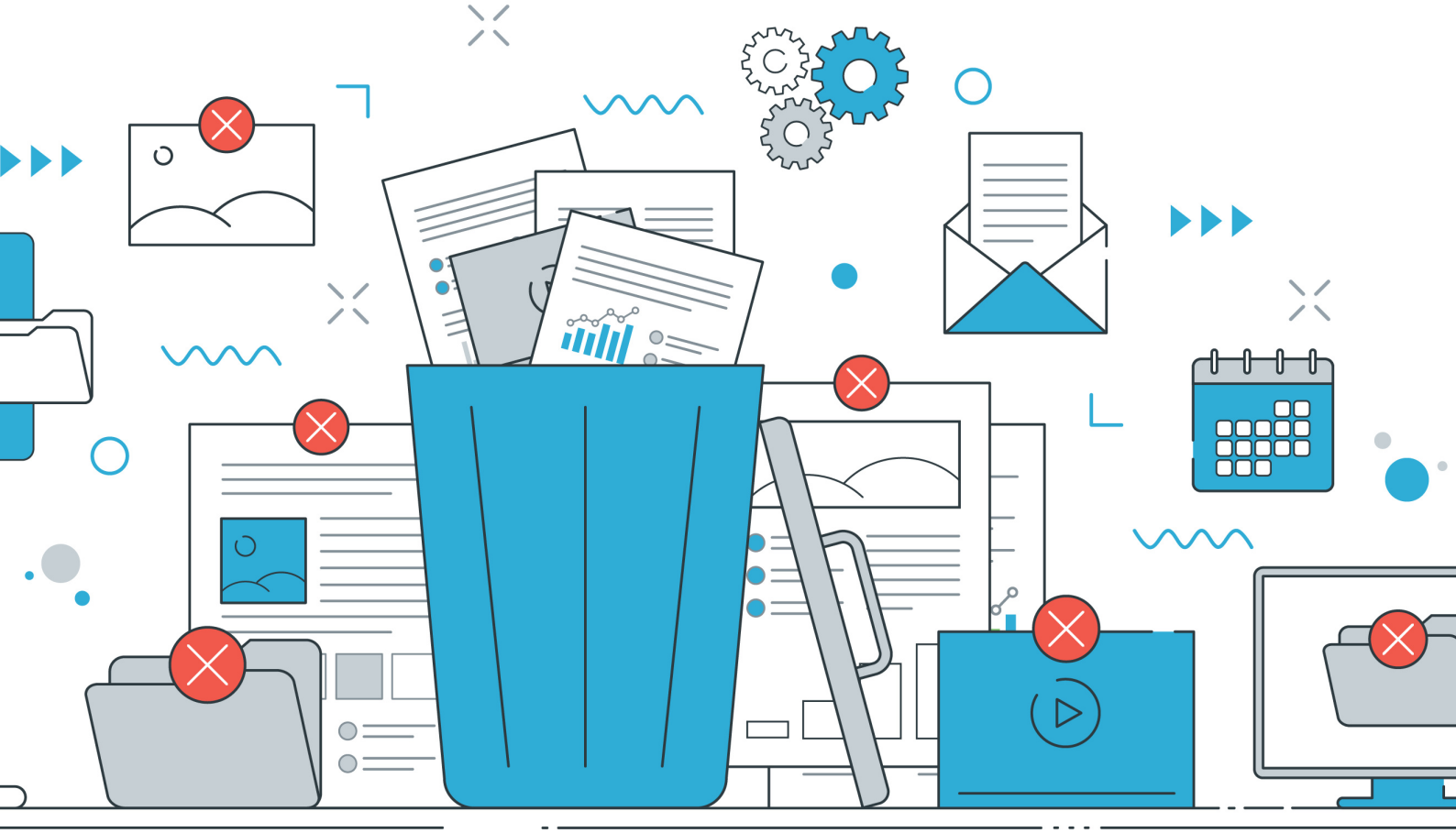
3/25

PRIVACY@WORK

DATENSCHUTZ FÜR MITARBEITER



LÖSCHEN LEICHT GEMACHT

Ihr Beitrag zum Datenschutz!

BETROFFENENRECHTE

So meistern Sie Anfragen im Jahr 2025

powered by
PRIVACYXPERTS

Liebe Leserin, lieber Leser,

Ausmisten tut gut – das fühlt sich so an, wie Ballast abzuwerfen. Gerade jetzt im Frühling gehört das zum Frühlingsputz dazu. Aber Vorsicht: Beim Datenschutz und insbesondere bei personenbezogenen Daten dürfen Sie nicht so einfach kurzen Prozess machen, um zu entsorgen, um Ordnung ins Datenchaos zu bringen und Schaden von unserem Unternehmen abzuwenden.Denn hier müssen Sie Regeln einhalten, die Sie ab Seite 3 in dieser Ausgabe finden.

Ebenso gibt es Regeln für den Umgang mit Anfragen von Betroffenen, wenn es um ihre Daten geht. Oft melden sich betroffene Personen dann auch noch, wenn es ohnehin bereits Unstimmigkeiten zwischen ihnen und Ihrem Unternehmen gibt. Deshalb ist es umso wichtiger, hier keinen Fehler zu machen, um rechtliche Probleme zu vermeiden. Wie Sie dabei korrekt vorgehen, erfahren Sie ab Seite 5 dieser Ausgabe.

Sie sehen: Auch in dieser Ausgabe finden Sie viele Tipps, damit keiner Ihrer Mitarbeiter in einen „Daten-Fettnapf" tritt.

Wir wünschen Ihnen einen guten Start in den 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.

LÖSCHEN LEICHT GEMACHT: IHR BEITRAG ZUM DATENSCHUTZ!

„Weg damit!" – so einfach ist es leider nicht, wenn es um das Löschen von personenbezogenen Daten geht. Aber keine Sorge, wir machen es Ihnen leicht! Datenschutz ist Teamarbeit und Sie als Mitarbeiterin oder Mitarbeiter sind der Schlüssel, um Daten sicher und rechtzeitig loszuwerden. Warum das so wichtig ist? Weil jede überflüssige Information nicht nur Platz wegnimmt, sondern auch Risiken mit sich bringt! Heute erfahren Sie, was Sie konkret tun können, um Ordnung ins Datenchaos zu bringen und Schaden von unserem Unternehmen abzuwenden. Packen wir's an!

Was sind Ihre Aufgaben beim Thema Löschen?

Doch wie genau sorgen Sie dafür, dass unser Unternehmen sauber und aufgeräumt bleibt – digital und analog? Keine Angst, Sie müssen kein Datenschutzprofi sein. Mit ein paar einfachen Regeln und einem klaren Blick auf Ihre Aufgaben ist es ein Leichtes, Daten richtig zu löschen. Schauen wir uns an, worauf es ankommt.

1. Wann löschen?

Die Grundregel lautet: Alles, was Sie nicht mehr benötigen, sollte schnell und sicher gelöscht werden – natürlich unter Einhaltung der Aufbewahrungsfristen.

Beispiele aus dem Alltag:

- **Bewerbungen:** nach sechs Monaten löschen, wenn kein Arbeitsvertrag zustande kommt. Speichern Sie keine alten Bewerbungen „zur Sicherheit" ab. Dafür gibt es keine Grundlage und es kann zum Datenschutzproblem werden.
- **Kundenanfragen:** Haben Sie alte E-Mails mit personenbezogenen Daten (z. B. Adressen) in Ihrem Postfach, die nicht mehr relevant sind? Weg damit, sobald der Zweck erledigt ist!
- **Projektunterlagen:** Sind Projekte abgeschlossen und die Daten nicht mehr notwendig? Überprüfen Sie gemeinsam mit Ihrer Führungskraft, ob sie gelöscht werden können.

Mein Tipp:
Räumen Sie regelmäßig auf! Planen Sie z. B. einmal im Monat 15 Minuten ein, um Ihr E-Mail-Postfach, Ihren Desktop und Ordner auf dem Server nach veralteten Dateien zu durchsuchen. Was nicht mehr benötigt wird und keine Frist hat, löschen Sie sofort.

2. Wie löschen?

Einfach in den Papierkorb schieben? Leider nicht! Das ist wie eine halb leere Chipstüte: Sie nimmt Platz weg und irgendwann greift doch jemand rein.

So geht's richtig:

- **Digitale Daten:** Nutzen Sie die bereitgestellten Löschfunktionen in den Systemen. Damit stellen Sie sicher, dass die Daten vollständig entfernt werden und nicht in Back-ups landen.
- **Papierunterlagen:** Verwenden Sie ausschließlich die Aktenvernichter in Ihrer Abteilung, die die Sicherheitsstufe für personenbezogene Daten erfüllen. Keine Altpapiertonne!
- **Externe Geräte:** Arbeiten Sie mit USB-Sticks oder externen Festplatten? Prüfen Sie regelmäßig, ob darauf noch sensible Daten gespeichert sind. Löschen Sie diese vollständig, z. B. durch Formatieren oder spezielle Löschsoftware.

Mein Tipp:
Löschen Sie Daten direkt in den vorgesehenen Systemen. Sollten Sie sich nicht sicher sein, wie das geht, sprechen Sie mit Ihrer IT-Abteilung oder der Abteilungsleitung. Merken Sie sich: Daten, die sicher gelöscht sind, können nicht missbraucht werden.

3. Löschfristen kennen

Wussten Sie, dass jedes Dokument und jede Information ein „Verfallsdatum" haben? Das hängt davon ab, wofür es ursprünglich genutzt wurde.

Typische Löschfristen:

- **Steuerunterlagen:** 8 Jahre (§ 147 Abgabenordnung (AO), § 257 Handelsgesetzbuch (HGB)
- **Personalunterlagen:** 6 Jahre nach Ende des Arbeitsverhältnisses, z. B. Arbeitsverträge oder Gehaltsabrechnungen
- **Rechnungen und Buchungsbelege:** Die Aufbewahrungsfrist wurde von 10 Jahren auf 8 Jahre verkürzt (§ 257 Abs. 4 HGB und § 147 Abs. 3 AO).

>

- **Projekt- und Budgetpläne:** 6 Jahre Aufbewahrung, sofern keine steuerlichen oder rechtlichen Anforderungen bestehen
- **Investitionsdokumentationen:** 8 Jahre Aufbewahrungspflicht gemäß den neuen gesetzlichen Bestimmungen
- **Berichte und Auswertungen:** nach 3 bis 6 Jahren prüfen, ob sie noch benötigt werden
- **Arbeitsverträge und Kündigungsunterlagen:** 6 Jahre nach Beendigung des Arbeitsverhältnisses aufzubewahren
- **Lohn- und Gehaltsabrechnungen:** 8 Jahre Aufbewahrungspflicht gemäß § 147 Abs. 3 AO
- **Urlaubsanträge und Krankmeldungen:** nach 3 Jahren zu löschen, sofern keine rechtlichen oder betrieblichen Gründe für eine längere Aufbewahrung bestehen

Mein Tipp:

Prüfen Sie bei sensiblen Dokumenten immer zuerst: Gibt es eine gesetzliche oder betriebliche Aufbewahrungspflicht? Ihre Abteilungsleitung oder der Datenschutzbeauftragte kann Ihnen bei Unsicherheiten weiterhelfen.

5. Übernehmen Sie Verantwortung

Sie sind die „erste Löschinstanz" für die Daten, mit denen Sie arbeiten. Das bedeutet, dass Sie aktiv prüfen und handeln müssen.

Beispiele:

- **E-Mail-Postfach:** Regelmäßiges Aufräumen ist hier besonders wichtig. Sortieren Sie inaktive E-Mails aus, z. B. Kundenanfragen, die abgeschlossen und keine Geschäftsbriefe sind.
- **Laufwerke und Cloud-Speicher:** Speichern Sie nur, was wirklich gebraucht wird. Datenleichen sind nicht nur unpraktisch, sondern auch riskant.
- **Papierunterlagen:** Lassen Sie keine sensiblen Unterlagen auf Ihrem Schreibtisch herumliegen. Wenn Sie etwas nicht mehr benötigen, vernichten Sie es sofort, dann kann es auch nicht in die falschen Hände kommen. Prüfen Sie natürlich zuvor, ob diese Daten keiner Aufbewahrungspflicht unterliegen.

Checkliste: Sicheres Löschen von Daten

Prüfpunkt	✔
E-Mail-Postfach prüfen: Habe ich alte E-Mails mit personenbezogenen Daten, die nicht mehr benötigt werden, gelöscht?	○
Digitale Dokumente bereinigen: Habe ich veraltete Dateien auf meinem Desktop, in Netzlaufwerken oder Cloud-Speichern überprüft und gelöscht?	○
Sind die Löschfristen bekannt? Prüfe ich regelmäßig, ob Daten wie Bewerbungsunterlagen, Projektunterlagen oder andere personenbezogene Dokumente die vorgegebenen Fristen überschritten haben?	○
Löschpflicht versus Aufbewahrungspflicht: Habe ich sichergestellt, dass ich keine Unterlagen lösche, die noch gesetzlichen Aufbewahrungspflichten unterliegen?	○
Papierunterlagen sicher vernichten: Werden sensible Unterlagen sofort in den Aktenvernichter gegeben und nicht im Papierkorb entsorgt?	○
Digitale Daten korrekt löschen: Nutze ich die vorgesehenen Löschfunktionen der Systeme, um sicherzustellen, dass Daten vollständig entfernt werden?	○
Externe Speichermedien prüfen: Habe ich alte Daten auf USB-Sticks, externen Festplatten oder anderen Geräten sicher gelöscht?	○
Gibt es ungenutzte Datenleichen? Prüfe ich regelmäßig, ob ich veraltete oder ungenutzte Daten noch gespeichert habe?	○
Zusammenarbeit mit der IT: Melde ich unsichere Löschvorgänge oder technische Probleme der IT-Abteilung, damit sie mich unterstützen kann?	○
Fragen geklärt: Wende ich mich bei Unsicherheiten direkt an die Abteilungsleitung oder den Datenschutzbeauftragten?	○
Minimalismus beim Speichern: Speichere ich nur Daten, die wirklich benötigt werden, und vermeide unnötige Duplikate?	○

Mein Tipp:
Wenn Sie sich unsicher sind, ob etwas gelöscht werden kann, fragen Sie! Es ist besser, kurz nachzufragen, als Daten unnötig zu behalten oder fälschlicherweise zu löschen und ein Risiko einzugehen.

Ihr Datenschutz-Tool: die Checkliste fürs sichere Löschen!

Löschen klingt einfach, aber im Arbeitsalltag lauern die Tücken im Detail. Wer denkt schon an Löschfristen, ungenutzte Dateien oder alte Unterlagen auf dem USB-Stick? Genau hier hilft unsere Checkliste! Mit ihr haben Sie alle wichtigen Punkte im Blick und können Daten nicht nur sicher, sondern auch datenschutzkonform löschen.

Mein Tipp:
Machen Sie sich das Leben leichter und helfen Sie dabei, unser Unternehmen und die Privatsphäre unserer Kunden zu schützen. Greifen Sie zur Checkliste und legen Sie los – Daten löschen war noch nie so einfach!

Mein Tipp:
Mit dieser Checkliste in der Hand haben Sie alles im Griff. Ein regelmäßiger Blick darauf hilft Ihnen, Ordnung zu halten und den Datenschutz aktiv zu leben. Denken Sie daran: „Weniger Daten, weniger Risiken!“

Fazit:

Mit jedem sorgfältig gelöschten Datensatz leisten Sie einen aktiven Beitrag zum Schutz unserer Unternehmensdaten und der Privatsphäre unserer Kunden und Kollegen. Wenn Sie Fragen haben, stehen wir Ihnen mit Rat und Tat zur Seite. Gemeinsam machen wir Datenschutz einfach und effizient! Ein sauberer Datenbestand ist wie ein aufgeräumter Schreibtisch – gut fürs Gewissen und die Sicherheit! (AH)

BETROFFENENRECHTE: SO MEISTERN SIE DEN UMGANG MIT ANFRAGEN IM JAHR 2025

Der Umgang mit Anfragen zu Betroffenenrechten kann herausfordernd sein – vor allem wenn solche Anfragen bei Ihnen im Unternehmen nur selten vorkommen. Oft melden sich betroffene Personen dann auch noch, wenn es ohnehin bereits Unstimmigkeiten zwischen ihnen und Ihrem Unternehmen gibt. Deshalb ist es umso wichtiger, hier keinen Fehler zu machen, um rechtliche Probleme zu vermeiden.

Die Betroffenenrechte nach Art. 12 bis 23 DSGVO

Die Betroffenenrechte werden größtenteils im Kapitel 3 in den Artikeln 12 bis 23 der EU-Datenschutz-Grundverordnung (DSGVO) geregelt. Einige Rechte, wie die Informationspflichten nach Art. 13, 14 DSGVO („Datenschutzhinweise“ oder im Alltag auch „Datenschutzerklärung“), müssen von Verantwortlichen, also etwa Ihrem Unternehmen, ohne Aufforderung erfüllt werden. Andere Rechte, wie das Auskunftsersuchen nach Art. 15 DSGVO, müssen auf Anfrage erfüllt werden.

Diese Rechte haben Betroffene:

Art. 15 DSGVO: Recht auf Auskunft

Art. 16 DSGVO: Recht auf Berichtigung

Art. 17 DSGVO: Recht auf Löschung

Art. 18 DSGVO: Recht auf Einschränkung der Verarbeitung

Art. 19 DSGVO: Recht auf Unterrichtung über die Benachrichtigung von Empfängern

Art. 20 DSGVO: Recht auf Datenübertragbarkeit

Art. 21 DSGVO: Recht auf Widerspruch

Art. 7 Abs. 3 DSGVO: Recht auf Widerruf von erteilten Einwilligungen

Art. 77 DSGVO: Recht, sich bei der Aufsichtsbehörde zu beschweren

Aufforderung trifft ein – zeitnahe Reaktion erforderlich!

Leider kommt es in der Praxis immer wieder vor, dass Aufforderungen zur Erfüllung von Betroffenenrechten nicht bearbeitet werden. Gerade in Konfliktfällen führt dies immer wieder dazu, dass sich die betroffenen Personen bei der Aufsichtsbehörde beschweren und diese dann Auskunft zu dem Sachverhalt einfordern. Die Bearbeitung muss nach Art. 12 Abs. 3 DSGVO üblicherwei- >

> se unverzüglich und spätestens innerhalb eines Monats erfolgen. Doch gerade ein Auskunftsersuchen kann – ohne die entsprechende Vorbereitung – einige Zeit in Anspruch nehmen, weshalb die Bearbeitung möglichst schnell beginnen sollte. Wenn Sie oder Ihre Kollegen eine Anfrage zu Betroffenenrechten erhalten, sollten Sie diese schnell und gemäß den internen Vorgaben bearbeiten oder an die zuständigen Stellen weiterleiten. Lesen Sie, welche Schritte Sie oder ggf. Ihre internen Ansprechpartner dann üblicherweise durchführen sollten und welche „Fettnäpfchen" lauern.

Identität muss sichergestellt sein

In manchen Unternehmen erfolgt die Erfüllung der Betroffenenrechte „per Klick", etwa wenn ein Newsletter-Empfänger seine Einwilligung zum Empfang per Klick auf den „Austrage-Link" widerruft. Hier geht man regelmäßig davon aus, dass nur die entsprechende Person Zugriff auf das Postfach, die Nachricht und den entsprechenden Link zum Austragen aus dem Newsletter hat. Bei anderen Betroffenenrechten muss die Identität der Person häufig noch durch weitere Angaben nachgewiesen werden.

Gerade bei einer Auskunft nach Art. 15 DSGVO erhält der Empfänger unter Umständen auch sehr sensible Daten. Da wäre es fatal, wenn ein Unternehmen diese Daten an eine Person sendet, die eine entsprechende Auskunft in einem anderen Namen angefordert hat. In größeren Unternehmen gibt es deshalb interne Vorgaben, wie die Identität einer Person je nach gefordertem Recht geprüft werden muss. In kleineren Unternehmen oder Unternehmen, in denen eher selten entsprechende Anfragen eintreffen, wird jede Anfrage entsprechend individuell geprüft.

Klärung bei unklaren Forderungen

Immer wieder kommt es vor, dass Personen nicht eindeutig formulieren, welches Betroffenenrecht umgesetzt werden soll, oder sich diese teilweise widersprechen. So wird etwa das „Löschen" gefordert, aber aus dem Text ergibt sich, dass nicht das komplette Kundenkonto gelöscht werden soll, sondern nur die Entfernung aus dem E-Mail- oder Werbeverteiler. Solche Unklarheiten müssen im Bedarfsfall geklärt werden, um spätere Streitigkeiten zu vermeiden.

Darf die Forderung erfüllt werden?

Ist geklärt, was die betroffene Person möchte, gilt es zu prüfen, ob man dieser Forderung überhaupt nachkommen darf oder in welchem Umfang. Fordert eine betroffene Person etwa die „Löschung aller Daten", steht dem häufig eine gesetzliche Aufbewahrungsfrist entgegen. So müssen insbesondere Rechnungen üblicherweise für mehrere Jahre aufbewahrt werden.

Je nach Situation in den Unternehmen werden die Daten der Person dann nur aus bestimmten Anwendungsprogrammen gelöscht oder etwa bei „Komplett-Lösungen" aus Warenwirtschaft und Buchhaltung die nicht benötigten Datenfelder entfernt und der Kundendatensatz gesperrt oder auf inaktiv gesetzt.

Bitte beachten Sie: Einwilligungen von Endverbrauchern für Telefonwerbung müssen gemäß § 7a Gesetz gegen den unlauteren Wettbewerb (UWG) für 5 Jahre nach der letzten Verwendung aufbewahrt werden.

Die Erfüllung der Betroffenenrechte wird zur Einhaltung der Rechenschaftspflicht üblicherweise für 3 Jahre dokumentiert. Mögliche Aufbewahrungsfristen sollten unbedingt beachtet werden!

Systembedingte Probleme bei der Umsetzung

Eine wesentliche Ursache für Probleme bei der Erfüllung der Betroffenenrechte ist häufig, dass personenbezogene Daten in einer Vielzahl von Anwendungen verarbeitet und diese nicht alle berücksichtigt werden.

Dies kann dazu führen, dass

- Auskünfte nicht vollständig sind,
- trotz Bestätigung der Löschung noch Daten vorhanden sind und
- im schlimmsten Fall diese Personen bei einem Konfliktfall dann auch noch werblich kontaktiert werden, weil genau diese Anwendungen übersehen wurden.

Eine weitere Konsequenz kann sein, dass Beschäftigte die Daten der betroffenen Person ändern oder löschen und diese Daten nach einer Synchronisation am Folgetag wieder vorhanden sind.

Teilweise werden auch individuell gepflegte Adressbücher oder entsprechende (Excel-)Listen übersehen. Nutzt eine Kollegin oder Kollege diese zur Kontaktaufnahme, werden auch hier möglicherweise Personen kontaktiert, denen vorher durch das Unternehmen bestätigt wurde, dass ihre Daten gelöscht sind. Hinzu kommt natürlich, dass auch weitere gesetzliche Datenschutzvorschriften nicht eingehalten wurden. >

Rückmeldung nicht vergessen!

Immer wieder kommt es vor, dass von der anfragenden Person keine Daten vorliegen. Manchmal wurden die Daten schon gelöscht, da der Zweck entfallen war, manchmal wurde zwischenzeitlich der Name geändert, etwa nach einer Eheschließung, oder die Nachricht kommt von einer E-Mail-Adresse bzw. von Kontaktdaten, die nicht verifiziert werden können. Auch wenn keine Daten der Person vorhanden sind, muss zeitnah eine entsprechende Rückmeldung erfolgen.

Sind Daten vorhanden und wurde das eingeforderte Betroffenenrecht erfüllt, sollte dies entsprechend zurückgemeldet werden. Die betroffene Person erfährt ansonsten beispielsweise nicht, dass die gewünschten Daten geändert oder gelöscht wurden.

Bei der Rückmeldung sollte darauf geachtet werden, dass alle notwendigen Angaben enthalten sind. Zudem sollte die Rückmeldung – je nach Umfang der Daten und dem Risiko – entsprechend sicher erfolgen. Gerade im werblichen Bereich weisen Unternehmen auch auf mögliche Überschneidungen hin, also etwa dass die Person in den nächsten Tagen noch Werbepost erhalten kann, wenn diese sich bereits in Produktion oder Auslieferung befindet.

Bitte immer dokumentieren

Manchmal können die Betroffenenrechte auch einfach und schnell umgesetzt werden, etwa wenn ein Kunde nicht mehr werblich telefonisch kontaktiert werden möchte, sondern ihm eine E-Mail ausreicht. In manchen Systemen ist das mit wenigen Klicks erledigt. Wichtig ist dennoch, dass das Erfüllen der Betroffenenrechte dokumentiert wird, sofern dies nicht automatisch durch das System erfolgt. Ich durfte bereits mehrere Vorfälle begleiten, in denen etwa ein Familienmitglied sich regelmäßig in einen werblichen Verteiler hat eintragen lassen und ein anderes Familienmitglied sich laufend über die Zusendung trotz Bestätigung der Löschung beschwert hat.

Die Dokumentation ist auch zur Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO erforderlich. Diese Dokumentation der Bearbeitung eines Betroffenenrechts wird regelmäßig 3 Jahre als Nachweis aufbewahrt.

Ihre Mitwirkung kann ausschlaggebend sein!

Sofern Sie eine entsprechende Aufforderung zur Erfüllung eines Betroffenenrechts erhalten, sollten Sie zeitnah reagieren. Wie die Bearbeitung erfolgen muss und wer für die Bearbeitung zuständig ist, variiert von Unternehmen zu Unternehmen. Im besten Fall erkundigen Sie sich bereits im Vorfeld, wie die Regelungen in Ihrem Unternehmen sind. Wichtig ist jedoch, dass entsprechende Aufforderungen unverzüglich bearbeitet werden und innerhalb der gesetzlichen Frist eine Rückmeldung erfolgt. (ST)

WUSSTEN SIE SCHON? DER ANGRIFF VIA MICROSOFT TEAMS!

Nach Untersuchungen des Sicherheitsunternehmens Sophos haben Kriminelle eine neue Masche gefunden, mit der sie in Unternehmensnetzwerke eindringen, um Schadsoftware zu installieren.

Schritt 1: Tausende E-Mails

Die Angreifer fluten zuerst die E-Mail-Postfächer von ausgewählten Mitarbeitern mit Tausenden E-Mails. Nach dem Bericht von Sophos wurden bis zu 3.000 E-Mails innerhalb von 45 Minuten gesendet.

Schritt 2: Hilfsangebot

Während dann weitere E-Mails in dem Postfach eintreffen, meldet sich einer der Kriminellen dann per Microsoft Teams bei diesen Mitarbeitern. Die Täter geben sich als Mitarbeiter des IT-Supports aus und bieten – vermeintlich – Hilfe an.

Schritt 3: Angriff

Die Angreifer verlangen eine Bildschirmfreigabe und installieren dann Schadsoftware. Damit haben die Angreifer dann etwa Zugriff auf das Gerät und Unternehmensnetzwerk.

Nicht in Panik versetzen lassen

Sofern Ihr Postfach mit Tausenden E-Mails geflutet wird, sollten Sie sich aktiv an die Ihnen bekannten Ansprechpartner wenden und die bekannten Kontaktmöglichkeiten nutzen. (ST)

MEHR DATENSICHERHEIT

5 kleine Gewohnheiten mit großer Wirkung für mehr Datensicherheit und Datenschutz: nicht immer sind es technisch raffinierte Hackingangriffe, welche für Stress und Kosten bei Unternehmen sorgen. Manchmal reicht hierfür eine Unachtsamkeit einer einzelnen Person, aber mit 5 kleinen Angewohnheiten können Sie das Risiko im Arbeitsalltag erheblich reduzieren.

Um diese kleinen Gewohnheiten auch in Ihren Arbeitsalltag zu integrieren, scannen Sie 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

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: Cifoart – 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