4/26

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER

PHISHING 2.0

Wenn die Betrugs-Mail plötzlich in perfektem Deutsch formuliert ist

DATEN RICHTIG WEITERGEBEN

Datenschutzkonformer Austausch mit anderen Organisationen 2026

powered by
PRIVACYXPERTS

Datenschutz beginnt mit Bewusstsein

Liebe Leserinnen und Leser,

Datenschutz wirkt im Arbeitsalltag oft wie ein Thema für Spezialisten: juristische Begriffe, technische Maßnahmen und umfangreiche Regelwerke. Doch in der Praxis begegnet uns Datenschutz vor allem in ganz alltäglichen Situationen. Eine E-Mail wird geöffnet, ein QR-Code gescannt, eine Telefonnummer an einen Dienstleister weitergegeben oder eine Liste an ein Partnerunternehmen geschickt. Genau in diesen Momenten entscheidet sich, ob Daten sicher bleiben – oder ob Risiken entstehen.

Doch nicht nur Angriffe von außen stellen Unternehmen vor Herausforderungen. Auch der Austausch von Daten mit Dienstleistern, Behörden oder anderen Unternehmen gehört zum normalen Geschäftsalltag. Dabei gilt: Daten dürfen weitergegeben werden – aber nur, wenn klar ist, wer sie verarbeitet, zu welchem Zweck und auf welcher rechtlichen Grundlage.

Die gute Nachricht ist: Wirksamer Datenschutz beginnt nicht mit komplizierten Maßnahmen, sondern mit Bewusstsein. Ein kurzer Moment des Innehaltens vor dem Klick oder eine frühzeitige Abstimmung bei der Weitergabe von Daten können bereits einen großen Unterschied machen.

Diese Ausgabe zeigt, wie sich digitale Betrugsversuche weiterentwickeln und worauf Sie achten sollten. Gleichzeitig erfahren Sie, unter welchen Voraussetzungen Daten mit anderen Organisationen ausgetauscht werden dürfen. Denn wer die Regeln kennt und aufmerksam bleibt, schützt nicht nur Informationen – sondern auch Menschen, Vertrauen und das Unternehmen insgesamt.

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.

PHISHING 2.0 – WENN DIE BETRUGS-MAIL PLÖTZLICH IN PERFEKTEM DEUTSCH FORMULIERT IST

Stellen Sie sich vor. Sie öffnen morgens Ihr E-Mail-Postfach und finden eine Nachricht Ihrer Hausbank. Perfektes Deutsch. Korrektes Logo. Persönliche Anrede. Die Bank bittet Sie, Ihre Zugangsdaten im Rahmen einer Systemmigration zu bestätigen. Klingt seriös. Ist es aber nicht.

Willkommen in der Welt von Phishing 2.0. Die Zeiten, in denen Sie Betrugs-Mails an holprigem Deutsch und merkwürdigen Absenderadressen erkennen konnten, sind endgültig vorbei. Angreifer setzen heute künstliche Intelligenz (KI) ein, um täuschend echte Nachrichten zu erzeugen. Und das betrifft längst nicht nur Ihr privates Postfach. Auch Ihr berufliches E-Mail-Konto steht im Visier.

In dieser Ausgabe zeigen wir Ihnen, welche neuen Tricks die Angreifer verwenden. Und vor allem, wie Sie sich und unser Unternehmen davor schützen können.

Warum die alten Faustregeln nicht mehr funktionieren: Was hat sich verändert?

Noch vor zwei Jahren konnte man viele Phishing-Mails auf den ersten Blick erkennen. Grammatikfehler. Seltsame Formulierungen. Unpersönliche Anreden wie „Sehr geehrter Kunde“. Daran konnte man sich orientieren. Doch diese Merkmale verschwinden gerade.

Kriminelle nutzen heute KI-Modelle, um Nachrichten in fehlerfreiem Deutsch zu verfassen. Die Texte klingen wie echte Unternehmenskommunikation. Sie verwenden das korrekte Corporate Design, die richtigen Logos und sogar aktuelle Geschäftsvorgänge als Aufhänger. Seit Anfang Februar 2026 beobachten Sicherheitsbehörden eine massive Welle solcher Angriffe auf deutsche Unternehmen und Privatpersonen.

Das Bundesamt für Sicherheit in der Informationstechnik und der Verfassungsschutz haben Anfang Februar gemeinsam vor einer neuen Angriffsform gewarnt: Phishing über Messenger-Dienste wie Signal. Die Angreifer haben es dabei nicht nur auf Passwörter abgesehen. Sie greifen gezielt die Zwei-Faktor-Authentifizierung an. Und sie tun das so geschickt, dass selbst erfahrene Nutzer Schwierigkeiten haben, den Betrug zu erkennen.

Mein Tipp:

Verlassen Sie sich nicht mehr auf Rechtschreibfehler als Erkennungsmerkmal. Achten Sie stattdessen auf den Kontext. Werden Sie zu einer ungewöhnlichen Handlung aufgefordert? Wird Zeitdruck aufgebaut? Dann ist höchste Vorsicht geboten.

Quishing, Smishing & Co.: Welche neuen Angriffsformen gibt es?

Phishing kommt längst nicht mehr nur per E-Mail. Die Angreifer nutzen heute jeden Kanal, der ihnen zur Verfügung steht. Und sie kombinieren verschiedene Kanäle geschickt miteinander.

Quishing nennt man Phishing über QR-Codes. Sie finden einen gefälschten QR-Code auf einem Aushang, in einer E-Mail oder sogar auf einem Parkscheinautomaten. Beim Scannen landen Sie auf einer manipulierten Webseite, die Ihre Zugangsdaten abgreift. Das Tückische daran ist, dass Sie die Zieladresse eines QR-Codes vor dem Scannen nicht sehen können, wenn Sie diese Funktion nicht aktiviert haben. Sie kaufen also die Katze im Sack.

Smishing ist Phishing per SMS. Sie erhalten eine Kurznachricht, angeblich von Ihrer Bank, einem Paketdienst oder einer Behörde. Der enthaltene Link führt auf eine gefälschte Seite. Besonders gefährlich ist das auf dem Smartphone, weil dort die vollständige URL oft nicht sichtbar ist. Ein Tipp auf den Link reicht aus.

Vishing bezeichnet den telefonischen Betrug. Ein Anrufer gibt sich als IT-Mitarbeiter, Bankberater oder Behördenvertreter aus. Dank KI können die Täter heute sogar Stimmen täuschend echt nachahmen. Der vermeintliche Anruf vom Geschäftsführer, der dringend eine Überweisung braucht, kann vollständig gefälscht sein.

Mein Tipp:

Scannen Sie keine QR-Codes aus unbekannten Quellen. Klicken Sie keine Links in SMS an. Und wenn Sie ein ungewöhnlicher Anruf erreicht, legen Sie auf und rufen Sie über die Ihnen bekannte offizielle Nummer zurück. Das ist kein Misstrauen. Das ist gesunder Menschenverstand.

>

> Phishing im Büroalltag: Wie erkenne ich einen Angriff?

Die wichtigste Erkenntnis lautet. Es geht nicht mehr darum, wie eine Nachricht aussieht. Es geht darum, was sie von Ihnen will.

Phishing-Nachrichten erzeugen fast immer Druck. Ihr Konto wird gesperrt. Eine Frist läuft ab. Ein Vorgesetzter braucht sofort eine Überweisung. Eine Systemmigration steht an und Sie müssen jetzt handeln. Genau dieser Zeitdruck soll Sie daran hindern nachzudenken. Denn wer in Eile ist, klickt schneller.

Achten Sie auf diese Warnsignale: Die Nachricht fordert Sie auf, einen Link anzuklicken oder einen Anhang zu öffnen. Sie sollen Zugangsdaten eingeben oder bestätigen. Die Nachricht kommt unerwartet, auch wenn der Absender bekannt erscheint. Es wird Dringlichkeit suggeriert. Oder die Nachricht enthält eine ungewöhnliche Bitte, etwa eine Zahlung auf ein neues Konto.

Besonders hinterhältig sind interne Phishing-Mails. Der Absender scheint ein Kollege oder Vorgesetzter zu sein. Die Mail bezieht sich auf ein laufendes Projekt. Alles wirkt vertraut. Trotzdem kann der Absender gefälscht sein. Auch intern heißt nicht automatisch sicher.

Mein Tipp:

Wenn eine Nachricht Sie unter Druck setzt, halten Sie inne. Genau dieser Moment des Innehaltens ist Ihr bester Schutz. Prüfen Sie die Absenderadresse genau. Rufen Sie im Zweifel den vermeintlichen Absender an. Und leiten Sie verdächtige Mails nicht weiter, sondern melden Sie diese direkt an die IT.

Was tun, wenn ich doch geklickt habe? Wie verhalte ich mich richtig?

Vielleicht ist es Ihnen schon passiert. Sie haben auf einen Link geklickt und merken erst danach, dass etwas nicht stimmt. Das kann jedem passieren. Wichtig ist jetzt, wie Sie reagieren.

Trennen Sie Ihr Gerät sofort vom Netzwerk. Informieren Sie umgehend die IT-Abteilung. Ändern Sie Ihre Passwörter, falls Sie Zugangsdaten eingegeben haben. Und dokumentieren Sie, was passiert ist. Welche Mail war es? Wann haben Sie geklickt? Was haben Sie eingegeben?

Wichtig ist vor allem, dass Sie den Vorfall melden. Auch wenn es Ihnen unangenehm ist. Niemand wird Ihnen einen Vorwurf machen. Im Gegenteil. Frühes Melden kann verhindern, dass aus einem kleinen Fehler ein großes Problem wird. Jede verschleppte Meldung dagegen gibt den Angreifern mehr Zeit, Schaden anzurichten.

Mein Tipp:

Melden ist kein Zeichen von Schwäche. Es ist verantwortungsvolles Handeln. Je schneller wir von einem Vorfall erfahren, desto besser können wir reagieren und Schäden begrenzen. Denken Sie daran. Sie schützen damit nicht nur sich selbst, sondern auch Ihre Kolleginnen und Kollegen.

Ihre Checkliste gegen Phishing 2.0

- Klicken Sie niemals auf Links in unerwarteten Nachrichten. Rufen Sie Webseiten immer manuell im Browser auf.
- Öffnen Sie keine Anhänge von unbekannten oder unerwarteten Absendern.
- Achten Sie auf Zeitdruck und Dringlichkeit als Warnsignal.
- Prüfen Sie die Absenderadresse genau. Auch wenn der Name vertraut klingt.
- Scannen Sie keine QR-Codes aus unbekannten oder ungeprüften Quellen.
- Geben Sie niemals Zugangsdaten über Links in E-Mails oder SMS ein.
- Melden Sie verdächtige Nachrichten sofort an die IT-Abteilung.

Fazit: Aufmerksamkeit ist Ihr bester Schutz

Phishing wird immer raffinierter. Aber die wirksamste Gegenmaßnahme bleibt die gleiche: Ihr gesundes Misstrauen. Nehmen Sie sich die zwei Sekunden, um innezuhalten, bevor Sie klicken. Diese kurze Pause kann den Unterschied zwischen einem normalen Arbeitstag und einer ernsthaften Datenpanne machen.

Und vergessen Sie nicht: Wenn Sie unsicher sind oder einen Verdacht haben, sprechen Sie mich an. Dafür bin ich da. Gemeinsam sorgen wir dafür, dass die Angreifer bei uns keine Chance haben.

Auftraggeber sollten deshalb einen verbindlichen Prozess etablieren, der sicherstellt, dass am Ende eines Auftrags die Löschung oder Rückgabe der Daten dokumentiert bestätigt wird. Auch die Zuständigkeiten sollten klar definiert sein, damit dieser Schritt nicht „zwischen Einkauf, Fachabteilung und IT“ verloren geht. (AH)

DATEN WEITERGEBEN – ABER RICHTIG!

Die Personalabteilung arbeitet mit einem externen Büro zusammen. Der Steuerberater erhält regelmäßig Unterlagen mit personenbezogenen Daten. Ein Kollege aus einem anderen Unternehmen der Unternehmensgruppe bittet um eine interne Telefonliste. Solche Situationen gehören zum Arbeitsalltag. Kaum ein Unternehmen arbeitet heute isoliert. Daten werden ausgetauscht – mit Dienstleistern, Beratern, Konzernunternehmen, Banken, Lieferanten oder Behörden. Doch wann ist eine Datenweitergabe eigentlich erlaubt? Und was muss dabei beachtet werden?

Datenaustausch ist möglich

Unsere Wirtschaft ist arbeitsteilig organisiert. Unternehmen greifen auf spezialisierte Dienstleister zurück, lagern Aufgaben aus oder arbeiten in Unternehmensverbünden zusammen. Die Datenschutzvorschriften ermöglichen dies auch – unter Einhaltung der festgelegten Regeln.

Grundfrage: Wer verarbeitet die Daten – und warum?

Für die erste Einordnung ist entscheidend:

- Müssen wir aufgrund gesetzlicher Vorschriften Daten weitergeben oder möchten wir Daten an andere übermitteln?
- Verarbeitet der Empfänger die Daten ausschließlich für unser Unternehmen oder nutzt er sie für eigene Zwecke?
- Wer entscheidet über Zwecke und Mittel der Verarbeitung?

Je nach Antwort ergeben sich unterschiedliche rechtliche Konstellationen.

Wichtig: Kein „Konzernprivileg“

Besonders häufig entsteht Unsicherheit innerhalb von Unternehmensgruppen. Nur weil mehrere Unternehmen zu einem Konzern oder Verbund gehören, dürfen personenbezogene Daten nicht automatisch frei ausgetauscht werden. Selbstständige Unternehmen gelten grundsätzlich als eigenständige Verantwortliche – und damit als „Dritte“. Das bedeutet: Auch zwischen Konzernunternehmen muss geprüft werden, ob eine Rechtsgrundlage für die Datenübermittlung besteht.

Beispiel: Eine unternehmensübergreifende interne Telefonliste mit dienstlichen Kontaktdaten könnte unter Umständen auf ein berechtigtes Interesse gestützt werden – etwa zur Verbesserung der Zusammenarbeit. Aber auch hier muss das berechtigte Interesse geprüft werden, also etwa ob

- die Weitergabe erforderlich ist,
- nur die notwendigen Daten übermittelt werden und
- überwiegende Interessen der betroffenen Personen dem entgegenstehen.

Übernimmt eine Gesellschaft aus dem Unternehmensverbund für die anderen Leistungen wie eine eigene Abteilung oder ein externer Dienstleister, also etwa die Buchhaltung, Personalabrechnung oder IT, ist so gut wie immer eine Vereinbarung zur Auftragsverarbeitung zwischen den Unternehmen erforderlich.

1. Datenübermittlung: gesetzliche Verpflichtungen

Nicht jede Datenweitergabe erfolgt freiwillig oder im Rahmen einer Zusammenarbeit mit Dienstleistern. In vielen Fällen ist ein Unternehmen sogar gesetzlich verpflichtet, bestimmte personenbezogene Daten weiterzugeben.

Beispiele:

- Die Personalabteilung muss Entgelt- und Beschäftigtendaten an Sozialversicherungsträger übermitteln.
- Steuerliche Angaben werden an Finanzbehörden gemeldet.
- Behörden können im Rahmen gesetzlicher Befugnisse Auskünfte verlangen.

In solchen Fällen bildet die gesetzliche Verpflichtung die Rechtsgrundlage für die Datenübermittlung. Das Unternehmen hat hier regelmäßig keinen Entscheidungsspielraum – wohl aber die Pflicht, nur die gesetzlich erforderlichen Daten zu übermitteln.

2. Datenübermittlung: die Auftragsverarbeitung – der „Klassiker“

Regelmäßig verarbeiten andere Unternehmen die Daten nicht zu eigenen Zwecken, sondern für den Auftraggeber. In diesen Fällen liegt häufig eine Auftragsverarbeitung vor.

Typische Beispiele:

- IT-Hosting oder Cloud-Speicher

>

- Lohnabrechnung durch externes Lohnbüro
- Akten- oder Datenträgervernichtung
- Newsletter-Anbieter und Werbebrief-Dienstleister

Wichtige Erkennungsmerkmale für eine Auftragsverarbeitung

Der Auftragsverarbeiter ist eng an den Auftraggeber gebunden und muss dessen Weisung befolgen. Unter anderem muss der Dienstleister auf Weisung des Auftraggebers die Daten löschen oder er stellt etwa in Software-Lösungen entsprechende Funktionen bereit. Ein IT-Dienstleister darf z. B. nicht die Kundendaten seiner Kunden dafür nutzen, um seine Leistungen bei diesen zu bewerben.

Wichtig: Es gibt Ausnahmen bei der Auftragsverarbeitung!

Auf den ersten flüchtigen Blick erfüllt ein externes Buchhaltungsbüro die gleichen Aufgaben wie ein Steuerberater mit seiner Kanzlei. Aber auf den zweiten Blick gibt es einen wesentlichen Unterschied: Der Steuerberater unterliegt eigenen gesetzlichen Pflichten und entscheidet gemäß diesen Regelungen eigenverantwortlich über Art und Weise der Verarbeitung. Deshalb kann er in diesem Sinne nicht „auf Weisung" im Hinblick auf den Datenschutz tätig werden und gilt als eigenverantwortlicher Dritter. Dadurch ergibt sich, dass ein externes Buchhaltungsbüro regelmäßig eine Vereinbarung zur Auftragsverarbeitung benötigt, ein Steuerberater in der Regel nicht.

3. Datenübermittlung: gesetzlich eigenständig Verantwortliche

Neben den Steuerberatern gibt es viele weitere Organisationen, die als eigenständig Verantwortliche gelten, etwa:

- Rechtsanwalt
- Wirtschaftsprüfer
- Banken und Zahlungsdienstleister
- Post- und Paketdienstleister
- Telekommunikationsanbieter

Die oben genannten Anbieter haben häufig bekannte gesetzliche Pflichten, die als „Schweigepflicht", „Postgeheimnis" oder „Fernmeldegeheimnis" bekannt sind. Oft werden hier sensible personenbezogene Daten verarbeitet.

Aber auch andere Berufsgruppen bzw. Branchen können eigenverantwortlich tätig sein. Dies kann sich ebenfalls aus gesetzlichen Regelungen ergeben, wie bei Handelsvertretern. Gemäß den Regelungen des Handelsgesetzbuchs sind selbstständige Handelsvertreter damit betraut, für ein anderes Unternehmen Geschäfte zu vermitteln oder in dessen Namen abzuschließen. Entsprechend erheben diese Daten von Kunden und leiten diese an ihren Auftraggeber weiter.

4. Datenübermittlung: andere eigenständig Verantwortliche

Zudem gibt es zahlreiche Fälle, in denen eine Datenübermittlung erforderlich ist, der Empfänger eigenverantwortlich tätig ist und es keine speziellen Verschwiegenheitsgesetze oder Regelungen gibt, dass dieser eigenverantwortlich tätig wird. Beispiele:

- Ein Unternehmen beauftragt etwa eine Spedition zur Auslieferung von Ware an einen Kunden,
- ein Hausbesitzer gibt die Kontaktdaten eines Mieters an einen Handwerker.

Hinweise auf diese Art von Datenübermittlung sind, wenn

- der Empfänger in der Liefer-/Dienstleistungskette eingebunden ist,
- er keinen besonderen gesetzlichen Schweigepflichten unterliegt,
- die Verarbeitung nicht im Kern die Verarbeitung personenbezogener Daten vorsieht und
- er regelmäßig nur die absolut notwendigen Daten für seine Zwecktätigkeit erhält.

Die Datenübermittlung an eigenständig Verantwortliche (Möglichkeit 3 und 4) erfolgt häufig auf Basis eines berechtigten Interesses. Voraussetzungen sind jedoch eine sorgfältige Interessenabwägung, die Beschränkung auf die erforderlichen Daten sowie die transparente Information der betroffenen Personen.

Kleine Änderung – große Wirkung!

Ein Reisebüro, das für Beschäftigte von Unternehmen lediglich Reisen bucht, ist oftmals eigenständig verantwortlich. Bietet es zusätzlich ein Onlineportal mit Mitarbeiterverwaltung, Budgetsteuerung und Freigabeprozessen an, kann die Bewertung ganz oder teilweise anders ausfallen.

5. Datenübermittlung: gemeinsame Verantwortlichkeit

In manchen Konstellationen entscheiden zwei oder mehr Unternehmen gemeinsam über Zwecke und Mittel der Verarbeitung. Dies ist etwa der Fall, wenn mehrere Unternehmen ein gemeinsames Presse- oder

Bewerberportal betreiben. Das können z. B. Unternehmen aus einem Unternehmensverbund sein, aber auch zwei oder mehr eigenständige Unternehmen.

In solchen Fällen spricht man von gemeinsamer Verantwortlichkeit und es müssen die Regelungen des Art. 26 EU-Datenschutz-Grundverordnung eingehalten werden. Im Wesentlichen geht es hier um die Erfüllung der Betroffenenrechte.

Der Unterschied zur Auftragsverarbeitung ist, dass alle Verantwortlichen gemeinsam über die Mittel, z. B. ein Webportal und die dahinterliegende Software, entschieden haben.

Zudem nutzen die Unternehmen zu jeweils eigenen Zwecken die Daten und kontaktieren etwa in ihrem Interesse die dort registrierten Journalisten. Eine Auftragsverarbeitung würde hinzukommen, wenn die gemeinsamen Verantwortlichen das Webportal von einem Dienstleister betreiben lassen.

Fazit: Datenaustausch ist erlaubt – wenn die Regeln beachtet werden

Die Weitergabe personenbezogener Daten ist im Geschäftsalltag häufig notwendig und zulässig. Wichtig ist, die Verarbeitung bzw. Verarbeitungen im Detail möglichst frühzeitig zu prüfen und die jeweilige Rechtsgrundlage zu klären. Denn alle beteiligten Verantwortlichen benötigen eine Rechtsgrundlage und müssen die Datenschutzvorgaben einhalten. Ihre Datenschutzbeauftragte oder Ihr Datenschutzbeauftragter ist Ihnen sicherlich gerne dabei behilflich. Kontaktieren Sie Ihre Datenschutzexperten bitte so früh wie möglich. Denn je nach Einordnung ergeben sich weitere notwendige Maßnahmen. Dies kann der Abschluss einer Vereinbarung zur Auftragsverarbeitung oder gemeinsamen Verantwortlichkeit sein und auch die Umsetzung der notwendigen Maßnahmen, welche sich aus der Vereinbarung oder gesetzlichen Vorgaben ergibt. (ST)

WUSSTEN SIE SCHON? URTEIL DES BGH: AM ENDE DER AUFTRAGSVERARBEITUNG IST KONTROLLE NOTWENDIG!

Der Bundesgerichtshof (BGH) hat am 11.11.2025 (Az. VI ZR 396/24) eine für Unternehmen wichtige Entscheidung getroffen: Die Verantwortung für personenbezogene Daten endet nicht automatisch mit dem Vertragsende einer Auftragsverarbeitung.

Im entschiedenen Fall hatte ein Unternehmen einen Dienstleister mit der Verarbeitung personenbezogener Daten beauftragt. Nach Beendigung der Zusammenarbeit wurde offenbar nicht ausreichend überprüft, ob die Daten beim ehemaligen Auftragsverarbeiter gelöscht wurden. Später wurde der Dienstleister Opfer eines Cyberangriffs – und es waren auch personenbezogene Daten des Verantwortlichen beteiligt. Betroffene machten daraufhin Schadensersatz geltend.

Der BGH stellte klar: Der Verantwortliche muss sicherstellen, dass personenbezogene Daten nach Vertragsende gelöscht oder zurückgegeben werden. Eine bloße vertragliche Regelung genügt nicht. Es bedarf zumindest einer nachvollziehbaren Kontrolle oder einer dokumentierten Löschbestätigung.

Hintergrund ist Art. 28 Abs. 3 Satz 2 Buchst. g Datenschutz-Grundverordnung. Danach ist der Auftragsverarbeiter verpflichtet, personenbezogene Daten nach Abschluss der Verarbeitung zu löschen oder zurückzugeben. Der Verantwortliche muss jedoch im Rahmen seiner Rechenschaftspflicht überprüfen, ob dies tatsächlich erfolgt ist.

Auftraggeber sollten deshalb einen verbindlichen Prozess etablieren, der sicherstellt, dass am Ende eines Auftrags die Löschung oder Rückgabe der Daten dokumentiert bestätigt wird. Auch die Zuständigkeiten sollten klar definiert sein, damit dieser Schritt nicht „zwischen Einkauf, Fachabteilung und IT“ verloren geht.

Denn auch nach Beendigung der Zusammenarbeit bleibt das Unternehmen nach diesem Urteil in der Verantwortung – und kann im Schadensfall haften.

Gerade bei IT-Dienstleistern, Cloud-Anbietern oder externen Lohnabrechnungsstellen kann sich die Beendigung eines Vertrags sonst noch Jahre später auswirken. Denn auch nach Beendigung der Zusammenarbeit bleibt das Unternehmen nach diesem Urteil in der Verantwortung – und kann im Schadensfall haften. (ST)

VIDEO: DATENÜBERMITTLUNG

Wenn über Datenschutzverletzungen berichtet wird, denken viele zuerst an Cyberangriffe. Tatsächlich entstehen jedoch zahlreiche meldepflichtige Vorfälle durch einfache Übermittlungsfehler oder beim Transport von Datenträgern. In diesem Video erfahren Sie, warum Datenübermittlungen besonders fehleranfällig sind und welche typischen Risiken bei E-Mail, Fax, Post oder Online-Freigaben bestehen, und wie Sie sie mit einfachen Maßnahmen deutlich reduzieren.

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: Feodora – 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