

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER



HAPPY DSGVO-DAY!

**7 Jahre Datenschutz –
und wie fit sind Sie?**

DATENSCHUTZ ...

**... beim mobilen Arbeiten
im Jahr 2025**

Liebe Leserin, lieber Leser,

happy birthday! Sie haben heute nicht Geburtstag? Die DSGVO wird 7 Jahre alt. Am 25. Mai feiert die Datenschutz-Grundverordnung (DSGVO) Geburtstag. Deshalb nutzen wir diesen besonderen Anlass für einen kleinen Selbst-Check:

- *Wie steht es um Ihren Datenschutz-Alltag?*
- *Welche guten Gewohnheiten haben sich etabliert – und wo könnten wir gemeinsam noch besser werden?*

Starten Sie gleich auf Seite 3 mit unserem kleinen Selbst-Check für Sie.

*Und noch ein aktuelles Thema haben wir für Sie aufbereitet: **Datenschutz und Sicherheit beim mobilen Arbeiten im Jahr 2025. Das ist so wichtig, denn** je mehr wir außerhalb des Büros arbeiten, desto größer wird das Risiko, dass sensible Unternehmens- oder persönliche Daten in falsche Hände geraten. In unserem Beitrag ab Seite 5 erfahren Sie, welche Gefahren bestehen und wie Sie Ihre Daten auf Reisen effektiv schützen.*

Wir wünschen Ihnen einen schönen Wonnemonat Mai.

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 DATENSCHUTZ-BEAUFTRAGTER UND BERATER IM BEREICH CYBERSECURITY.

HAPPY DSGVO-DAY! 7 JAHRE DATENSCHUTZ – UND WIE FIT SIND SIE?

Am 25. Mai feiert die Datenschutz-Grundverordnung (DSGVO) Geburtstag – und damit auch sieben Jahre mehr Verantwortung für den Schutz personenbezogener Daten. Klingt trocken? Muss es nicht! Denn Datenschutz ist kein lästiger Pflichttermin, sondern ein wichtiger Baustein für Vertrauen – bei unseren Kunden, Partnern und natürlich auch im Team.

Sie als Mitarbeitende spielen dabei eine Schlüsselrolle. Deshalb nutzen wir diesen besonderen Anlass für einen kleinen Selbst-Check: Wie steht es um Ihren Datenschutz-Alltag? Welche guten Gewohnheiten haben sich etabliert – und wo könnten wir gemeinsam noch besser werden?

Spoiler: Es geht nicht um Paragrafenreiterei. Sondern um einfache Fragen, die helfen, Datenschutz im Arbeitsalltag pragmatisch und sicher umzusetzen. Und vielleicht entdecken Sie dabei sogar die eine oder andere Überraschung.

Datenschutz-Quiz für Fortgeschrittene (und Neugierige). 10 Fragen, die es in sich haben

Frage 1: „Alexa, hörst du mit?“

Im Büro steht eine smarte Kaffeemaschine mit Sprachsteuerung. Der Hersteller weist darauf hin, dass Sprachdaten zur Verbesserung der Spracherkennung verarbeitet werden. Ist das problematisch?

- a. Nein – das ist ja kein personenbezogenes Datum.
- b. Ja – Sprachdaten sind personenbezogen, besonders im Büro.
- c. Nur wenn jemand „Bitte mit Milch“ sagt.

Richtige Antwort: b) – Sprachaufzeichnungen können Personen identifizierbar machen und sind daher besonders schützenswert. Im geschäftlichen Kontext gilt: Smart Devices mit Mikrofonen nur mit vorheriger Datenschutzprüfung.

Frage 2: Geburtstag vergessen – mit Absicht?

Sie möchten einem Kollegen zum Geburtstag gratulieren, wissen aber nicht, wann er ihn hat. Dürfte das Unternehmen eigentlich Geburtstagslisten in der Abteilung führen?

- a. Klar – das ist doch eine nette Geste.
- b. Nur mit Einwilligung der betroffenen Person.
- c. Nur, wenn auch das Sternzeichen erfasst wird.

Richtige Antwort: b) – Geburtstage sind personenbezogene Daten. Für deren Verarbeitung im Unternehmen – selbst für abteilungsinterne Geburtstagslisten – ist eine freiwillige Einwilligung erforderlich (Art. 6 Abs. 1 Satz 1 lit. a bis f DSGVO).

Frage 3: Fotos auf dem Sommerfest?

Wir organisieren im Unternehmen ein Sommerfest und machen Fotos für die interne Mitarbeiterzeitung. Müssen alle vorher unterschreiben, dass sie fotografiert werden dürfen?

- a. Nein, das geht auch ohne Einwilligung – bei berechtigtem Interesse.
- b. Ja, immer. Ohne Einwilligung kein Foto.
- c. Nur wenn der Betriebsrat auch mit auf dem Bild ist.

Richtige Antwort: a) – Solche Fotos können unter das „berechtigzte Interesse“ (Art. 6 Abs. 1 lit. f DSGVO) fallen – aber: Betroffene müssen vorher über die Aufnahmen informiert werden und ein Widerspruchsrecht haben. Für Porträtfotos oder Veröffentlichungen im Internet ist meist eine Einwilligung nötig.

Hätten Sie es gewusst? Noch ein paar harte Nüsse – für echte Datenschutz-Detektive

Viele datenschutzrechtliche Fragen bewegen sich in Grauzonen. Was zählt, sind: Verhältnismäßigkeit, Information und Transparenz. Und manchmal hilft ein gesunder Menschenverstand mehr als jedes Fachbuch. Weiter geht es mit Frage 4.

Frage 4: Bewerbung gelöscht?

Ein Bewerber wird nach dem Vorstellungsgespräch abgelehnt. Wie lange dürfen seine Daten im Unternehmen gespeichert bleiben?

- a. Bis zum Ende der Probezeit eines anderen Bewerbers.
- b. Maximal sechs Monate, danach müssen sie



- > gelöscht werden – es sei denn, der Bewerber stimmt einer längeren Aufbewahrung zu.
- c. Solange noch jemand daran denkt, wer das war.

Richtige Antwort: b) – Nach dem Allgemeinen Gleichbehandlungsgesetz beträgt die Aufbewahrungsfrist für Bewerbungsunterlagen sechs Monate, falls es zu einer Klage kommen sollte. Für längere Aufbewahrung (z. B. Talentpool) ist eine freiwillige Einwilligung erforderlich.

Frage 5: WhatsApp & Co. – Gruppenfotos im Außendienst

Ein Team im Außendienst macht ein Gruppenfoto nach einem erfolgreichen Einsatz. Eine Kollegin stellt es stolz in die WhatsApp-Gruppe. Datenschutzproblem?

- a. Nein – das ist rein intern.
- b. Ja – auch interne Messenger können Datenschutzrisiken bergen, insbesondere bei privaten Geräten.
- c. Nur wenn jemand keinen Helm trägt

Richtige Antwort: b) – Fotos sind personenbezogene Daten. Auch die Verbreitung über Messenger-Dienste auf privaten Geräten kann problematisch sein, insbesondere wenn die Geräte nicht durch unser Unternehmen verwaltet werden. Besser: dienstliche Plattformen nutzen und vorher informieren. Im Zweifel prüfen, ob für die Veröffentlichung eine Einwilligung der Betroffenen erforderlich ist.

Frage 6: Persönliche Meinung = Personenbezug?

Ein Mitarbeitender schreibt in einem anonymen Online-Feedbackbogen: „Ich finde die neue Führungskraft arrogant.“ Ist das eine personenbezogene Angabe?

- a. Nein – es steht kein Name dabei.
- b. Ja – wenn die Führungskraft dadurch identifizierbar ist, z. B. wenn der Name des Unternehmens oder die Abteilung erkennbar ist.
- c. Nur wenn es alle so sehen.

Richtige Antwort: b) – Auch Meinungen oder Bewertungen können personenbezogene Daten sein, wenn sie einer bestimmten Person zugeordnet werden können. Solche Daten unterliegen dem Schutz der DSGVO.

Datenschutz oder Detektivspiel? Was erlaubt ist und was nicht

Wenn Sie bei einer Frage ins Grübeln kamen – super! Genau das ist der Sinn dieses Quiz. Datenschutz lebt vom Mitdenken, vom Fragenstellen und vom Aus-

tausch. Ihr Datenschutzteam ist für Sie da – mit Workshops, Sprechstunden oder einfach einem guten Tipp für den Alltag.

Frage 7: Die neugierige Kollegin

Sie hören, dass ein Kollege länger krank ist. Eine Kollegin fragt: „Was hat er denn? Burn-out? Rücken?“

Was antworten Sie?

- a. „Weiß ich nicht genau, aber es klang nach was Psychischem.“
- b. „Das geht uns beide nichts an.“
- c. „Ich frag mal in der Personalabteilung nach.“

Richtige Antwort: b) – Gesundheitsdaten gehören zu den besonders sensiblen Informationen nach Art. 9 DSGVO. Selbst wenn man „nur helfen will“, darf man ohne Zustimmung des Betroffenen keine Infos weitergeben. Auch der Flurfunk hat Grenzen.

Frage 8: „Ich habe da was in der Akte gelesen ...“

Ein Mitarbeiter aus der IT wirft einen Blick in die digitale Personalakte eines Kollegen, „einfach so – aus Interesse“. Was sagen Sie dazu?

- a. Ist doch nicht schlimm – reine Neugier.
- b. Nur wer eine dienstliche Notwendigkeit hat, darf auf Personalakten zugreifen.
- c. Wenn nichts verändert wird, ist es okay.

Richtige Antwort: b) – Die Prinzipien der Zweckbindung und Vertraulichkeit gelten auch für interne Systeme. Unbefugter Zugriff auf Personalakten ist ein klarer Datenschutzverstoß – unabhängig davon, ob die Daten geändert werden oder nicht.

Frage 9: Pseudonymisierung = Anonymisierung?

Ein Team verarbeitet Teilnehmerdaten für eine interne Evaluation. Die Namen werden durch Codes ersetzt, aber es gibt eine Liste, mit der man die Codes wieder zurückverfolgen kann. Ist das anonymisiert?

- a. Ja – die Namen stehen ja nicht mehr da.
- b. Nein – das ist eine Pseudonymisierung.
- c. Kommt drauf an, ob jemand das Passwort zur Liste hat.

Richtige Antwort: b) – Die Daten sind pseudonymisiert, nicht anonymisiert. Das bedeutet: Solange ein Rückschluss auf die Person möglich ist (z. B. über eine Zuordnungstabelle), gilt die DSGVO weiterhin.

Frage 10: „Ich habe nur zufällig zugehört ...“

Sie stehen im Großraumbüro an der Kaffeemaschine und hören zufällig ein Telefongespräch mit, bei dem es um eine Kündigung geht. Später erzählen Sie es weiter. Ist das ein Problem?

- a. Nein – es war ja öffentlich zu hören.
- b. Ja – selbst ungewollte Informationen unterliegen der Vertraulichkeit.
- c. nur wenn es vor 10 Uhr war.

Richtige Antwort: b) – Wer zufällig Informationen mitbekommt, darf sie trotzdem nicht verbreiten. Vertraulichkeit gilt auch im Flurfunk. Ein sensibler Umgang mit Gehörtem ist Teil einer guten Datenschutzkultur.

Auswertung: Wie viel Datenschutz steckt in Ihnen?

- **0 bis 2 richtige Antworten:** Sie sind nicht ausreichend informiert – jetzt lohnt sich ein Blick in unser Datenschutz-Wissenscenter.

- **3 bis 4 richtige Antworten:** Gutes Gespür, aber da geht noch was! Vielleicht beim nächsten Lunch and Learn?
- **5 bis 6 richtige Antworten:** Wow! Sie kennen sich aus und wissen, wo Datenschutz im Alltag spielt. Teilen Sie Ihr Wissen!
- **7 bis 10 richtige Antworten:** Super – Sie kennen sich sehr gut aus und sollten Ihre Kolleginnen und Kollegen ermuntern, den Datenschutz ebenso ernst zu nehmen wie Sie.

Fazit: Datenschutz fängt bei uns selbst an

Ob Pseudonymisierung oder das richtige Verhalten im Büro: Datenschutz ist kein starres Regelwerk – sondern ein lebendiges Zusammenspiel von Wissen, Haltung und Gewohnheiten. Und ganz ehrlich: Es macht sogar ein bisschen Spaß, sich auf die Spurensuche nach datenschutzkonformem Verhalten zu begeben. Geben Sie das Quiz auch an Ihre Kolleginnen und Kollegen. Vielleicht sehen diese das dann auch so mit Spaßfaktor. (AH)

DATENSCHUTZ UND SICHERHEIT BEIM MOBILEN ARBEITEN IM JAHR 2025

Geschäftsreisen, mobiles Arbeiten beim Kunden, im Hotel oder auf Messen – die Arbeitswelt wird immer flexibler. Doch je mehr wir außerhalb des Büros arbeiten, desto größer wird das Risiko, dass sensible Unternehmens- oder persönliche Daten in falsche Hände geraten. In diesem Beitrag erfahren Sie, welche Gefahren bestehen und wie Sie Ihre Daten auf Reisen effektiv schützen.

Risiko: Diebstahl, Geräte- und Datenverlust

Viele Menschen führen allein mit ihrem Smartphone dauerhaft riesige Datenmengen mit sich. Bei Reisen kommen dann häufig noch Tablets, Notebooks, ggf. mobile Datenträger und Unterlagen hinzu. Diese können dabei gestohlen werden, verloren- oder kaputtgehen. Mit vier wichtigen Maßnahmen können Sie dazu beitragen, in diesen Fällen Datenverluste und unbefugte Einsichtnahmen möglichst zu vermeiden.

Datenträgerverschlüsselung

Nahezu alle üblicherweise eingesetzten Betriebssysteme für Notebooks, Tablets und Smartphones ermöglichen, eine Datenträgerverschlüsselung zu aktivieren. Nach der Einrichtung fällt diese Datenträgerverschlüsselung im Alltag kaum auf. Je nach System lassen sich

auch externe Datenträger, wie mobile Festplatten oder USB-Sticks, damit verschlüsseln.

Im Falle eines Verlusts können die Finder oder möglichen Diebe nicht oder zumindest nicht so einfach auf die Daten auf dem Gerät zugreifen. Dies kann auch zur Folge haben, dass ein entsprechender Vorfall zumindest nicht den Betroffenen gemeldet werden muss (Art. 34 Abs. 3 lit. a Datenschutz-Grundverordnung).

Mobile Device Management

Unternehmen mit vielen mobilen Geräten haben oftmals auch ein sogenanntes Mobile Device Management (MDM) im Einsatz. Diese Systeme erlauben im Bedarfsfall und je nach Hersteller und Gerät etwa die Lokalisierung des Geräts und die Fernlöschung von Daten. Sie sollten herausfinden, wen Sie im Falle eines Geräteverlusts im Unternehmen kontaktieren müssen, damit die möglichen Maßnahmen getroffen werden. ➤

- > Übrigens: Für private Smartphones stehen mit „Wo ist“ (Apple) und „Meine Geräte finden“ (Android) Ortungsmöglichkeiten und teilweise auch weiterführende Sicherheitsmaßnahmen zur Verfügung. Welche das sind und wie diese eingerichtet werden müssen, finden Sie unter nachfolgenden Links:

<https://support.apple.com/de-de/120340>

<https://kurzlinks.de/android-diebstahlschutz>

Starke Authentifizierung

Damit ein Finder oder Dieb eines Gerätes – auch mit aktivierter Datenträgerverschlüsselung – nicht auf die Daten zugreifen kann, ist es auch erforderlich, dass sich dieser nicht einfach einloggen kann. Der Zugang sollte so gut wie möglich abgesichert sein. Neben möglichst langen und kryptischen Passwörtern kann es je nach Gerät und Betriebssystem auch helfen, die Anmeldung nach mehreren Falscheingaben zu sperren.

Nicht vergessen: Datensicherung auch im mobilen Einsatz

Gerade wenn Sie möglicherweise viele Tage oder Wochen mobil arbeiten, sollten Sie sicherstellen, dass Ihre Daten auch außerhalb des Unternehmens gesichert werden. Einige Unternehmen und Anwender synchronisieren die Daten auf Mobilgeräten und sichern die dann synchronisierten Daten. Damit werden Daten etwa mit dem Onlinespeicher „OneDrive“ zuerst synchronisiert und die synchronisierten Daten werden zentral gesichert. Was teilweise aber übersehen wird, ist, dass die Synchronisation bei Nutzung des Mobilfunknetzes oder während des Roamings manchmal deaktiviert ist. Gerade bei längeren Auslandsaufenthalten ohne WLAN-Zugriff kann dies zur Folge haben, dass die Daten nicht synchronisiert und somit im späteren Back-up enthalten sind.

Denken Sie auch an eine Datensicherung von wichtigen Dokumenten und Belegen. Entsprechende Dokumente können je nach individuellen Gegebenheiten per Smartphone fotografiert oder mit entsprechenden Apps gescannt werden.

Sicherer Transport & Aufbewahrung

Mobiles Arbeiten in Verbindung mit langen An- und Abreisen kann sehr anstrengend und stressig sein. Verlorene und gestohlene Geräte sind deshalb nicht ungewöhnlich.

Deshalb sollten mobile Geräte, Datenträger und Dokumente während des Transports und später im Hotel

oder Einsatzort so sicher wie möglich aufbewahrt werden. Abschließbare Koffer und spezielle Geräteschlösser können hierzu hilfreich sein. Geräte und Datenträger mit sensiblen Daten sollten, wann immer möglich, nicht etwa im geparkten Fahrzeug bleiben.

Neugierige Einblicke verhindern

Beim mobilen Arbeiten am Bahnhof, Flughafen, Café oder auch beim Kunden kann Ihnen schnell jemand über die Schulter und auf den Bildschirm oder Ihr Dokument blicken. Um das Risiko zu minimieren, dass die Person sensible Daten einsehen kann, sollten Sie sich bestenfalls so setzen, dass niemand von hinten oder seitlich Ihren Bildschirm einsehen kann. Wenn Sie öfter unterwegs sind, kann eine Blickschutzfolie hilfreich sein, die seitlichen Einblicke zu verhindern.

Grenzkontrollen und Datenzugriff durch Behörden und Spionage

In einigen Ländern ist es erlaubt, dass bei der Einreise elektronische Geräte auch ohne richterlichen Beschluss durchsucht werden dürfen. Selbst die Herausgabe der Zugangsdaten kann teilweise verlangt oder die Geräte auch beschlagnahmt werden. Hinzu kommen immer wieder Berichte und Warnungen, dass Apps zur Spionage verwendet werden können. Entsprechende Apps sind dann etwa für die Registrierung für große Veranstaltungen erforderlich.

Je nach Situation kann es hilfreich sein, ein separates Gerät für entsprechende Reisen und Zwecke zu nutzen oder keine sensiblen Daten auf dem mitgeführten Gerät zu speichern. Falls Sie die Daten kurz vor Reiseantritt löschen, sollten Sie bedenken, dass diese über spezielle Tools möglicherweise wiederhergestellt werden können bzw. der Löschvorgang nachvollziehbar ist.

Vorsicht bei Gesprächen

Sicherlich achten Sie bei Gesprächen und Telefonaten unterwegs darauf, dass keine unerwünschten Mithörer dabei sind. Diese Vorsicht sollten Sie auch im Hotel walten lassen. Durch offene Fenster, Zwischentüren oder dünne Wände ist es teilweise möglich, die Gespräche und Telefonate vom Nachbarzimmer aus problemlos mitzuhören.

Entsorgung vertraulicher Unterlagen unterwegs

Möglicherweise fallen auf Ihrer Reise auch vertrauliche Unterlagen an, die Sie sicher und datenschutzkonform

>

entsorgen wollen. Sofern dies nicht etwa beim Kunden oder Geschäftspartner möglich ist, ist es häufig kein Problem, ein paar Seiten über den Hotel-Schredder (Partikel- und nicht Streifenschnitt) zu entsorgen. Geht auch das nicht, müssen diese Unterlagen im Zweifel zum Unternehmen mitgenommen werden. Die Unterlagen sollten nicht lesbar im Altpapier entsorgt werden.

Mobile Internetnutzung und WiFi

Gerade in Deutschland ist nicht überall mobiles Internet vorhanden und je nach Tarif ist auch das Datenvolumen eingeschränkt. Deshalb ist es oftmals notwendig, auf ein (kostenfreies) WLAN auszuweichen. Ob und in welchem Umfang das WLAN gesichert oder sogar

überwacht wird, ist oftmals unklar. Zudem gibt es die Möglichkeit, dass Kriminelle eigene WLANs anbieten und hierfür bekannte WLAN-Bezeichnungen verwenden. Verbinden sich Benutzer oder ggf. Geräte sogar automatisch damit, können die kriminellen Betreiber den Datenverkehr schlimmstenfalls ausforschen.

Die im Alltag einfachste Maßnahme, um sich zu schützen, ist der Einsatz eines „Virtual Private Network“ (VPN). Üblicherweise wird beim Einsatz von VPN der gesamte Internetverkehr über diese verschlüsselte und gesicherte Verbindung geleitet. Einige Unternehmen ermöglichen via VPN den Zugang in das Unternehmensnetzwerk bzw. Zugriff auf Unternehmensanwendungen. (ST)

WUSSTEN SIE SCHON? CAPTCHAS KÖNNEN GEFÄHRLICH SEIN!

Viele Webseiten- und Onlineshop-Betreiber schützen ihre Webformulare mit CAPTCHAs vor Missbrauch.

Nun wurde bekannt, dass Cyberkriminelle CAPTCHAs auch für Angriffe missbrauchen. Verdächtig wird es, wenn nach dem Setzen des Häkchens plötzlich die Aufforderung erscheint, eine Tastenkombination zu drücken. Diese Kombination löst einen Befehl aus, der zuvor unbemerkt in den Zwischenspeicher kopiert wurde – etwa beim Klick auf das CAPTCHA. Dadurch kann Schadsoftware heruntergeladen werden.

Laut Medienberichten verfügt die so eingeschleuste Schadsoftware über weitreichende Fähigkeiten: Sie kann Informationen sammeln oder Fernzugriffe auf den Rechner ermöglichen.

So können Sie sich schützen

Wenn Sie nach dem Lösen eines CAPTCHAs zur Eingabe einer Tastenkombination aufgefordert werden,

sollten Sie äußerste Vorsicht walten lassen. Führen Sie die Kombination nicht aus, bevor Sie Rücksprache mit dem Anbieter der Webseite oder einem internen IT-Ansprechpartner gehalten haben.

Falls Sie bereits betroffen sind, informieren Sie umgehend Ihre Sicherheits- oder IT-Verantwortlichen. Diese können prüfen, ob eine Infektion vorliegt und welche Maßnahmen, z. B. eine Neuinstallation oder Passwortänderung, notwendig sind.

Da Schadsoftware auch auf anderen Wegen auf das Gerät kommen kann, etwa über Schadsoftware-verseuchte Werbefbanner, sollten Sie im Alltag – wann immer es möglich ist – nur mit Benutzerkonten ohne administrative Rechte online tätig sein. Ein Virenschutz mit aktuellem Stand sollte ebenfalls aktiv sein. (ST)

Kontaktformular

Bitte Anliegen wählen



Anti-Roboter-Verifizierung

Hier klicken

FriendlyCaptcha

MOBILES ARBEITEN

Geschäftsreisen, mobiles Arbeiten beim Kunden, im Hotel oder auf Messen – die Arbeitswelt wird immer flexibler.

Doch je mehr wir außerhalb des Büros arbeiten, desto größer wird das Risiko, dass sensible Unternehmens- oder persönliche Daten in falsche Hände geraten.

In diesem Beitrag erfahren Sie, welche Gefahren bestehen und wie Sie Ihre Daten auf Reisen effektiv schützen. Scannen Sie dafür einfach den QR-Code.



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, 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: dlyastokiv – 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

© 2025 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau

