DATENSCHUTZAKTUELL
FEB I 2026
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

OFFBOARDING FÜR BETRIEBSRÄTE IM MÄRZ: DAS IST IHRE CHECKLISTE

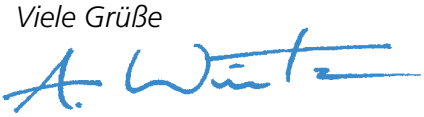
Manchmal ist Geduld gefragt

Liebe Leserin, lieber Leser,

vielleicht kennen Sie das: Sie haben sich etwas vorgenommen, etwa um den Datenschutz im Unternehmen vorwärtszubringen. Doch Ihren guten Ansatz will niemand sehen, geschweige denn unterstützen. Hier können Sie natürlich frustriert sein, entnervt aufgeben und die Flinte ins Korn werfen.

Besser ist es jedoch, wenn Sie die Sache eher als einen kurzen Halt auf dem Weg zu Ihrem Ziel sehen. Greifen Sie das Thema mit etwas zeitlichem Abstand erneut auf, unter Umständen leicht abgewandelt. Und vielleicht sieht man dann die Dinge etwas anders. Geduld und Beharrlichkeit können sich auszahlen. Probieren Sie es einfach aus.

Viele Grüße



Andreas Würtz,
Rechtsanwalt und Chefredakteur

Ihr Experte für Datenschutz
Andreas Würtz verfügt über mehr als 20 Jahre Berufserfahrung als Vollzeit-Datenschützer im Unternehmen. Er zeigt Ihnen, wie sich Datenschutz pragmatisch umsetzen lässt.

Inhalt

Zum neuen Onlinebereich!
www.privacyxperts.de/login

Expertensprechstunde:
https://t1p.de/andreas-wuertz

Impressum

PRIVACYXPERTS

ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Bonn

V.i.S.d.P.: Michael Jodda (Adresse s. oben)

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | Ada; Seite 1: Adobe Stock | Fotosphaere

Erscheinungsweise: 26-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Alle Angaben 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.

Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer alle Geschlechterformen gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

Zwei Bereiche stehen im Fokus: Änderungen in der DSGVO und auf EU-Ebene.

Änderungen im Datenschutz: Das sollten Sie wissen

Schon Ende 2025 war klar: Es ist sehr wahrscheinlich, dass es in den nächsten Jahren Änderungen beim Datenschutz geben wird, und zwar sowohl in der Datenschutz-Grundverordnung (DSGVO) als auch beim Bundesdatenschutzgesetz (BDSG). So steht es um die Vorhaben:

Aktuell gibt es zwei Fokusbereiche: Einerseits will die EU ihre Regelwerke vereinfachen, etwa die DSGVO. Andererseits haben in Deutschland Bund und Länder vor, die Unternehmen zu entlasten und Bürokratie abzubauen – auch beim Datenschutz.

Das ist auf EU-Ebene angedacht

Die EU-Kommission hat am 19.11.2025 das Ziel ausgerufen, ein „Digitalpaket" auf den Weg zu bringen, um EU-Regelwerke zu vereinfachen und Innovationen zu fördern. Kernelement ist ein Omnibus-Gesetz in Form einer „Digital-Omnibus-Verordnung". Mit einem „Omnibus-Gesetz" werden in einem Rutsch gleich mehrere Regelwerke oder Teile von diesen angepasst oder aufgehoben.

Konkret ist angedacht, dass es auf EU-Ebene bei diesen Regelwerken Veränderungen gibt: Für Ihr Unternehmen und Sie auf jeden Fall relevant ist die Verordnung (EU) 2016/679: Das ist die DSGVO. Auch die Verordnung (EU) 2023/2854: Das ist der Data Act bzw. ins Deutsche übersetzt die Datenverordnung. Auch will man die Verordnung (EU) 2024/1689 (AI Act oder KI-Verordnung) anpassen. Daneben soll es Anpassungen in den Verordnungen (EU) 2018/1724 und (EU) 2018/1725 sowie in den Richtlinien (EU) 2002/58/EC, (EU) 2022/2555 und (EU) 2022/2557 geben. Aufgehoben werden sollen die Verordnungen (EU) 2018/1807, (EU) 2019/1150, (EU) 2022/868 sowie die Richtlinie (EU) 2019/1024.

Das soll sich in der DSGVO inhaltlich ändern

Mit der Omnibus-Verordnung oder kurz dem „Digitalen Omnibus" soll es in der DSGVO einige Anpassungen geben, insbesondere:

- **Schärfung des Begriffs der personenbezogenen Daten**
  Art. 4 Nr.1 DSGVO soll um einen Satz ergänzt werden. Dieser soll klarstellen, dass Daten nicht personenbezogen sind, wenn der Verantwortliche nicht über die erforderlichen Mittel zur Identifikation verfügt.
- **Anpassung des Grundsatzes der Zweckbindung (Art. 5 Abs. 1 Buchst. b DSGVO)**
  Die Anpassung führt dazu, dass etwa eine Weiterverarbeitung zu statistischen Zwecken als vereinbar anzusehen ist, und zwar unabhängig von den Vorgaben des Art. 6 Abs. 4 DSGVO (Zweckänderung).
- **Überarbeitung der Regeln zu sensiblen Daten (Art. 9 DSGVO)**
  Hier werden Rahmenbedingungen integriert, um besondere Kategorien personenbezogener Daten auch für die Entwicklung und den Betrieb von KI-Systemen nutzen zu können.
- **Anpassung bei den Betroffenenrechten**
  Art. 12 Abs. 5 DSGVO wird durch eine neue Formulierung ersetzt. Kernelement hier: Werden die Rechte für andere Zwecke als den Schutz der Daten geltend gemacht, kann ein Verantwortlicher Kostenersatz verlangen oder die Erfüllung des Rechts verweigern. Auch bei den Informationspflichten soll es Anpassungen geben. So soll Art. 13 Abs. 4 DSGVO ersetzt werden. Unter bestimmten Umständen, etwa bei nicht datenintensiven Verarbeitungen bzw. Kenntnis des Betroffenen von der Identität des Verantwortlichen und des verfolgten Zwecks, kann eine weitere Information entfallen.
- **Veränderungen bei der Meldung von Datenpannen (Art. 33 DSGVO)**
  Meldepflichtig sollen grundsätzlich nur Pannen sein, die wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen. Ferner: Die bisherige Meldefrist von 72 Stunden soll auf 96 Stunden erhöht werden.

Hier finden Sie den Entwurf

Sie wollen sich die Sache genauer ansehen? Kein Problem. Den Entwurf der EU-Kommission zur „Digital-Omnibus-Verordnung" können Sie über folgenden Link abrufen: https://t1p.de/rzylb.

Es ist noch ein langer Weg!

Auch wenn schon viel über den „Digitalen Omnibus" und die Anpassungen an der DSGVO diskutiert wird. Bedenken Sie stets, dass das ganze Vorhaben noch ziemlich am Anfang steht. Aktuell gibt es nur einen Entwurf der EU-Kommission. Auch das EU-Parlament und die Mitgliedsstaaten werden noch mitreden und ihre Vorschläge einbringen. Es ist also hoch wahrscheinlich, dass es noch einige Änderungen gibt. Wann die Verhandlungen (sog. Trilog) zwischen diesen drei Institutionen beginnen, wann sie abgeschlossen sein werden und wann die Änderungen kommen, etwa 2027, kann aktuell niemand genau sagen. Denn: Die Erfahrung mit der ePrivacy-Verordnung zeigt nicht nur, dass sich das Verfahren ziehen kann. Eventuell wird ein Vorhaben auch wieder beerdigt und kommt nie.

Das soll in Deutschland geändert werden

Geht es nach dem Bundeskanzler und den Regierungschefs der Länder, soll auch in Deutschland viel entbürokratisiert, modernisiert und verschlankt werden. Wie aus einem Beschluss zu einer Besprechung zwischen Kanzler und Regierungschefs vom 4.12.2025 hervorgeht, gilt das auch für den Datenschutz und einige Regelungen im BDSG. Folgende Veränderungen sind insbesondere angedacht:

- **Pflicht zur Benennung von Datenschutzbeauftragten wird angepasst**
  Bis Ende 2026 soll die Regelung in § 38 Abs. 1 BDSG entfallen. Die deutschen Vorgaben zur Pflicht zur Benennung eines Datenschutzbeauftragten werden gestrichen. Ein Datenschutzbeauftragter wäre dann nur noch erforderlich, wenn die Voraussetzungen des Art. 37 Abs. 1 DSGVO erfüllt sind. So zum Beispiel, wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung von Daten nach Art. 9 Abs. 1 DSGVO (z. B. Gesundheitsdaten) besteht. Liegt kein Fall von Art. 37 Abs. 1 DSGVO vor, ist kein Datenschutzbeauftragter mehr erforderlich.
- **Die Datenschutzaufsicht soll reformiert werden**
  Die Aufsicht für den nicht öffentlichen Bereich, etwa Unternehmen, soll bis Ende 2027 neu geordnet werden. In Betracht gezogen wird hier die Bündelung von Kompetenzen beim Bund oder bei Aufsichtsbehörden in den Ländern. Zudem soll geprüft werden, inwieweit es noch Landesdatenschutzbeauftragter bedarf.

Hier finden Sie den Beschluss

Den besagten Beschluss können Sie über folgenden Link abrufen: https://t1p.de/nfxhj. Die beabsichtigten Anpassungen im Datenschutz finden Sie ab Listenpunkt 158 auf Seite 30 des Dokuments.

Viel Kritik von Datenschützern

Gerade aus Datenschutzverbänden und aus Richtung der Datenschutzaufsichtsbehörden gibt es starke Kritik an den beabsichtigten Änderungen. So hätte sich in Deutschland die Rolle des Datenschutzbeauftragten etwa in Unternehmen bewährt. Entbürokratisierung gebe es keine. Die Anforderungen aus der DSGVO bzw. aus dem BDSG müssten Verantwortliche trotzdem im vollen Umfang einhalten. Ohne Datenschutzbeauftragte dürfte das mehr schlecht als recht funktionieren. Im Ergebnis würde dem Datenschutz ein Bärendienst erwiesen.

Und nun? Das machen Sie aus den Vorhaben

Dass es Veränderungen geben wird, ist wahrscheinlich. Wann diese kommen und wie diese konkret aussehen werden, muss sich noch zeigen. In der Zwischenzeit können Sie Folgendes tun:

- **Bewahren Sie Ruhe und beruhigen Sie andere**
  Machen Sie sich und andere nicht verrückt. Aktuell ist nichts spruchreif. Insofern brauchen Sie auch noch nichts in die Wege leiten. Bis etwas spruchreif ist, kann es noch ein ganz schönes Weilchen dauern. Dass vor 2027 etwas in trockenen Tüchern sein wird, ist nicht sehr wahrscheinlich. Werden Sie auf die möglichen Neuerungen angesprochen, können Sie entspannt antworten, dass es noch zu früh ist, um die Dinge konkret einschätzen zu können. Bei wichtigen Ansprechpartnern können Sie anbieten, dass Sie diese bezüglich eventueller Neuigkeiten und Entwicklungen auf dem Laufenden halten.
- **Halten Sie die Augen offen**
  Verfolgen Sie die Nachrichten oder die Statements von Datenschutzverbänden bzw. Aufsichtsbehörden. Garantiert wird es auch im Rahmen des Gesetzgebungsverfahrens noch zahlreiche Diskussionen geben. Vielleicht ändert sich dann auch noch das eine oder andere an dem Vorhaben auf EU-Ebene oder in Deutschland. Auch ‚Datenschutz aktuell' wird Sie über die Entwicklungen auf dem Laufenden halten.
- **Prüfen Sie, inwieweit Ihr Unternehmen betroffen ist**
  Auch wenn es Änderungen gibt, muss das nicht unbedingt größere Auswirkungen auf Ihr Unternehmen haben. Eventuell sind gerade bei genauerem Hinsehen die Veränderungen nur minimal. Ob größerer Anpassungsbedarf besteht, sollten Sie bewerten, wenn es verlässliche Entwürfe zu den Gesetzen gibt. Dabei versteht es sich geradezu von selbst: Das kann sich noch ein Weilchen hinziehen.
- **Zeigen Sie, dass Sie wichtig sind**
  Es liegt auf der Hand: Selbst, wenn kein Datenschutzbeauftragter mehr benannt werden muss, müssen dennoch alle Regelungen zum Datenschutz eingehalten werden. Hier braucht es jemanden mit Know-how und Erfahrung, der die richtigen Hinweise zur Umsetzung geben kann. Beraten Sie also proaktiv. Bringen Sie sich ein und machen Sie Ihren Wert für das Unternehmen deutlich, und zwar bei allen sich bietenden Gelegenheiten. Denn sicher ist: Gerade mit Ihrer Beratung tragen Sie dazu bei, dass Datenschutzcompliance nicht zum Problem wird. Auch wenn es keine Pflicht nach Art. 38 Abs. 1 BDSG mehr für einen Datenschutzbeauftragten geben sollte, sollte man an Ihnen auf freiwilliger Basis festhalten. Auch das ist Teil einer unternehmerischen, wirtschaftlichen und vorausschauenden Risikovorsorge.

Schnell mal ein Audit machen: Diese To-dos gibt es für Sie

Zählen Sie zu den Datenschutzbeauftragten, die wenig Zeit für die Wahrnehmung ihrer Aufgaben haben, ist umso wichtiger: Sie müssen dennoch das Bestmögliche aus der bestehenden Situation machen. Wichtig ist daher nicht nur, dass Sie risikoorientiert beraten. Risikoorientiert sollten Sie auch beim Kontrollieren vorgehen. Dabei ist klar: Audits können auch kurz und knapp ausfallen.

Ihrem gesetzlichen Auftrag können Sie rechtssicher nur gerecht werden, wenn Sie die Dinge professionell angehen. Das gilt eben auch dann, wenn Sie nur mal eben ein kurzes Audit durchführen wollen. Denn selbst dann sollte alles Hand und Fuß haben. Geht es nämlich geordnet und strukturiert zu, haben alle Beteiligten und auch die Geschäftsleitung mehr Vertrauen in Ihr Können und Ihre Professionalität. Daher: Setzen Sie auch bei kleineren Prüfungen auf die folgende Checkliste.

Checkliste: To-dos bei jedem Audit

To-do	Darauf sollten Sie achten	Erledigt?
Vorbereitung		
Inwieweit sind passende Schwerpunkte gesetzt oder Prüfthemen festgelegt?	Legen Sie konkret fest, was Sie unter die Lupe nehmen wollen. Hier sollten Sie sich an der Schutzwürdigkeit der personenbezogenen Daten, der Bedeutung für Ihr Unternehmen und den denkbaren Gefahren bzw. Risiken orientieren.	○ Ja ○ Nein
Ist ein Fragenkatalog erstellt und erfassen die Fragen alle relevanten Aspekte?	Erstellen Sie sich vorab einen strukturierten Fragenkatalog. Ausgangspunkt können gesetzliche oder betriebliche Vorschriften sein. Diese ergeben das Soll, gegen das Sie prüfen können.	○ Ja ○ Nein
Sind die Prüfobjekte und Unterlagen vorab und zum Prüfungszeitpunkt verfügbar?	Achten Sie darauf, dass dies gewährleistet ist. Wollen Sie etwa die Videoüberwachung prüfen und kann niemand das System bedienen, kann die Prüfung schnell vorbei sein. Lassen Sie sich auch relevante Unterlagen bereitstellen. Werfen Sie zudem einen Blick ins Verzeichnis von Verarbeitungstätigkeiten.	○ Ja ○ Nein
Wurden Rollen für die Prüfung festgelegt?	Als Datenschutzbeauftragter nehmen Sie die Rolle des Auditors, sprich des Prüfers und Fragenden, ein. Legen Sie fest, wen Sie prüfen, etwa eine verantwortliche Führungskraft für ihre Abteilung. Zudem können weitere Teilnehmer nötig sein, etwa um ein System zu bedienen oder Auskunft zu geben.	○ Ja ○ Nein
Ist ein Termin vereinbart und sind die relevanten Teilnehmer eingeladen und verfügbar?	Legen Sie einen Termin fest, an dem die relevanten Teilnehmer verfügbar sind. Fallen wichtige Personen aus, etwa wegen Krankheit, sollten Sie aus Effizienzgründen die Prüfung ganz oder zumindest teilweise verschieben.	○ Ja ○ Nein
Ist alles in technischer und organisatorischer Hinsicht vorbereitet?	Bereiten Sie alles Relevante vor. Ggf. sind Berichte oder Zugriffsrechte erforderlich, um überhaupt etwas prüfen zu können.	○ Ja ○ Nein
Durchführung		
Wurden alle vorbereiteten Fragen beantwortet?	Arbeiten Sie alle vorbereiteten Fragen ab. Halten Sie direkt fest, was Ihnen geantwortet wurde. Denken Sie unbedingt auch an die praktischen Prüfungen, etwa Begehungen oder Einsichtnahmen.	○ Ja ○ Nein
Sind die gemachten Beobachtungen objektiv beschrieben und dokumentiert?	Halten Sie Ihre Feststellungen und Beobachtungen direkt fest. Achten Sie auf Sachlichkeit und Objektivität. Ggf. können auch Anlagen oder Fotos wichtige Teile einer Dokumentation sein.	○ Ja ○ Nein
Wurden relevante Nachweise oder Belege eingesehen bzw. in die Dokumentation aufgenommen?	Akzeptieren Sie nur als Nachweis, was Ihnen tatsächlich zur Verfügung steht bzw. was Sie gesehen haben. Fügen Sie relevante Belege der Auditdokumentation bei.	○ Ja ○ Nein
Sind Abweichungen vom Sollzustand konkret beschrieben?	Beschreiben Sie konkret, worin eine erkannte Abweichung besteht. Dazu vergleichen Sie die Istsituation mit dem Sollzustand.	○ Ja ○ Nein
Wurden Ergebnisse mit den Teilnehmern bzw. Geprüften besprochen?	Erklären Sie insbesondere, warum eine Abweichung nicht akzeptabel ist. Zudem sollten Sie die Schwere einer Abweichung erläutern, etwa als gering, erheblich oder kritisch. Davon kann auch der Handlungsdruck abhängen.	○ Ja ○ Nein
Sind Maßnahmen zur Behebung eventueller Defizite vereinbart?	Es sollte idealerweise direkt ein Maßnahmenplan zur Behebung der Defizite vereinbart werden. Achten Sie auf klare Verantwortlichkeiten und feste Termine.	○ Ja ○ Nein
Nachbereitung		
Ist ein Auditbericht erstellt und den Geprüften zur Verfügung gestellt worden?	Stellen Sie den Teilnehmern einen Bericht zur Verfügung. Das fördert die Nachvollziehbarkeit und die Akzeptanz.	○ Ja ○ Nein
Wurde ggf. die Unternehmensleitung informiert?	Gerade wenn es kritische oder systemische Defizite gibt, muss ggf. auch die Unternehmensleitung informiert werden. Im Gespräch können Sie die Defizite und ergriffene Maßnahmen erläutern.	○ Ja ○ Nein
Haben die Umsetzungsverantwortlichen die Erledigung der Maßnahmen bestätigt?	Bei der Umsetzung können Sie vor allem beratend unterstützen. Die Erledigung von Maßnahmen ist jedoch nicht Ihre Sache. Haken Sie nach, wenn die Erledigung nicht rechtzeitig erfolgt ist.	○ Ja ○ Nein
Ergibt sich aus der Prüfung genereller Handlungsbedarf im Datenschutz?	Audits bringen Ihnen wichtige Informationen. Ggf. müssen Anpassungen an Regelungen vorgenommen oder bei Beschäftigten für mehr Awareness gesorgt werden.	○ Ja ○ Nein

Offboarding für Betriebsräte im März: Das ist Ihre Checkliste

Vielleicht ist es auch in Ihrem Unternehmen im März wieder so weit: Es wird ein neuer Betriebsrat gewählt. Ist das passiert, heißt das auch: Die Amtszeit des bisherigen Betriebsrats endet. Für manches Betriebsratsmitglied wird das auch das Ende seines Mandats sein. Und hier gibt es dann einiges unter Datenschutzaspekten zu beachten.

Darum sollten Sie aktiv werden

Geht eine Tätigkeit zu Ende, gibt es auch hier so einiges zu bedenken. Für Mitarbeiter, die das Unternehmen verlassen oder die eine andere Aufgabe im Unternehmen wahrnehmen, gibt es häufig einen Prozess, mit dem der Ausstieg bzw. das Ende der Tätigkeit organisiert wird.

Insofern gibt es häufig auch Checklisten mit wichtigen Punkten rund um die Rückgabe von Unterlagen oder den Entzug von Berechtigungen.

Doch ein solches Offboarding kann auch für den Betriebsrat von großer Wichtigkeit sein. Schließlich arbeitet ein Betriebsrat viel mit Schützenswertem, das auf keinen Fall in falsche Hände geraten darf. Und gerade das zu vermeiden muss Ihr Anliegen sein.

Leisten Sie Hilfe zur Selbsthilfe

Eventuell ist Ihr Verhältnis zum Betriebsrat nicht das Beste. Und dennoch müssen Sie den Datenschutz beim Betriebsrat nicht sich selbst überlassen. Schließlich ist der Betriebsrat Teil des Unternehmens und damit Teil des Verantwortlichen. Damit sind auch Sie als Datenschutzbeauftragter für den Betriebsrat zuständig und nehmen Ihre Aufgaben auch diesem gegenüber wahr.

Zudem muss der Betriebsrat alle Vorgaben aus der Datenschutz-Grundverordnung (DSGVO) einhalten. Denn § 79a Satz 1 Betriebsverfassungsgesetz (BetrVG) stellt fest, dass der Betriebsrat bei der Verarbeitung personenbezogener Daten die Vorschriften über den Datenschutz einzuhalten hat. Das bedeutet dann eben gerade, dass die Grundsätze der Verarbeitung nach Art. 5 Abs. 1 DSGVO gewahrt werden müssen.

So können Sie es angehen

Um den Betriebsrat für das Thema Offboarding beim Ende der Betriebsratstätigkeit zu sensibilisieren, können Sie Folgendes machen:

- **Sprechen Sie das Gremium bzw. den Vorsitzenden an und schauen Sie gemeinsam, wie etwa das Ende einer Betriebsratstätigkeit gemanagt werden kann.**
- **Machen Sie ein Brainstorming, welche Besonderheiten etwa im Hinblick auf die Rückgabe von Arbeitsmitteln oder die Übergabe von Unterlagen zu bedenken sind.**
- **Erarbeiten Sie gemeinsam eine praxisnahe Checkliste, die beim Ende der Tätigkeit als Betriebsrat abgearbeitet werden kann.**

Übrigens: Stellt man sich quer und will man nicht mit Ihnen reden, sollten Sie klarmachen: Datenschutz ist keine Option, es ist eine Verpflichtung. Und die trifft auch den Betriebsrat. Verstößt das Gremium bzw. einzelne Mitglieder gegen die Vorgaben zum Datenschutz, kann auch das richtig viel Ärger nach sich ziehen.

Starten Sie mit dieser Checkliste

Klar ist: Jede Checkliste gewinnt an Wert, wenn sie an die spezifischen Anforderungen im Unternehmen bzw. in der konkreten Situation angepasst ist. Starten Sie mit dieser Vorlage und passen Sie diese so an, dass sie den individuellen Anforderungen in Ihrem Unternehmen entspricht.

Checkliste: Offboarding Betriebsratsmitglied

Prüfpunkt	Hintergrund	Erledigt?
Besteht Klarheit darüber, welche Funktion und Rolle das betreffende Betriebsratsmitglied innehatte?	› Im Gremium kann es verschiedene Arbeitsgruppen, Ausschüsse oder Zuständigkeiten geben. Hier sollte zumindest grob bekannt sein, welche Funktionen das Mitglied übernommen hat. › Schauen Sie auf die Intranetseiten des Betriebsrats. Aus einer Vorstellung bzw. aus der Aufgaben- und Zuständigkeitsbeschreibung lässt sich vieles ableiten.	○ Ja ○ Nein
Sind alle überlassenen Arbeitsmittel zurückgegeben worden?	› Klären Sie, inwieweit es eine Übersicht gibt, in der die ausgehändigten Arbeitsmittel vermerkt sind. Das erleichtert es erheblich, die Rückgabe zu überprüfen. › Typischerweise kommen als Arbeitsmittel Notebook, Smartphone und Datenträger wie USB-Sticks oder externe Festplatten in Betracht.	○ Ja ○ Nein
Ist geklärt, inwieweit noch eine Löschung der Geräte erforderlich ist?	› Sollen etwa datenspeichernde Geräte weiter genutzt werden, sollten diese komplett „sauber" sein. Klären Sie, inwieweit eine sichere Löschung der Daten erfolgt. › Idealerweise wird das Löschen in geeigneter Weise dokumentiert. Das können auch Fotos sein, auf denen ein Löschen oder Zurücksetzen von Geräten erkennbar ist.	○ Ja ○ Nein

Wurden überlassene Unterlagen zurückgegeben bzw. vernichtet?	› Betriebsräte haben unter Umständen viele Unterlagen, die personenbezogene Daten enthalten können. Teilweise können die Daten sehr sensibel sein. Umso wichtiger ist, dass hier nichts bei einem demnächst „Unbefugten" zurückbleibt. › Beim Vernichten von nicht mehr benötigten Unterlagen muss darauf geachtet werden, dass dies datenschutzkonform geschieht. Soll ein Schredder zum Einsatz kommen, müssen die Partikel so klein sein, dass ein Zusammensetzen des Geschredderten nur mit extremem Aufwand möglich ist. › Auch das Homeoffice sollte berücksichtigt werden. Hier muss ebenfalls klar Schiff gemacht werden.	○ Ja ○ Nein
Wurde bezüglich eines dem Betriebsrat zugeordneten E-Mail-Postfachs alles Relevante veranlasst?	› Hier sollte eine Sichtung stattfinden. Privates sollte entfernt, Relevantes zusammengestellt und dem Betriebsrat bzw. einem Nachfolger zur Verfügung gestellt werden. › Idealerweise wird das Postfach mit Ende der Tätigkeit als Betriebsrat geschlossen und zeitnah gelöscht.	○ Ja ○ Nein
Sind relevante Informationen in anderen persönlichen E-Mail-Postfächern, Datei- und Dokumentenablagen gesichtet worden?	› Unter Umständen verfügte das betreffende Betriebsratsmitglied über kein gesondertes Postfach. Endet sein Mandat, sollten sich im persönlichen Postfach keine relevanten E-Mails mehr befinden. › Für die Arbeit des Betriebsrats relevante E-Mails sollten diesem übergeben werden. Nicht mehr Relevantes ist zu löschen.	○ Ja ○ Nein
Wurden nicht mehr erforderliche Unterlagen, Notizen oder Akten übergeben bzw. in Abstimmung datenschutzkonform vernichtet?	› Eventuell gibt es Papierunterlagen und Akten, die zukünftig keine Relevanz mehr haben. Sofern diese vernichtet werden können, muss das datenschutzkonform erfolgen. › Für die Betriebsratsarbeit noch relevante Unterlagen sollten an den Betriebsrat bzw. einen Ansprechpartner übergeben werden.	○ Ja ○ Nein
Wurden relevante Zugriffsrechte entzogen?	› Hatte der Betriebsrat im Zusammenhang mit seinem Mandat Berechtigungen, sollten diese mit Ende der Tätigkeit als Betriebsrat entzogen werden. › Denken Sie nicht nur an Zugriffsrechte auf Dateiablagen. Relevant sind auch Einwahlmöglichkeiten, etwa aus dem Homeoffice.	○ Ja ○ Nein
Wurden Zutrittsrechte entzogen und wurden Schlüssel oder Zutrittskarten zurückgegeben?	› Eventuell verfügte die betreffende Person über Schlüssel zum Betriebsratsbüro. Diese müssen unverzüglich zurückgegeben werden. › Gerade wenn eventuell mehrere Standorte oder Gebäude betreut wurden, müssen auch dort die Zutrittsrechte angepasst werden, etwa bei einer Chipkarte oder einem Mitarbeiterausweis. Zutritt ist dort zumindest aufgrund der nun entfallenen Betriebsratstätigkeit nicht mehr erforderlich.	○ Ja ○ Nein
Sind Informationen zum Betriebsratsmitglied aus dem Intranet entfernt?	› Grundsätzlich sollten Informationen angepasst oder entfernt werden. Das gilt insbesondere für Kontaktdaten, Aufgaben, Zuständigkeiten oder ein Foto. › Sollen bestimmte Informationen weiter veröffentlicht bleiben, sollte eine konkrete Einwilligung hierzu vorliegen. Dabei ist wichtig: Auch hier müssen die besonderen Anforderungen zur Einwilligung im Beschäftigtenverhältnis beachtet werden, sprich neben Art. 7, 4 Nr. 11 DSGVO auch § 26 Abs. 2 Bundesdatenschutzgesetz.	○ Ja ○ Nein
Wurden externe Konten oder Abos angepasst, geändert oder gekündigt?	› Eventuell verfügt der ausscheidende Betriebsrat über entsprechende Nutzerkonten. Die sollten auf andere Betriebsratsmitglieder oder einen Nachfolger übertragen werden. › Werden Benutzerkonten nicht mehr gebraucht, können diese ggf. auch gelöscht werden. Auch das trägt zu mehr Datenschutz und einem gewissen Schutz vor Cyberkriminellen bei. Schließlich kann nichts gestohlen werden, was es nicht mehr gibt.	○ Ja ○ Nein
Sind interne bzw. externe Stellen über die Veränderung informiert?	› Unter Umständen gab es Arbeitsgruppen oder spezifische Ansprechpartner für das betreffende Betriebsratsmitglied, etwa bei der IT-Abteilung oder in der Personalabteilung. Diese sollten über ein Ausscheiden oder einen Wechsel in eine andere Aufgabe informiert werden. Eine solche Änderungsmitteilung kann auch an alle Mitarbeiter verschickt werden. So wird vermieden, dass Mitarbeiter aus Unkenntnis den nunmehr ehemaligen Betriebsrat weiterhin ansprechen. › Eine Information externer Stellen kann ebenfalls geboten sein, etwa wenn es Ansprechpartner bei Gewerkschaften gibt. Achten Sie hier darauf, dass nur unbedingt erforderliche Informationen gegeben werden. So ist es nicht in Ordnung, wenn persönliche Gründe für eine Aufgabe der Funktion mitgeteilt werden.	○ Ja ○ Nein
Gab es eine Übergabe, etwa an einen Nachfolger?	› Vor allem wenn es zu einem vorzeitigen Ausscheiden aus dem Betriebsrat kommt, wird es einen Nachfolger geben. Diesem sollten in Abstimmung mit dem Betriebsratsvorsitzenden etwa Unterlagen oder E-Mails übergeben werden. › Idealerweise wird der Nachfolger über Vorgehensweisen, Prozesse und Besonderheiten informiert. Auch das kann davor schützen, dass etwas falsch gemacht wird, was auch zum Datenschutzproblem werden kann. › Im Rahmen einer Übergabe kann der ausscheidende Kollege daran erinnert werden, dass er auch nach Ende seiner Betriebsratstätigkeit zur Vertraulichkeit verpflichtet ist. Das ergibt sich insbesondere aus Art. 79 Abs. 1 Satz 3 BetrVG.	○ Ja ○ Nein
Ist die Umsetzung der vorgenannten Punkte nachvollziehbar dokumentiert?	› Die Umsetzung der Maßnahmen sollte dokumentiert sein. Nur so ist sichergestellt, dass alle Punkte erledigt sind. › Eine Dokumentation kann auch anhand dieser Checkliste erfolgen. Wurden alle Maßnahmen umgesetzt, reicht auch ein Erledigungsvermerk mit Datum und Unterschrift. Denken Sie daran, die Checkliste in geeigneter Weise abzulegen.	○ Ja ○ Nein

Gratiswissen: Nutzen Sie Tätigkeitsberichte der Aufsicht

Eines ist klar: Für eine effektive Wahrnehmung Ihrer Aufgaben brauchen Sie viel Fachwissen. Und das können Sie beispielsweise bei Schulungen und Tagungen bekommen. Doch gerade wenn Ebbe in der Kasse herrscht, sollten Sie auf Alternativen setzen. So z. B. auf Tätigkeitsberichte von Aufsichtsbehörden. Die sind sehr praktisch, eben Ihr sehr praktisches Schweizer Taschenmesser in Sachen Rechtsanwendung.

Vielleicht ist Ihnen auch schon mal die Meldung untergekommen, dass die eine oder andere Datenschutzaufsichtsbehörde ihren neuen Tätigkeits- oder Jahresbericht veröffentlicht hat. Doch vielleicht hat eine solche Meldung nicht wirklich Ihr Interesse geweckt. Das sollten Sie ändern. Denn Tätigkeitsberichte sind sehr praktisch für Ihre Arbeit. Das erkennen Sie schnell, wenn Sie diese Tipps beherzigen:

Tipp Nr. 1: Durchforsten Sie das Angebot Ihrer Aufsichtsbehörde

Wann waren Sie zuletzt auf der Webseite der für Ihr Unternehmen zuständigen Datenschutzaufsichtsbehörde? Ist das schon länger her, sollten Sie die Seiten unbedingt ansteuern. Machen Sie es sich zum Standard, regelmäßig nach relevanten Veröffentlichungen zu schauen. Gibt es einen neuen Tätigkeitsbericht der Behörde, sichern Sie sich diesen. Legen Sie die PDF-Datei so ab, dass Sie sie schnell wiederfinden. Halten Sie aber nicht nur Ausschau nach dem Tätigkeitsbericht. Oftmals finden Sie Lesenswertes, etwa gerade dort, wo Sie es nicht vermutet hätten. Prüfen Sie also auch die sonstigen Veröffentlichungen, einen Bereich Aktuelles oder eine A-bis-Z-Liste.

Tipp Nr. 2: Erweitern Sie Ihren Horizont

Natürlich ist wichtig, dass Sie wissen, wie die für Ihr Unternehmen zuständige Datenschutzaufsicht tickt. Doch das ist eventuell nur eine Meinung unter vielen. So kann es für Sie von Interesse sein, wie andere Aufsichtsbehörden die Dinge sehen und bewerten. Insofern sollten Sie auch ein Auge auf deren Tätigkeitsberichte werfen. Denn damit können Sie nicht nur feststellen, ob es unterschiedliche Sichtweisen gibt. Sie haben auch Belege dafür, die Dinge ggf. anders als die für Ihr Unternehmen zuständige Aufsichtsbehörde zu sehen. Und das ist in der Praxis von großem Wert. Wird etwa eine Verarbeitung von einer Aufsichtsbehörde als zulässig erachtet, dürften andere Aufsichtsbehörden es schwer haben, aufgrund ihrer Sicht ein Bußgeld zu verhängen.

Tipp Nr. 3: Ordnen Sie Berichte richtig ein

Bedenken Sie stets: Aufsichtsbehörden geben in ihren Berichten ihre Praxis wieder und stellen dar, wie sie die Dinge sehen und bewerten. Auch wenn in Aufsichtsbehörden sehr kompetente Experten tätig sind, heißt das nicht automatisch, dass die in einem Bericht enthaltene Sicht richtig und verbindlich ist. Im Ergebnis können auch Aufsichtsbehörden mit ihrer Einschätzung falschliegen. So z. B., wenn Gerichte und in letzter Instanz der Europäische Gerichtshof über die Deutung und Anwendung der Regelungen zur Datenschutz-Grundverordnung anders entscheiden.

Daher ist wichtig: Betrachten Sie ein Thema oder einen Aspekt immer auf Basis mehrerer Quellen. Weitere Quellen können Berichte und Stellungnahmen anderer Aufsichtsbehörden sein. Daneben sind auch Gesetzeskommentare, rechtswissenschaftliche Veröffentlichungen oder die Stellungnahmen anderer Praktiker wichtig für eine solide Einordnung einer konkreten Auffassung oder Sichtweise.

Tipp Nr. 4: Arbeiten Sie geschickt mit PDF-Dateien

Bei manchen Aufsichtsbehörden gibt es noch gedruckte Berichte, die Sie anfordern können. Doch die verstauben wahrscheinlich eher in Ihrem Bücherregal. Wollen Sie Berichte effizient nutzen, sollten Sie sich das Dokument im PDF-Format herunterladen. Denn dann haben Sie die Möglichkeit, richtig viel mit dem Dokument anzufangen. Sie können beispielsweise

- Lesezeichen setzen und Anmerkungen anbringen. So können Sie über die Lesezeichenübersicht schnell zu wichtigen Punkten navigieren,
- farbliche Markierungen nutzen, um schnell überblicken zu können, wo etwas Relevantes im Bericht steht. Markieren Sie etwa Aspekte, die das Geschäft Ihres Unternehmens betreffen, gelb. Themen, die für das Steigern der Awareness gut geeignet sind, markieren Sie grün. Themen, die auch für Ihr Unternehmen Handlungsbedarf bedeuten, markieren Sie rot,
- mehrere Berichte in einem Dokument zusammenführen, um besser über Jahre hinweg nach Themen oder Stichworten suchen zu können. Dabei sollten Sie die Indexierung Ihres PDF-Programms nutzen, damit bei umfangreichen Dokumenten die Suche ruckzuck erledigt ist.

Tipp Nr. 5: Nutzen Sie Berichte fürs Überzeugen und Sensibilisieren

Tätigkeitsberichte sind ein großes Hilfsmittel, wenn Sie Ihre Argumentation untermauern wollen. Was Aufsichtsbehörden sagen, das hinterlässt meist einigen Eindruck. Schließlich sagt das nicht irgendwer, sondern eine offizielle Stelle. Und die kann im Zweifel sogar dafür sorgen, dass Ihrem Unternehmen der Spaß vergeht, etwa mit einem Bußgeldverfahren. Außerdem sind Tätigkeitsberichte eine wahre Fundgrube, wenn es um Praxisbeispiele geht. Bauen Sie relevante Fälle in Schulungen ein. Gerade wenn Pannen oder Nachlässigkeiten zu ernsten Konsequenzen führen, kann das manchen Teilnehmer nachhaltig beeindrucken.

Soll ich Quartalsberichte für die Unternehmensleitung ablehnen?

FRAGE: Die Unternehmensleitung möchte sich eng mit mir abstimmen. Dazu will die Unternehmensleitung gut darüber informiert sein, was im Datenschutz passiert. Sie hat den Wunsch geäußert, dass ich am Ende jedes Quartals einen Bericht erstelle. Ich meine, dass ein solcher Bericht sehr aufwendig ist. Insofern würde der Bericht doch einiges an Zeit fressen, die ich doch für andere Erledigungen besser einsetzen könnte. Ich frage mich also, ob ich das nicht einfach ablehnen sollte. Was raten Sie?

ANTWORT: Lehnen Sie das nicht einfach ab. Denn: Im Prinzip sollten Sie es zunächst sehr positiv sehen, dass sich Ihre Unternehmensleitung mit dem Datenschutz auseinandersetzt. Zudem ist der enge Austausch eine gute Sache. Das vor allem, weil das in manchen Unternehmen und bei manchem Datenschutzbeauftragten leider eher nicht Standard und die Zusammenarbeit eher schwierig ist.

Die DSGVO macht keine Vorgaben

Für Datenschutzbeauftragte in Unternehmen gibt es in der Datenschutz-Grundverordnung (DSGVO) keine Vorgaben dazu, ob und wie der Unternehmensleitung Bericht zu erstatten ist. Um allerdings einen Überblick über die Datenschutzsituation im Unternehmen zu geben, erstellen viele Datenschutzbeauftragte einen Tätigkeits- oder Jahresbericht. In der Tat kann die Erstellung eines solchen Jahresberichts viel Arbeit und Aufwand mit sich bringen. Allerdings können Sie sich einen solchen Bericht für das Gesamtjahr unter Umständen sparen, wenn Sie im Quartal einen Überblick zum Stand der Dinge geben. Insofern können Quartalsberichte auch eine Erleichterung für Sie sein.

Sehen Sie die Vorteile

Ein Quartalsbericht macht zwar auch Arbeit. Er bringt aber auch so manche Vorteile mit sich, die Sie nicht unterschätzen sollten: Sie können zeitnah die Datenschutzsituation im Unternehmen darlegen. Handlungsbedarf können Sie ohne größeren Verzug aufzeigen. Neue Entwicklungen in rechtlicher, technischer und organisatorischer Hinsicht können früher thematisiert werden. Notwendige Unterstützung können Sie schneller einfordern.

Stimmen Sie sich ab

Klären Sie mit der Unternehmensleitung, was sie sich von einem Bericht verspricht und was ihr am Bericht besonders wichtig ist. Natürlich können auch Sie die Initiative ergreifen. Machen Sie einen Vorschlag, wie ein aus Ihrer Sicht „schlanker" Bericht aussehen kann. Das können beispielsweise einige Kennzahlen sein, etwa zu Anfragen, Beratungen oder Vorfällen. Auch Neuigkeiten zum Datenschutzrecht oder ganz allgemein Berichtenswertes können Punkte sein. Dabei können Sie eine Standardpräsentation mit festen Kapiteln nutzen, die Sie schnell befüllen können.

Was fange ich mit noch genutztem Uralt-Computer an?

FRAGE: Bei einem Gespräch in einer Abteilung kamen wir beiläufig auch auf einen alten Computer mit Windows XP zu sprechen. Der wird noch für eine eigenprogrammierte Software genutzt. Das ist doch ein gewaltiges Sicherheits- und Datenschutzrisiko, oder? Was fange ich mit diesem Uralt-Computer an?

ANTWORT: In der Tat gibt es für das Betriebssystem Windows XP spätestens seit 2014 keinen Support mehr, sprich, Fehler oder Sicherheitslücken werden seit Jahren nicht mehr behoben. Das muss jedoch nicht bedeuten, dass im konkreten Anwendungsszenario erhöhte Risiken für die Sicherheit und für den Datenschutz bestehen.

Werden mit dem Computer personenbezogene Daten verarbeitet, muss mit risikoangemessenen Schutzmaßnahmen dafür gesorgt werden, dass die Sicherheit der Verarbeitung gewährleistet ist.

Damit die Sicherheit passt, sollten Sie mit den Kollegen die Gefahren und die sich ergebenden Risiken ausmachen. Darauf basierend müssen dann Schutzmaßnahmen ergriffen werden, damit die Risiken auf ein vertretbares Maß reduziert werden.

Typische Maßnahmen dürften in diesem Fall etwa sein: Trennung des Computers vom Internet sowie die Übertragung von Daten nur per USB-Stick und nach erfolgter Prüfung auf Viren und Schadsoftware. Flankiert werden sollte das Ganze durch klare Arbeitsanweisungen.

SG Dresden: Gelöscht ist nur, wenn tatsächlich gelöscht ist

Als Datenschutzprofi wissen Sie: Personenbezogene Daten müssen irgendwann gelöscht werden. Doch was ist, wenn das technisch nicht geht? Unter anderem damit beschäftigte sich das Sozialgericht (SG) Dresden in einem Urteil vom 22.10.2025 (Az. S 15 SF 304/24 DS).

Der Sachverhalt

Eine Frau, die spätere Klägerin, war bei einer Migrationsberatungsstelle tätig. Dort unterstützte sie ausländische Mitbürger bei der Beantragung von Leistungen beim Jobcenter, dem späteren Beklagten. In den Systemen des Jobcenters war die Klägerin auch mit einem eigenen Datensatz gespeichert, weil sie früher Anträge für sich selbst stellte. Enthalten waren z. B. ihr Name und ihre Privatanschrift.

Nun passierte Folgendes: Die Klägerin unterstützte eine Mitbürgerin, eine sogenannte Klientin, bei der Beantragung von Leistungen. Dazu legte sie eine Schweigepflichtentbindung vor und erbat vom Jobcenter Informationen. Das Jobcenter sah die Klägerin nun als Bevollmächtigte dieser Klientin an. In der Folge wurden in der Akte der Klientin auch die bereits vorhandenen Stammdaten der Klägerin hinterlegt, sprich insbesondere ihr Name und ihre Privatadresse. Anstatt an die dienstliche Adresse schickte das Jobcenter die angefragten Informationen zur Klientin an die Privatanschrift der Klägerin und nicht an die dienstliche Postanschrift.

Die Klägerin meldete sich beim Jobcenter und beanstandete eine Datenschutzverletzung. Zudem beantragte sie die Löschung ihrer Privatadresse und persönlicher Informationen aus der Akte.

Jobcenter lehnt Löschung ab

Gegen diesen Bescheid legte die Klägerin Widerspruch ein. Zwar räumte das Jobcenter eine Datenschutzverletzung ein. Allerdings habe man die fehlerhafte Datenverknüpfung der Adressen behoben. Ferner wären die Datenblätter mit den privaten Adressdaten in der elektronischen Akte der Klientin ausgeblendet worden, sodass etwa eine unrechtmäßige Kenntnisnahme ausgeschlossen sei. Mehr als ein Ausblenden sei technisch nicht möglich.

Die Frau akzeptierte das nicht. Sie klagte vor dem SG gegen den Ablehnungs- und den Widerspruchsbescheid. Dort bekam sie teilweise recht, allerdings erhielt sie insbesondere den geltend gemachten Schadensersatz in Höhe von 200 € nicht zugesprochen.

So urteilte das SG

Die angefochtenen Bescheide waren rechtswidrig. Allerdings nur, soweit die Löschung der Privatadresse der Klägerin aus der Akte der Klientin abgelehnt wurde. Die Klägerin hat einen Anspruch auf Löschung der Privatadresse nach Art. 17 Abs. 1 Buchst. d Datenschutz-Grundverordnung (DSGVO). Hinsichtlich des Namens besteht jedoch kein Anspruch auf Löschung. Eine unrechtmäßige Verarbeitung durch das Jobcenter gab es nur hinsichtlich der Privatadresse der Klägerin. Diesbezüglich gab es für das Jobcenter keine Rechtsgrundlage. Insbesondere gab es kein Einverständnis für eine Verwendung der Privatadresse. Die Verwendung ihres Namens, etwa im Zusammenhang mit der Zusendung von Informationen der Klientin an die dienstliche Adresse, wäre hingegen zulässig. Aus Sicht des Gerichts liegt hierfür eine Einwilligung vor, die nicht widerrufen wurde. Zudem ist der Name der Klägerin im Zusammenhang mit einem Auskunftsanspruch bezüglich Leistungen des Jobcenters verarbeitet worden. Insofern steht einer Löschung Art. 17 Abs. 3 Buchst. b Variante 2 DSGVO entgegen.

Ausblenden ist kein Löschen

Zwar ist Löschen in der DSGVO nicht definiert. Allerdings ist darunter der Entzug des Personenbezugs zu verstehen, sodass es faktisch unmöglich ist, die zuvor in den zu löschenden Daten verkörperte Information wahrzunehmen. Die personenbezogenen Daten dürfen nicht mehr Teil der Datenverarbeitung sein, was unumkehrbar sichergestellt sein muss. Ein Ausblenden führt jedoch nicht zu einem Löschen. Die Daten sind vorhanden, auch wenn sie nicht sichtbar sind. An der Irreversibilität fehlt es, wenn ein Wiedereinblenden möglich ist. Dass ein Programm technisch nicht löschen kann, führt nicht dazu, dass ein Ausblenden dem Löschen gleichkommt. Es muss vielmehr technisch dafür gesorgt werden, dass geltende Gesetze und Betroffenenrechte umgesetzt werden können.

Keinen Schaden nachgewiesen

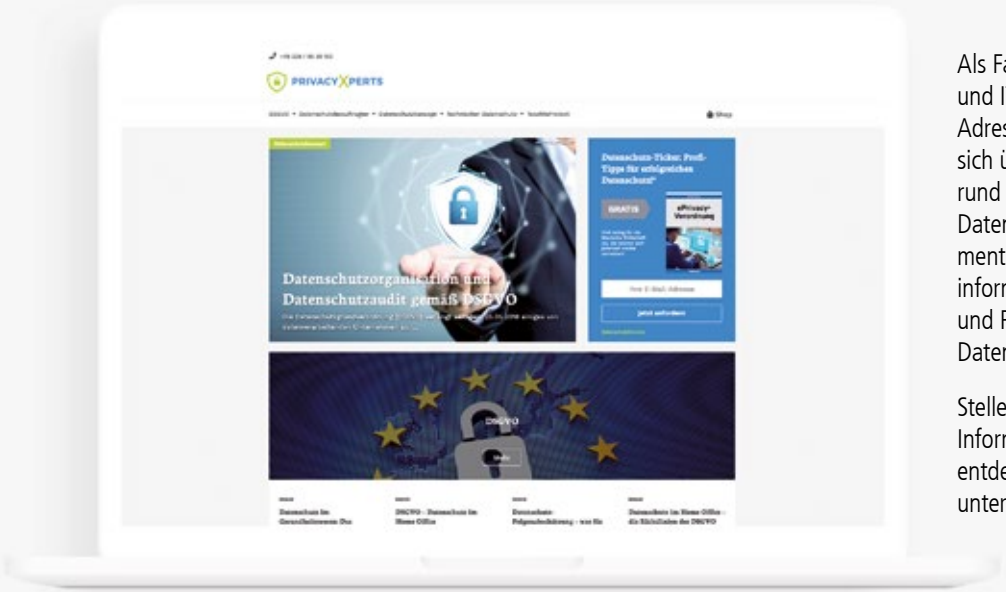
Ein Anspruch auf Schadensersatz nach Art. 82 Abs. 1 DSGVO besteht nicht. Zwar gibt es hier einen Datenschutzverstoß. Allerdings ist der Klägerin kein konkreter Schaden entstanden. In diesem Zusammenhang hätte die Klägerin den Zusammenhang mit dem Verstoß nachweisen müssen. Zudem reicht ein rein hypothetisches Risiko für einen Datenmissbrauch nicht aus. Hier hatten Dritte die betreffenden Daten gerade nicht zur Kenntnis genommen.

§

Das können Sie aus der Entscheidung folgern

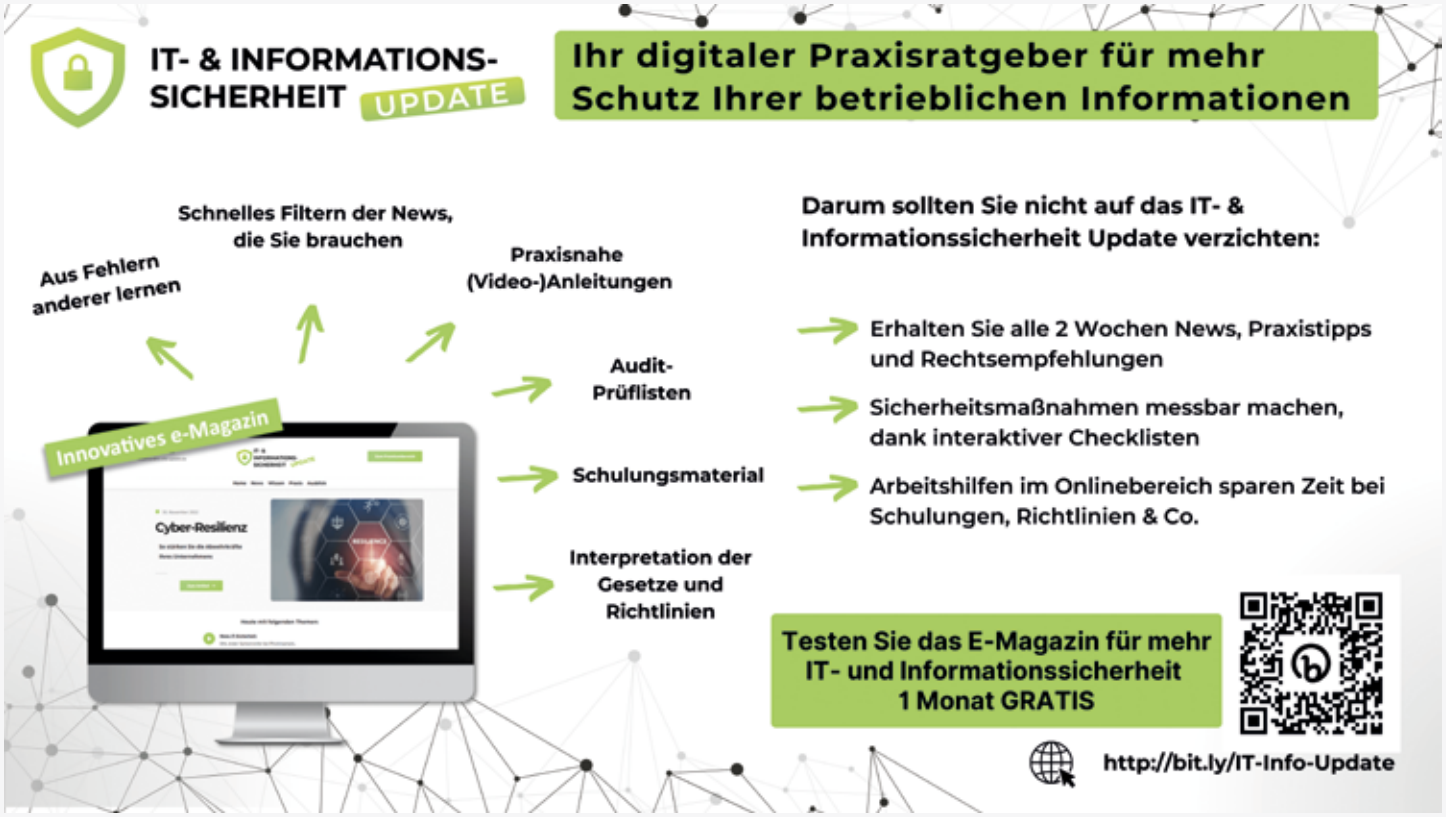
Die Entscheidung macht klar, dass Löschen nur Löschen ist, wenn der Personenbezug bei Daten irreversibel entfernt wird. Eine spätere Zuordnung von Informationen darf tatsächlich nicht mehr möglich sein. Dass ein System oder eine Software keine Löschung vorsieht, ist kein Grund, um dem Löschanspruch nicht nachzukommen. In einem solchen Fall muss die entsprechende Funktion nachgerüstet oder es muss eine andere Software beschafft werden.

„Datenschutz aktuell“ ist ein Produkt der PrivacyXperts-Familie!



Als Fachverlag für Beratung im Bereich Datenschutz und IT-Security sind Sie bei uns genau an der richtigen Adresse, wenn es um Ihre Themen geht. Lassen Sie sich über unsere Fachinformationsdienste und Portale rund um neue EU-Verordnungen, aktuelle Urteile zum Datenschutzrecht oder über die umfangreichen Dokumentationspflichten für Datenschutzverantwortliche informieren. So erhalten Sie nützliche Informationen und Praxistipps für Ihre Arbeit und sind beim Thema Datenschutz bestens aufgestellt.

Stellen Sie eine direkte Verbindung zu verlässlichen Informationen und aktuellen Entwicklungen her und entdecken Sie viele weitere Datenschutz-Produkte unter **www.privacyxperts.de/shop**



Telefon: 02 28 95 50 150
Fax: 02 28 36 96 480
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de

Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2–4
53177 Bonn