2/26

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER

GUT GEMEINT, SCHLECHT GEMACHT

Wie Bequemlichkeiten im Arbeitsalltag zum Datenschutzproblem werden

DIGITALER FRÜHJAHRSPUTZ 2026

Warum alte E-Mails und Dateien ein Sicherheitsrisiko sind

powered by PRIVACYXPERTS

Zwischen Abkürzung und Aufräumen: Warum Datenschutz im Alltag beginnt

Liebe Leserinnen und Leser,

Hand aufs Herz: Wir alle wollen unsere Arbeit gut machen. Schnell, pragmatisch, lösungsorientiert. Und genau deshalb greifen wir im Alltag manchmal zu kleinen Abkürzungen. Die Datei schnell an die private Mail schicken, die Liste kurz fotografieren, dem Kollegen fix das Passwort geben. Gut gemeint – und meistens ohne böse Absicht.

Gleichzeitig sammeln sich über Jahre hinweg E-Mails, Dateien, Scans und Notizen an, die „man vielleicht noch mal braucht". Der Posteingang wächst, Ordner quellen über, alte Dokumente wandern von Rechner zu Rechner. Irgendwann verliert man den Überblick – und merkt gar nicht mehr, was alles noch da ist.

Beides hat mehr miteinander zu tun, als man auf den ersten Blick denkt. Denn Datenschutz- und Sicherheitsprobleme entstehen selten durch große, spektakuläre Fehlentscheidungen, sondern durch viele kleine, alltägliche Gewohnheiten. Durch Bequemlichkeit. Durch Zeitdruck. Durch das Gefühl: „Das wird schon passen."

Datenschutz funktioniert nicht mit Angst, sondern mit Bewusstsein. Nicht mit Schuldzuweisungen, sondern mit klaren Regeln und gegenseitiger Unterstützung. Jeder aufgeräumte Ordner, jede vermiedene Abkürzung, jedes gelöschte Altdokument reduzieren Risiken. Am Ende schützen wir damit nicht nur Daten. Wir schützen Menschen. Wir schützen unser Unternehmen. Und wir schützen uns selbst. Und vielleicht ist genau jetzt ein guter Moment, damit anzufangen.

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.

GUT GEMEINT, SCHLECHT GEMACHT – WIE KLEINE BEQUEMLICHKEITEN IM ARBEITSALLTAG ZUM DATENSCHUTZPROBLEM WERDEN

Kennen Sie das? Der Drucker streikt, also schicken Sie sich die Datei schnell an Ihre private E-Mail-Adresse. Oder Sie fotografieren mit dem privaten Smartphone eine Kundenliste ab, weil Sie diese im Homeoffice brauchen. Alles praktische Lösungen, oder?

Leider nein. Denn genau solche Bequemlichkeiten sind oft der Anfang ernsthafter Datenschutzprobleme. Nicht, weil Sie böse Absichten haben. Sondern weil Sie einfach Ihre Arbeit erledigen wollen. Deshalb möchte ich Ihnen heute zeigen, wo die typischen Stolperfallen lauern und wie Sie diese vermeiden.

Private E-Mail-Adressen und Messenger: Was muss ich dazu wissen?

Sie sind unterwegs und brauchen dringend ein Dokument. Also schicken Sie es sich an Ihre Gmail-Adresse. Oder Sie fragen den Kollegen per WhatsApp schnell nach der Kundennummer von Frau Müller.

Private E-Mail-Dienste und Messenger erfüllen allerdings nicht unsere Sicherheitsstandards. Die Daten liegen auf Servern, über die wir keine Kontrolle haben. Und Sie haben faktisch eine Kopie sensibler Informationen außerhalb des Unternehmens angelegt.

Mein Tipp:

Nutzen Sie ausschließlich Ihre dienstliche E-Mail-Adresse und unsere freigegebenen Kommunikationskanäle. Wenn Sie von unterwegs auf Dokumente zugreifen müssen, verwenden Sie unsere bereitgestellten Tools. Falls diese nicht funktionieren, wenden Sie sich an die IT. Das mag umständlicher erscheinen, ist aber der einzig sichere Weg.

Cloud-Speicher und das Smartphone als Scanner: Was daran ist gefährlich?

Dropbox, Google Drive, WeTransfer – herrlich praktisch für große Dateien. Aber wenn Sie Unternehmensdaten in einen privaten Cloud-Speicher hochladen, verlieren Sie die Kontrolle darüber. Wir wissen nicht, wo die Daten gespeichert werden und wer noch Zugriff darauf hat.

Gleiches gilt für das schnelle Foto der Teilnehmerliste mit Ihrem privaten Smartphone. Damit haben Sie personenbezogene Daten auf Ihrem Gerät gespeichert. Diese werden möglicherweise automatisch in eine Cloud synchronisiert oder sind für andere Apps zugänglich.

Mein Tipp:

Verwenden Sie ausschließlich unsere bereitgestellten Cloud- und Sharing-Lösungen. Fotografieren Sie keine geschäftlichen Dokumente mit Ihrem privaten Smartphone. Nutzen Sie stattdessen die dienstlichen Geräte und Anwendungen.

Passwörter teilen und Zugänge weitergeben: Ist das gefährlich?

Ihr Kollege braucht dringend Zugriff auf ein System, sein Account funktioniert nicht. Also geben Sie ihm kurz Ihre Zugangsdaten. Problem gelöst?

Nein. Mit Ihren Zugangsdaten werden alle Aktionen unter Ihrem Namen protokolliert. Sie haften also für alles, was mit Ihrem Account passiert. Außerdem umgehen Sie damit bewusst unser Berechtigungskonzept.

Mein Tipp:

Teilen Sie niemals Ihre Passwörter oder Zugangsdaten. Wenn ein Kollege Zugriff auf ein System benötigt, muss er einen eigenen Account erhalten. Wenden Sie sich an die IT. Ja, das dauert manchmal länger. Aber es ist die einzige korrekte Vorgehensweise.

Ausdrucke und Notizen am Arbeitsplatz: Was muss ich dabei beachten?

Sie drucken eine Liste aus und lassen sie auf dem Drucker liegen. Oder Sie notieren eine Kundennummer auf einem Post-it und kleben es an den Monitor. Beides erscheint harmlos.

Aber jeder, der vorbeikommt, kann diese Informationen sehen. Das kann ein Kollege aus einer anderen

>

> Abteilung sein, ein Besucher oder die Reinigungskraft. Personenbezogene Daten sollen nicht offen sichtbar sein.

Mein Tipp:

Holen Sie Ihre Ausdrucke sofort vom Drucker ab. Lassen Sie keine Dokumente mit personenbezogenen Daten offen auf dem Schreibtisch liegen. Wenn Sie Notizen machen müssen, bewahren Sie diese sicher auf und vernichten Sie sie nach Gebrauch ordnungsgemäß. Und sperren Sie Ihren Bildschirm, wenn Sie den Arbeitsplatz verlassen.

USB-Sticks und externe Datenträger: Darf ich das nutzen?

Ein USB-Stick ist praktisch, um Daten schnell zu transportieren. Aber USB-Sticks gehen auch schnell verloren. Und wenn darauf personenbezogene oder vertrauliche Daten gespeichert sind, haben wir ein ernsthaftes Problem.

Ein USB Stick passt in jede Tasche. Und genau deshalb verschwindet er oft unbemerkt. Im Auto, im Zug oder auf dem Schreibtisch eines anderen. Wer ihn findet, braucht keine besonderen Kenntnisse.

Einstecken reicht. Und schon sind die Daten offen zugänglich. Nicht für Kollegen, sondern für Unbefugte. Aus einem kleinen Hilfsmittel wird so schnell ein echtes Risiko.

Mein Tipp:

Vermeiden Sie die Nutzung von USB-Sticks für geschäftliche Daten. Nutzen Sie stattdessen unsere Netzwerklaufwerke oder Cloud-Dienste. Falls Sie ausnahmsweise einen USB-Stick verwenden müssen, stellen Sie sicher, dass er verschlüsselt und freigegeben ist.

Homeoffice und mobiles Arbeiten: Wie verhalte ich mich richtig?

Im Homeoffice verschwimmen die Grenzen zwischen Privat und Geschäftlich oft. Das Kundendokument liegt neben dem Einkaufszettel. Das Diensthandy nutzt der Partner mal kurz. Der Sohn schaut über Ihre Schulter.

All das sind potenzielle Datenschutzprobleme. Auch im Homeoffice gelten dieselben Regeln wie im Büro.

Mein Tipp:

Richten Sie sich einen festen, abgegrenzten Arbeitsplatz ein. Lassen Sie keine Dokumente offen liegen. Sperren Sie Ihren Bildschirm, wenn Sie den Raum verlassen. Geben Sie dienstliche Geräte nicht an Familienmitglieder weiter. Und vernichten Sie Ausdrucke mit personenbezogenen Daten ordnungsgemäß.

Was passiert, wenn es schiefgeht? Wie verhalte ich mich richtig?

Vielleicht denken Sie jetzt: „Das ist alles übertrieben. Mir ist noch nie etwas passiert."

Aber Datenpannen geschehen oft unbemerkt. Und wenn es auffliegt, sind die Konsequenzen real. Für unser Unternehmen können empfindliche Bußgelder drohen. Für Sie persönlich kann es arbeitsrechtliche Folgen haben. Und für die betroffenen Personen kann ein Datenschutzverstoß erheblichen Schaden bedeuten.

Ihre Checkliste für den Alltag

- Nutzen Sie ausschließlich Ihre dienstliche E-Mail-Adresse für geschäftliche Kommunikation.
- Verwenden Sie nur freigegebene Kommunikationskanäle und Tools.
- Fotografieren Sie keine geschäftlichen Dokumente mit Ihrem privaten Smartphone.
- Teilen Sie Ihre Zugangsdaten mit niemandem.
- Holen Sie Ausdrucke sofort ab und räumen Sie Ihren Schreibtisch auf.
- Nutzen Sie keine privaten Cloud-Dienste oder USB-Sticks für Unternehmensdaten.
- Achten Sie auch im Homeoffice auf Datenschutz und Vertraulichkeit.

Fazit: Wir schaffen das gemeinsam

Datenschutz funktioniert nur, wenn wir alle mitmachen. Jeder Einzelne trägt Verantwortung. Die gute Nachricht: Es ist gar nicht so schwer, wenn Sie ein paar grundlegende Regeln beachten.

Nehmen Sie sich die Zeit, kurz innezuhalten, bevor Sie zu einer vermeintlich praktischen Abkürzung greifen. Fragen Sie sich: Ist das wirklich datenschutzkonform? Und wenn Sie unsicher sind, sprechen Sie mich gerne an. Ich helfe Ihnen weiter.

Denn am Ende schützen wir nicht nur die Daten anderer Menschen. Wir schützen auch uns selbst und unser Unternehmen. (AH)

DIGITALER FRÜHJAHRSPUTZ 2026: WARUM ALTE E-MAILS UND DATEIEN ZUM SICHERHEITSRISIKO WERDEN

Der Frühling steht traditionell für Ordnung und Neuanfang. Was für Keller, Garage oder Büro gilt, ist im digitalen Alltag oft längst überfällig. In Unternehmen sammeln sich über Jahre hinweg E-Mails, Dateien und Notizen an, die oftmals niemand mehr benötigt – die aber im Falle eines Sicherheitsvorfalls erhebliche Schäden verursachen können. Dabei geht es nicht nur um Ordnung oder Speicherplatz, sondern um IT-Sicherheit, Datenschutz und Schadensbegrenzung, im Falle eines erfolgreichen unbefugten Zugriffs.

Vergessene Daten sind besonders gefährlich

Moderne Schadsoftware und aktuelle Angriffe beschränken sich längst nicht mehr darauf, Systeme „nur" zu verschlüsseln. Häufig werden vor oder parallel zu einem Angriff gezielt Daten abgegriffen.

So wird etwa durch Schadsoftware Zugriff auf die vorhandene E-Mail-Korrespondenz erlangt, um weitere Schadsoftware an diese zu versenden. Damit sollen weitere Unternehmen zum Opfer werden.

Teilweise greifen Kriminelle auch auf online erreichbare E-Mail-Postfächer zu, um entsprechende E-Mails manuell zu versenden.

Häufig werden auch Daten aus lokalen Verzeichnissen oder zentralen Netzlaufwerken zuerst kopiert, bevor diese verschlüsselt werden. Denn zahlt das Unternehmen kein „Lösegeld" für die Entschlüsselung, wird mit einer Veröffentlichung gedroht. Da viele Unternehmen sich weigern, werden die Daten dann veröffentlicht.

Leider befinden sich unter den erbeuteten Daten oft sensible und eigentlich nicht mehr notwendige Daten. Diese sind als Dateien sowohl in der Dateiablage als auch als Anhang in E-Mails gespeichert. Bei der Analyse veröffentlichter Daten finden sich regelmäßig unter anderem:

- Ausweiskopien,
- Vertragsunterlagen,
- Zugangsdaten,
- eingescannte Dokumente,
- sensible interne Kommunikation.

Je mehr unnötige Daten vorhanden sind, desto größer ist der mögliche unnötige Schaden im Ernstfall.

Bitte nicht übersehen: Nahezu immer müssen die Aufsichtsbehörde und je nach Sensibilität auch die Betroffenen bzw. im Fall der Auftragsverarbeitung auch die Auftraggeber über den Vorfall informiert werden.

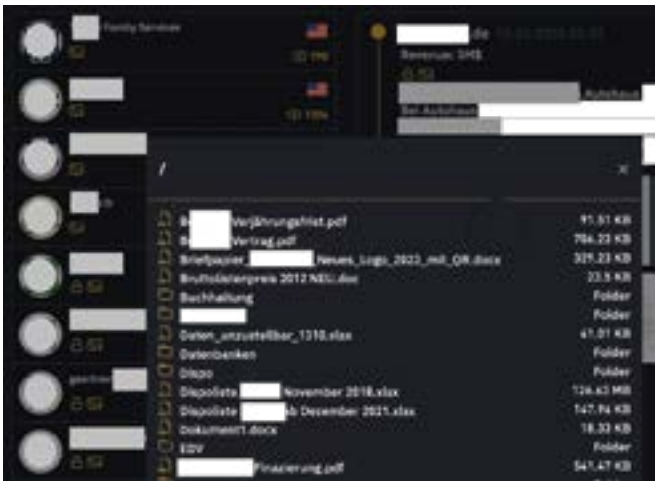

Bild: Screenshot „Veröffentlichte Daten eines zentralen Dateiservers im Darknet"

IT-Sicherheit endet nicht bei der IT-Abteilung

Die IT kümmert sich üblicherweise um die Infrastruktur, die Systeme, die Zugriffsrechte, die Datensicherung und – sofern vorhanden – um die Archivierungslösungen. Was sie jedoch nicht leisten kann, ist die fachliche Bewertung der einzelnen Inhalte. Nur die Nutzerinnen und Nutzer selbst wissen häufig, welche E-Mails erledigt, welche Dateien Arbeitskopien und welche Informationen doppelt oder veraltet sind. Genau hier setzt der digitale Frühjahrsputz an.

Hinzu kommt: Viele Daten liegen mehrfach vor – etwa als E-Mail-Anhang, als lokale Datei und zusätzlich in einem führenden System wie ERP, CRM oder DMS. Doppelte Datenspeicherung erhöht das Risiko, ohne einen Mehrwert zu schaffen.

Nicht wahllos löschen – Regeln beachten

Ein digitaler Frühjahrsputz bedeutet nicht, wahllos Daten zu löschen. Vor dem Löschen sollte immer geklärt werden:

>

- Gibt es eine zentrale E-Mail-Archivierung?
- Werden Dokumente zentral archiviert?
- Welche Aufbewahrungsfristen gelten?
- Welche internen Regelungen sind zu beachten?

Sind Daten ordnungsgemäß archiviert oder existieren sie in einem führenden System, können lokale Kopien und alte E-Mails oftmals gelöscht werden.

Im Zweifel sollte Rücksprache mit der IT oder dem Datenschutzbeauftragten erfolgen.

Beispiel

Ein sehr pragmatischer Ansatz in einem mittelständischen Unternehmen, den zentralen Datei-Server zu bereinigen, war folgender: Im Unternehmen wurde eine neue Verzeichnisstruktur festgelegt. Die Beschäftigten wurden gebeten, nur die absolut notwendigen Daten dort hinzuschieben, welche sie benötigen. Die anderen Daten wurden (mehrfach) auf externe Platten kopiert. Damit konnten sich alle Beschäftigten sicher sein, dass sie im Bedarfsfall auf die Daten zugreifen können, und beruhigt nur die notwendigen Daten in das neue Verzeichnis schieben.

Zentrale moderne Speichersysteme und Anwendungen erlauben zudem zunehmend, Speicher- und Löschfristen festzulegen, womit man sich im Anschluss eine manuelle Bereinigung sparen kann.

Checkliste: Digitaler Frühjahrsputz im Unternehmen

Bereich	Prüffragen
PC/Notebook	Benötige ich alle lokalen Dateien noch? Sind sie in der Datensicherung enthalten?
Zentrale Ablagen	Sind die Daten aktuell, doppelt oder überholt? Bestehen klare Ablagestrukturen?
Mobile Geräte	Welche Apps speichern Daten lokal? Sind Inhalte gesichert und notwendig?
Bilder und Videos	Enthalten Fotos oder Videos personenbezogene oder sensible Daten? Werden sie noch benötigt?
E-Mails	Können E-Mails gelöscht werden, etwa weil diese zentral archiviert werden oder nicht mehr erforderlich und aufbewahrungspflichtig sind?
Messenger und Chats	Enthalten Nachrichten (Messenger) oder Beiträge in Kanälen (z. B. Microsoft Teams) personenbezogene oder sensible Daten? Werden sie noch benötigt?
Kontakte und Termine	Enthalten Kontakte und Termine sensible (personenbezogene) Informationen oder Anhänge, die nicht mehr erforderlich sind?
Notizen und Notizbücher	Enthalten Notizbücher sensible (personenbezogene) Einträge?
Downloads und Scans	Wurden temporäre Ordner, Scan- und Download- Verzeichnisse geprüft und nicht mehr benötigte Dateien gelöscht?
Aushänge oder Einträge im Intranet	Enthalten Aushänge oder Intraneteinträge nicht mehr benötigte sensible (personenbezogene) Daten?

Fazit:

Das Löschen von Daten nach Wegfall des Zwecks oder Ablauf der Aufbewahrungsfrist ist nicht nur eine datenschutzrechtliche Pflicht. Es ist auch eine wirksame Maßnahme zur Reduzierung von möglichen Schäden. Denn Daten, die nicht mehr vorhanden sind, können weder gestohlen, missbraucht noch unbefugt veröffentlicht werden.

Ein regelmäßiger digitaler Frühjahrsputz schützt Unternehmen, Beschäftigte und Betroffene gleichermaßen – und sollte fester Bestandteil der IT- und Datenschutzpraxis sein. (ST)

WUSSTEN SIE SCHON? EU-OMNIBUS, DSGVO-REFORM UND MÖGLICHE ÄNDERUNGEN IM DEUTSCHEN DATENSCHUTZRECHT

Auf EU-Ebene wird derzeit an einer Bündelung und Vereinfachung verschiedener Digital- und Datenrechtsvorgaben gearbeitet. Das Ziel ist es, bestehende Regelungen – etwa aus der Datenschutz-Grundverordnung (DSGVO), dem Data Act, dem Data Governance Act oder der KI-Verordnung – besser aufeinander abzustimmen und Unternehmen zu entlasten, ohne das Schutzniveau grundsätzlich abzusenken.

Parallel dazu wird auch über Anpassungen der DSGVO selbst diskutiert. Im Fokus sollten dabei vor allem stehen:

- Entlastungen für kleine und mittlere Unternehmen,
- klarere Abgrenzungen von Pflichten sowie
- praxisnähere Dokumentationsanforderungen.

Auch auf nationaler Ebene gibt es Bewegung. Bei der Besprechung des Bundeskanzlers mit den Regierungschefinnen und -chefs der Länder am 4.12.2025 wurde unter anderem vereinbart, Vorschläge zu erarbeiten,

- um bis zum 31.12.2026 die Benennungspflicht für Datenschutzbeauftragte im nicht öffentlichen Bereich anzupassen und
- bis spätestens 31.12.2027 Regelungen zur Anonymisierung und Pseudonymisierung im Kontext des KI-Trainings und KI-Einsatzes vorzuschlagen.

Weiterhin soll in verschiedenen Kontexten die Schriftform durch die Textform ersetzt werden. Damit sollen Ausdrucke mit Unterschriften erheblich reduziert werden.

Wichtig:

Aktuell handelt es sich um Absichtserklärungen und Vorschläge. Solange keine gesetzlichen Änderungen in Kraft treten, gelten die bestehenden Regelungen unverändert weiter. Unternehmen sollten die aktuellen Entwicklungen aber beobachten, um frühzeitig mögliche Auswirkungen zu erkennen und notwendige Maßnahmen einleiten zu können. (ST)

KURZFILM: MULTI-FAKTOR-AUTHENTIFIZIERUNG

Multi-Faktor-Authentifizierung gilt als Goldstandard der IT-Sicherheit – doch sie ist kein unüberwindbares Hindernis. Cyberkriminelle haben längst raffinierte Methoden entwickelt, um auch MFA auszuhebeln.

In unserem Video zeigen wir, wie diese Angriffe funktionieren, wo die größten Risiken liegen und warum ein falsches Sicherheitsgefühl gefährlich sein kann. Jetzt reinschauen und erfahren, wie Angreifer wirklich vorgehen.

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: Ryhaysurjo S. 7 Angeline – beide 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