Sie Ihren Datenschutzbeauftragten, bevor Sie KI-Systeme nutzen.
- Setzen Sie KI nur ein, wenn Sie wissen, welche Daten verarbeitet werden.
- Löschen Sie sensible Daten aus KI-Systemen, wenn diese nicht mehr benötigt werden.

7. Social Engineering: Warum Hacker auf Ihre Freundlichkeit setzen

Manchmal braucht es keine Technik, sondern nur eine gute Geschichte – und schon gibt man Passwörter preis. Cyberkriminelle setzen auf Psychologie und nutzen die Hilfsbereitschaft von Mitarbeitenden aus.

Typische Betrügereien:

- Ein Anruf von der „IT-Abteilung“: „Bitte geben Sie Ihr Passwort durch.“
- Eine Mail vom „Chef“, der eine dringende Überweisung verlangt.
- Ein Techniker, der angeblich die Druckerwartung machen muss – aber nie beauftragt wurde.

So lassen Sie sich nicht reinlegen:

- Hinterfragen Sie ungewöhnliche Anliegen – auch wenn diese dringend klingen.
- Prüfen Sie die Identität von Anrufern oder Besuchern.
- Teilen Sie Passwörter niemals telefonisch oder per E-Mail mit.

8. Meetings – was darf besprochen werden und was lieber nicht?

Meetings sind zum Austausch da – aber oft hören mehr Leute mit als einem lieb ist. Offene Türen, ungesicherte Videokonferenzen oder laut geführte Telefonate bergen Datenschutzrisiken. Ein unbedachter Satz kann sensible Informationen in die falschen Ohren tragen.

Was falsch läuft:

- Flurfunk live: vertrauliche Kundendaten in der Kaffeeküche besprechen? Schlechte Idee!
- Unverschlüsselte Videomeetings: Jeder kann sich einwählen und mithören.
- Vergessene Notizen: Meeting-Protokolle auf dem Flipchart? Einladung zum Datenleck!

Wie Sie es besser machen:

- Sensible Themen nur hinter verschlossenen Türen besprechen.
- Videokonferenzen mit Passwort sichern und Teilnehmer prüfen.
- Notizen direkt sichern oder vernichten.

Fazit

Mit ein wenig Achtsamkeit und gesundem Misstrauen machen Sie unser Unternehmen sicherer. Beachten Sie aber, dass die hier aufgeführten Risiken und Maßnahmen nicht abschließend sind, sondern zentrale Themen aufgreifen. (AH)

WUSSTEN SIE SCHON, DASS HACKER ANRUFBEANTWORTER ABHÖREN?

Anrufbeantworter sind praktisch – aber leider auch eine unterschätzte Sicherheitslücke. Viele Unternehmen nutzen sie, um Kundenanfragen zu ermöglichen oder interne Informationen zu hinterlassen. Doch wussten Sie, dass Kriminelle mit wenig Aufwand Zugriff auf ungeschützte Mailboxen erhalten können?

Das Problem liegt oft an den voreingestellten PINs. Viele Telefonanlagen oder Mobilboxen haben Standard-PINs wie „0000“ oder „1234“. Wer diese nicht ändert, lädt Hacker quasi ein.

Diese nutzen automatisierte Programme, die systematisch einfache PINs durchprobieren, bis sie erfolgreich sind. Ist die Mailbox erst einmal geknackt, können Angreifer Sprachnachrichten abhören, wichtige Informationen abfangen oder sich beispielsweise mithilfe der abgehörten Gesprächsinhalte als Geschäftsführung ausgeben und den etwa Mitarbeitern betrügerische Anweisungen erteilen.

Ein bekanntes Beispiel aus der Praxis: In einem Unternehmen erhielt die Buchhaltung eine telefonische Anweisung, eine hohe Überweisung an einen vermeintlichen Geschäftspartner zu tätigen. Der Auftrag kam scheinbar vom Geschäftsführer – tatsächlich hatte ein Betrüger zuvor dessen Mailbox geknackt und anhand alter Nachrichten den Sprachstil und wichtige Informationen übernommen. Der Schaden? Sechsstellig!

Um sich zu schützen, sollten Sie unbedingt eine sichere individuelle PIN für Ihre Mailbox festlegen. Vermeiden Sie einfache Zahlenkombinationen und ändern Sie Ihre PIN regelmäßig. (AH)

PASSWORT-TOOL

Wer Passwörter teilt, möchte nicht, dass diese Daten ungeschützt in fremden E-Mail-Postfächern liegen, über die Sie keine Kontrolle haben. Genauso wenig möchten Sie zeitaufwendig und unpraktisch Passwörter per SMS oder telefonisch hinterherschicken. Mit unserem praktischen Passwort-Tool verschicken Sie Zugangsdaten verschlüsselt, behalten die volle Kontrolle und machen es sich und dem Empfänger so einfach wie nie. Scannen Sie dazu einfach den QR-Code und teilen in Zukunft sicher!

Ich habe die Ausgabe von Privacy@Work gelesen:

Name, Vorname, Abteilung	Unterschrift

Bei Fragen im Bereich Datenschutz wenden Sie sich bitte an Ihre Datenschutzbeauftragte oder Ihren Datenschutzbeauftragten!

Impressum:

PRIVACYXPERTS

PrivacyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, D-53177 Bonn; Großkundenpostleitzahl: D-53095 Bonn; Handelsregister: HRB 8165, Registergericht: Amtsgericht Bonn, Vertreten durch den Vorstand: Richard Rentrop, ISSN: 1614 – 5674; Kontakt: Telefon: 0228 – 9 55 01 60 (Kundendienst); Telefax: 0228 — 3 69 64 80, E-Mail: kundendienst@privacyxperts.de, Internet: https://www.privacyxperts.de, Umsatzsteuer: Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372, V.i.S.d.P.: Michael Jodda; Theodor-Heuss-Straße 2–4; D-53177 Bonn, Herausgeber: Michael Jodda, Bonn, Autoren: Andreas Hessel, Sebastian Tausch, Produktmanagement: Lisa Greiling, Bonn, Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen, Bildrechte Seite 1: Andrei – AdobeStock.com, Druck: Warlich Druck Meckenheim GmbH, Meckenheim

Erscheinungsweise: 16-mal pro Jahr; Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. Alle Angaben in Privacy@Work wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier