1/26

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER

ERNSTE LAGE DER IT-SICHERHEIT

Das sind die Herausforderungen für 2026

KÜNSTLICHE INTELLIGENZ AM ARBEITSPLATZ

Was ist hier wichtig für Sie?

powered by PRIVACYXPERTS

2026 – sicher, souverän, zuversichtlich

Liebe Leserinnen und Leser,

2026 wird ein Jahr, in dem wir gleichzeitig aufmerksam und mutig bleiben müssen. Die IT-Sicherheitslage bleibt angespannt: Cyberangriffe, Phishing, Lücken in Systemen und neue Methoden wie Vishing oder Angriffe auf KI-Dienste zeigen, dass digitale Risiken weiter wachsen.

Doch genauso klar ist: Wir sind ihnen nicht hilflos ausgeliefert. Schon kleine, konsequente Schritte – Updates, starke Passwörter, Mehr-Faktor-Anmeldung, ein kurzer Blick auf Links oder QR-Codes – erhöhen unsere Sicherheit erheblich.

Gleichzeitig hält KI längst Einzug in unseren Arbeitsalltag. Sie hilft uns beim Strukturieren, Formulieren und Denken, ohne uns zu ersetzen. Damit KI ein echter Gewinn bleibt, braucht es nur eine einfache Regel: keine personenbezogenen oder vertraulichen Daten eingeben. Werden Inhalte anonymisiert und Ergebnisse geprüft, wird KI zum täglichen Unterstützer, der Arbeit erleichtert und neue Ideen ermöglicht.

2026 wird damit zu einem Jahr bewusster Entscheidungen: Risiken ernst nehmen, Chancen nutzen, mit klugen Gewohnheiten Sicherheit schaffen und Digitalisierung aktiv gestalten. Wir begleiten Sie dabei – mit Rat, Aufmerksamkeit und einem offenen Ohr.

Auf ein Jahr voller Klarheit, guter Ideen und digitaler Stärke. Auf 2026!

Herzliche Grüße

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.

ERNSTE LAGE DER IT-SICHERHEIT: DAS SIND DIE HERAUSFORDERUNGEN FÜR 2026

Wie Sie wissen, ist eine sichere Verarbeitung personenbezogener Daten eine zentrale Anforderung der EU-Datenschutz-Grundverordnung (DSGVO). Kommt es zu einem Sicherheitsvorfall, also etwa zu einem erfolgreichen Hacking-Angriff, sind sehr häufig auch personenbezogene Daten betroffen. Dann greifen die Regelungen der DSGVO – inklusive möglicher Melde- und Benachrichtigungspflichten.

Die Lage der IT-Sicherheit: keine Entwarnung

Im Herbst hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) den aktuellen Bericht zur Lage der IT-Sicherheit veröffentlicht. Das Kurzfazit: Trotz positiver Trends gibt es keine Entwarnung, die Lage bleibt angespannt.

Mit welchen Bedrohungen Unternehmen aktuell rechnen müssen – und welche Maßnahmen das Risiko zumindest senken können –, zeigt dieser Beitrag anhand des Berichts, weiterer Quellen und Erfahrungen aus der Praxis.

Deutschland weltweit unter den Top 5 der angegriffenen Länder

Auch wenn es Sicherheitsbehörden immer wieder gelingt, kriminelle Hacker-Gruppen und deren Infrastruktur auszuschalten, bleiben APT- und Cybercrime-Gruppen die größten Bedrohungen für Unternehmen:

- **APT-Gruppen** (Advanced Persistent Threat) verfolgen meist geostrategische oder wirtschaftliche Ziele. Deutschland liegt nach den USA, Indien und Japan weltweit auf Platz vier der betroffenen Länder.
- **Cybercrime-Gruppen** sind vorwiegend an direktem finanziellem Gewinn interessiert. Dazu zählen etwa Ransomware-Gruppen, die Daten verschlüsseln und „Lösegeld" erpressen. Nach Statistiken wie ransomware.live liegt Deutschland hier nach den USA sogar auf Platz zwei der betroffenen Länder.

Schadprogramme, Phishing und QR-Betrug

Schadprogramme, Webseiten mit Schadsoftware und Phishing-Webseiten bleiben eine große Bedrohung. Die Anzahl der täglich neu entdeckten Schadsoftware-Varianten ist zwar auf durchschnittlich rund 280.000 gefallen, aber nach wie vor sehr hoch.

Phishing bleibt ebenfalls auf hohem Niveau. Ergänzend dazu gab es in einigen Städten Phishing-Angriffe mit QR-Codes, etwa auf Parkautomaten: Offizielle QR-Codes wurden überklebt und führten zu Bezahlseiten der Täter. Für den Alltag heißt das: weiterhin Vorsicht bei eingehenden Nachrichten wie auch bei der Nutzung von QR-Codes.

Bedrohungs-Trends: EDR-Killer und Vishing

Einige Entwicklungen richten sich gezielt gegen Schutzmaßnahmen oder nutzen neue Kommunikationswege:

- **EDR-Killer** sind Tools, mit denen Angreifer Schutzsysteme auf Endgeräten (Endpoint Detection and Response (der)), etwa Virenschutz, deaktivieren oder umgehen. Diese Werkzeuge werden auch von Ransomware-Gruppen verwendet. Verantwortliche sollten mit ihren IT-Dienstleistern oder internen Administratoren klären, ob die eingesetzten Schutzlösungen solche Angriffe erkennen oder abwehren können.
- **Vishing** (Voice Phishing) sind Phishing-Angriffe per Telefon oder Onlinegespräch. Angreifer nutzen Callcenter-Strukturen oder synthetische Stimmen. Das Ziel ist häufig, spontane Handlungen auszulösen: Einrichtung einer Fernwartung, Freigabe einer Überweisung oder Herausgabe von Zugangsdaten.

Beschäftigte sollten darauf vorbereitet sein, dass Kriminelle sie nicht nur per E-Mail, sondern auch telefonisch oder im Videocall ansprechen. Im Zweifel gilt: nicht unter Druck setzen lassen, Gespräch beenden und über einen bekannten Rückkanal nachfragen.

Das sind die zahlreichen Angriffsflächen

Zu den klassischen Angriffsflächen zählen online erreichbare Systeme wie Webseiten und Onlineanwendungen. Hinzu kommen Kommunikationssysteme, Schwachstellen in Hard- und Software sowie zunehmend vernetzte Geräte und KI-Dienste.

>

> Ergänzend zum BSI-Bericht gab es in den vergangenen Monaten zahlreiche Meldungen über Sicherheitslücken in Firewall-Systemen mehrerer Hersteller. Teilweise waren auch Wochen später noch verwundbare Systeme – auch in Deutschland – im Internet erreichbar. Einige dieser Lücken ermöglichten es Angreifern, Zugangsdaten auszulesen oder direkt in Unternehmensnetze einzudringen.

Weitere Angriffsflächen sind online angebundene Maschinen und Anlagen (z. B. Videoüberwachung, Solaranlagen, Produktionsmaschinen), IoT-Geräte, darunter auch Fahrzeuge und LLMs (Sprachmodelle) von KI-Anbietern, etwa ChatGPT.

Verantwortliche sollten prüfen (lassen), ob ihre Firewalls und übrigen Systeme von bekannten Schwachstellen betroffen sind, Updates einspielen und – falls möglich – Zugriffe auf notwendige Netze und Adressen beschränken.

Sicherheitsupdates: besonders für KMU eine Dauerbaustelle

Das BSI geht von durchschnittlich 119 neuen Schwachstellen pro Tag aus. Große Anbieter wie Microsoft schließen in ihrem monatlichen „Patchday" teilweise Dutzende dieser Lücken. Nicht jede Schwachstelle ist kritisch, aber einige ermöglichen es externen Angreifern oder eingeschleuster Schadsoftware, direkt Systeme zu übernehmen.

Die meisten Softwarehersteller stellen zeitnah Sicherheitsupdates bereit. Gerade kleine und mittlere Unternehmen (KMU) haben aber oft Schwierigkeiten, alle relevanten Lücken zu erkennen und Updates konsequent einzuspielen.

Positiv: Bei klassischen Arbeitsplatzrechnern wird die Update-Thematik durch automatische Updates und Monitoring-Systeme zunehmend besser. Häufig übersehen werden jedoch:

- kleinere lokal betriebene Fachanwendungen,
- Netzwerkgeräte wie Multifunktionsgeräte, Drucker, Smart-TVs sowie
- Smartphones und Tablets.

Diese Geräte hängen oft im selben Netzwerk wie Server und PCs, haben aber keine zusätzliche Schutzsoftware. Manche Systeme lassen sich über Suchmaschinen wie shodan.io gezielt auffinden – auch von Angreifern. Oftmals kennen IT-Verantwortliche aber nicht alle eingesetzten Anwendungen oder es gibt unklare Regelungen zur Verantwortlichkeit.

Was Sie tun können, um sich vor Angriffen zu schützen

Damit die vielen Informationen nicht nur theoretisch bleiben, sind hier die wichtigsten Maßnahmen kompakt zusammengefasst. Vorrang haben aber natürlich die individuellen Vorgaben Ihres Unternehmens:

1. Zugänge absichern

- Nutzen Sie, wann immer möglich, Mehr-Faktor-Authentifizierung (z. B. Zahlencode aus einer App).
- Stellen Sie – wo angeboten – auf Passkeys um. Sie gelten aktuell als sicher und werden von vielen Nutzern als komfortabel empfunden.

2. Vorsicht bei Nachrichten, QR-Codes und Anrufen

- Öffnen Sie Anhänge und Links nur, wenn Absender und Anlass plausibel sind. Im Zweifel lieber beim Absender nachfragen – über einen bekannten Rückkanal, nicht über die Kontaktdaten aus der Nachricht.
- Seien Sie bei QR-Codes skeptisch. Kontrollieren Sie die angezeigte Internetadresse, bevor Sie Daten eingeben.
- Legen Sie bei verdächtigen Anrufen oder Videocalls im Zweifel auf. Lassen Sie sich nicht zu spontanen Zahlungen, Installationen oder Fernwartungszugängen drängen. Klären Sie Rückfragen mit der IT, der Führungskraft oder der Bank über bekannte Kontaktdaten.

3. Updates und Zuständigkeiten klären

- Stellen Sie sicher, dass klar geregelt ist, wer für Updates zuständig ist: für Server, Fachanwendungen, Firewalls, Drucker, TK-Anlagen, Smartphones, Tablets und „smarte" Geräte, welche ggf. durch Sie in Betrieb genommen wurden.
- Bei extern bereitgestellten Systemen (z. B. Telefonanlage im Mietmodell, Drucker mit Wartungsvertrag) sollte vertraglich geregelt sein, wer Sicherheitsupdates einspielt.
- Prüfen Sie gemeinsam mit IT oder Dienstleistern, ob besonders kritische Systeme (z. B. Firewalls, VPN-Gateways, öffentlich erreichbare Server) auf dem aktuellen Stand sind.

4. Angriffsfläche verkleinern

- Prüfen Sie, ob Onlineanwendungen wirklich aus dem gesamten Internet erreichbar sein müssen

oder ob Zugriffe eingegrenzt werden können – z. B. auf bestimmte IP-Adressen oder per VPN.
- Setzen Sie nach Möglichkeit auf Netzwerk-Segmentierung: Maschinen, Kameras, Smart-TVs und ähnliche Geräte sollten nicht unbedingt im selben Netz wie zentrale Server und sensible Daten liegen. So wird ein möglicher Schaden begrenzt, falls ein System kompromittiert wird.

5. Aufräumen, archivieren und Vorfälle melden

- Alles, was nicht mehr vorhanden ist, kann auch nicht gestohlen, missbraucht oder veröffentlicht werden. Nutzen Sie den Jahresbeginn für einen **digitalen Frühjahrsputz:**
  - E-Mails, die nicht mehr benötigt werden, löschen (im Rahmen der Unternehmensvorgaben)
  - prüfen, ob zentrale Archivsysteme genutzt werden, sodass alte Unterlagen nicht zusätzlich in persönlichen Postfächern und Ordnern liegen müssen.
- Informieren Sie sich, **wo und wie Sie im Unternehmen Verdächtiges und Vorfälle melden** können – etwa suspekte E-Mails, ungewöhnliche Pop-ups oder Anrufe.

Gemeinsam gegen Kriminelle

Der BSI-Bericht zeigt: Die Bedrohungslage bleibt angespannt, aber Unternehmen und Beschäftigte sind dem nicht hilflos ausgeliefert.

Gerade in KMU hilft es, die eigene Sicherheitslage zumindest einmal im Jahr zu bewerten, mit den vorhandenen Maßnahmen abzugleichen und gezielt nachzubessern. Der Jahresbeginn ist dafür ein guter Zeitpunkt, um ein möglichst sicheres Jahr zu starten. (ST)

KI AM ARBEITSPLATZ: WAS IST HIER WICHTIG FÜR SIE?

KI ist längst kein Zukunftsversprechen mehr. Viele von Ihnen nutzen sie bereits im Alltag, oft ohne groß darüber nachzudenken. Ob Sie eine Formulierung verbessern lassen, sich einen Text erklären oder eine Idee ausarbeiten lassen möchten: Ein paar Klicks und schon arbeitet ein digitaler Assistent für Sie mit.

Deshalb wird es Zeit, dass wir diesen neuen Kollegen einmal offiziell begrüßen. Und wie bei jedem neuen Teammitglied lohnt es sich, kurz darüber zu sprechen, wie wir gut und sicher zusammenarbeiten. KI ist ein starkes Werkzeug und kann uns im Arbeitsalltag enorm unterstützen. Doch gerade beim Datenschutz verlangt sie ein bisschen Aufmerksamkeit. Nicht viel, aber genug, um sicherzustellen, dass keine sensiblen Informationen an Orte gelangen, die wir nicht kontrollieren können.

Durch einen klugen Umgang wird KI zu einem täglichen Helfer, der Ihnen Arbeit abnimmt, Kreativität schenkt und Ihnen Zeit zurückgibt.

Warum KI für Sie ein echter Gewinn sein kann – das sollten Sie beachten

Viele Mitarbeitende berichten, dass KI ihnen Aufgaben erleichtert, die sonst viel Energie kosten. Texte zusammenfassen, Ideen strukturieren, Formulierungen glätten, Tabellen umsortieren oder komplexe Inhalte verständlicher machen. Die Technik ist nicht fehlerfrei, aber sie liefert meist einen guten ersten Entwurf, den Sie nach Bedarf anpassen können.

Besonders hilfreich ist KI in Momenten, in denen man gedanklich feststeckt. Sie kennen das vielleicht: Man sitzt vor einem Dokument, weiß, was man sagen möchte, aber die richtigen Worte wollen einfach nicht kommen.

Ein KI-Tool kann hier Inspiration liefern und so etwas wie einen geduldigen Sparringspartner darstellen. Ohne Meckern, ohne Zeitdruck und mit erstaunlich viel Kreativität.

Mein Tipp:

Sie müssen einen Grundsatz beachten, der sich wie ein roter Faden durch diesen Artikel zieht. KI kann viel, aber sie weiß nicht, was vertraulich ist. Sie erkennt nicht automatisch, dass eine Kundennummer, eine interne E-Mail oder eine persönliche Information geschützt werden muss. Genau deshalb kommt es auf Ihren bewussten Umgang mit der künstlichen Intelligenz an.

>

> Die wichtigste Regel: keine personenbezogenen oder vertraulichen Daten eingeben

Wenn Sie sich nur einen Satz aus diesem Artikel merken, dann diesen: Bitte geben Sie in KI-Werkzeuge keine personenbezogenen Daten und auch keine internen Informationen wie Kundenlisten, Geschäftszahlen, vertrauliche Dokumente oder E-Mails ein. Dies gilt allerdings nicht für KI-Systeme, die lokal in Ihrem Unternehmen betrieben werden. Gängige KI-Tools verarbeiten Eingaben aber oft außerhalb des Unternehmens. Manchmal in anderen Ländern. Und häufig in Systemen, die wir nicht kontrollieren können. Es besteht nicht nur theoretisch die Möglichkeit, dass diese Daten gespeichert oder zur Verbesserung des Modells genutzt werden.

Mein Tipp:
Wenn Sie einen Text verbessern lassen möchten, entfernen Sie vorher sensible Inhalte. Formulieren Sie allgemein. Statt „Kundin Frau Müller hat uns gestern geschrieben" könnte es heißen: „Eine Kundin hat uns kürzlich kontaktiert." Schon ist der Vorgang anonym und risikofrei. Falls Sie unsicher sind, denken Sie kurz nach: Würde ich diese Information auch auf einer öffentlichen Seite posten? Wenn die Antwort Nein lautet, gehört sie nicht in ein KI-Eingabefeld.

5 typische KI-Stolperfallen im Büroalltag: Was muss ich konkret beachten?

Viele Fallen wirken harmlos. Deshalb hier ein paar klassische Situationen, in denen Mitarbeitende unbeabsichtigt gegen Datenschutzregeln verstoßen können. Mit einem entspannten Blick, aber einer klaren Botschaft:

1. Das „Kannst du schnell mal?"-Problem

Die KI soll einen E-Mail-Text umformulieren. Der ist schnell hineinkopiert. Dann merkt man: Ups. Da stehen Kundennamen und Auftragsnummern drin.

Mein Tipp:
Einfach vorab anonymisieren. Zwei Handgriffe und schon ist alles sicher.

2. Das Ideen-Brainstorming mit zu vielen Details

Man möchte ein Konzept entwickeln und erklärt der KI den gesamten Projektverlauf. Das klingt erst mal logisch. Aber interne Strategieinhalte haben in externen Tools nichts verloren.

Mein Tipp:
Bleiben Sie abstrakt. „Ein Projekt im Bereich Kundenservice" ist völlig ausreichend.

3. Der „Bitte analysiere dieses Dokument"-Wunsch

Der Klassiker. Ein PDF wird hochgeladen, weil die KI es zusammenfassen soll. Enthält das Dokument vertrauliche Inhalte, landet es automatisch außerhalb unserer sicheren Umgebung.

Mein Tipp:
Wenn Sie ein Dokument zusammenfassen lassen möchten, arbeiten Sie mit Auszügen oder anonymisierten Versionen.

4. Private KI-Accounts im beruflichen Kontext

Viele nutzen KI-Tools privat. Ein schneller Wechsel zum geschäftlichen Laptop und schon ist die berufliche Anfrage im privaten Account gelandet.

Mein Tipp:
Trennen Sie beruflich und privat konsequent. Das erspart Missgeschicke.

5. Die Archivfalle

Einige KI-Tools speichern Eingaben automatisch in einer Historie.

Mein Tipp:
Prüfen Sie die Einstellungen und löschen Sie alte Sessions regelmäßig.

Die goldene Dreierregel für den sicheren KI-Einsatz – so gehen Sie konkret vor

Damit Sie sich die wichtigsten Schritte gut merken können, hier eine einfache dreiteilige Faustformel, die Ihnen im Alltag Sicherheit gibt:

1. Regel: Anonymisieren

Entfernen Sie Namen, Adressen, Zahlen, interne Bezeichnungen oder andere Details, die jemanden identifizierbar machen.

2. Regel: Prüfen

Fragen Sie sich vor jeder Eingabe kurz, ob die Information auch extern geteilt werden dürfte. Wenn nicht, lassen Sie sie weg.

3. Regel: Nachbearbeiten

KI liefert Vorschläge. Sie entscheiden, ob diese korrekt, sinnvoll und angemessen formuliert sind. Der Mensch bleibt der Qualitätsfilter.

Mit dieser Dreierregel sind Sie jederzeit auf der sicheren Seite: Erst anonymisieren, dann prüfen, zuletzt nachdenken – so bleibt KI ein sicheres Werkzeug.

Fazit: Gemeinsamer Blick auf 2026

In diesem Jahr wird KI im Arbeitsalltag vieler Menschen ankommen. Das bedeutet für uns alle eine Mischung aus neuen Chancen und ein paar neuen Routinen. Vor allem aber stellt sie eine große Entlastung dar. Wenn wir bewusst und verantwortungsvoll mit der Technik umgehen, wird sie uns viele Wege erleichtern. Sehen Sie KI nicht als Bedrohung, sondern als ein Werkzeug, das, klug eingesetzt, einen echten Unterschied macht. Für Ihren Arbeitsalltag. Für unsere Sicherheit. Und für ein Unternehmen, das neugierig bleibt und neue Chancen sieht. Wir begleiten Sie dabei gern. Und wenn Sie eine Frage haben oder sich unsicher sind, wenden Sie sich einfach an Ihren Datenschutzbeauftragten. Er berät Sie gern und immer auf Augenhöhe.

Auf ein spannendes Jahr voller kluger Ideen und sicherer Entscheidungen. (AH)

WUSSTEN SIE SCHON? WARUM DER JANUAR DER GEFÄHRLICHSTE MONAT FÜR INTERNE DATENPANNEN IST

Wussten Sie, dass direkt nach der Weihnachtszeit besonders viele Datenschutzpannen passieren? Das liegt nicht an bösem Willen, sondern an lauter kleinen Gewohnheiten, die sich über die Feiertage einschleichen. Viele Mitarbeitende starten mit neuen Geräten ins Jahr. Neue Smartphones, frisch installierte Apps oder private Cloud-Back-ups können dabei schnell zu unerwarteten Stolperfallen werden.

Wussten Sie auch, dass E-Mails mit Weihnachtsgrüßen oft noch ungeöffnet im Posteingang liegen und manche davon gefährliche Anhänge enthalten? Angreifer nutzen die entspannte Stimmung gern aus. Ein harmlos aussehender Anhang mit „Weihnachtsfotos“ oder „Neujahrsrabatt“ reicht schon aus, um Schadsoftware einzuschleusen. Gerade im Januar sind viele Unternehmen davon betroffen, weil die Wachsamkeit nach den Feiertagen etwas nachlässt.

Und noch ein Punkt: der berühmte „Ich mache das gleich richtig sauber“-Vorsatz. Viele stürzen sich nach der Rückkehr ins Büro auf den überquellenden Schreibtisch. Doch beim hektischen Aufräumen wandern alte Ausdrucke oft in falsche Behälter oder bleiben offen liegen. Auch dadurch entstehen jedes Jahr Datenpannen.

Hinzu kommt, dass alte Nachrichten häufig weitergeleitet oder intern gespeichert werden, ohne ihren Ursprung noch einmal kritisch zu prüfen. So können sich Schadprogramme unbemerkt weiterverbreiten. Ein kurzer Blick auf Absender, Betreff und Anhang hilft oft schon, Risiken frühzeitig zu erkennen. Besonders kritisch wird es, wenn beim Aufräumen Unterlagen mit Kunden- oder Mitarbeiterdaten im normalen Papierkorb landen oder offen auf dem Schreibtisch liegen bleiben. Ordnung ist gut, kontrolliertes Aufräumen schützt jedoch vor unnötigen Datenschutzpannen.

Ergänzend lohnt sich ein bewusster Blick auf das E-Mail-Postfach. Löschen Sie alte Nachrichten, archivieren Sie nur das, was Sie wirklich noch benötigen, und prüfen Sie zweifelhafte Inhalte lieber ein zweites Mal.

Die gute Nachricht: Ein kurzer Sicherheitscheck zum Jahresstart wirkt wahre Wunder – Geräte prüfen, Cloud-Einstellungen checken, Papierablage bewusst sortieren und im E-Mail-Postfach lieber einmal mehr hinschauen als zu wenig. So starten Sie sicher und entspannt ins neue Jahr. (AH)

KURZFILM: IDENTITÄTSDIEBSTAHL

Identitätsdiebstahl beginnt oft harmlos – und endet mit echten Konsequenzen. Was Kriminelle mit gestohlenen Daten tun, überrascht viele Betroffene.

Vom Online-Shopping auf Ihren Namen bis zum Missbrauch bei Behörden. Dieser Kurzfilm zeigt reale Risiken, Warnsignale und was jetzt zählt.

Schauen Sie rein – bevor aus Ihren Daten ein Problem wird.

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 Suchy, Bonn, Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen, Bildrechte S. 1: Pixel Studio – AdobeStock.com, Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 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