DATENSCHUTZAKTUELL Professional
SEP II 2025
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

UNBEKANNTES RISIKO SCHATTEN-IT: BRINGEN SIE LICHT INS DUNKEL

Onlinebereich: www.privacyxperts.de/login
Expertensprechstunde: https://t1p.de/andreas-wuertz
PRIVACYXPERTS

Gesundes Misstrauen ist immer gut

Liebe Leserin, lieber Leser,

als Datenschutzbeauftragter sind Sie ein gefragter Ansprechpartner. Schließlich wollen auch die Mitarbeiter Ihres Unternehmens nach Möglichkeit nichts falsch machen, wenn personenbezogene Daten im Spiel sind. Doch manch einer will sich vielleicht eher Ihr „grünes Licht" ergaunern und bleibt bei seinen Informationen nicht ganz bei der Wahrheit.

Gerade wenn eine Sache irgendwie „zu rund" ist oder man nur ganz schnell noch Ihren „Segen" einholen will, sollten Sie misstrauisch sein. Lassen Sie sich kein X für ein U vormachen. Klären Sie alles, was Sie für Ihre Einschätzung brauchen. Dann passt auch Ihre Beratung.

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

Bildnachweise:
Titel: Adobe Stock | BalanceFormCreative
Seite 1: Adobe Stock | greenbutterfly

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: Deinzer Grafik, Gartow

Druck: Warlich Druck Meckenheim GmbH, Am Hambuch 5, 53340 Meckenheim

Erscheinungsweise: 36-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

Nutzen Sie unsere Anleitung, um Schatten-IT aufzuspüren.

Unbekanntes Risiko Schatten-IT: Bringen Sie Licht ins Dunkel

Als Datenschutzprofi wissen Sie: Für den Schutz aller Daten im Unternehmen ist es unerlässlich, dass Risiken erkannt und angemessene Maßnahmen ergriffen werden, um diese zu minimieren. Doch manche Gefahren sind nicht offenkundig und gleichen dennoch einer Zeitbombe. So ist das beispielsweise beim Thema Schatten-IT der Fall. Bringen Sie hier Licht ins Dunkel.

Das ist das Problem

Schatten-IT und Schatten-Software hat nichts mit viel Sonne zu tun. Gemeint sind insbesondere IT-Systeme oder Software, die unerkannt „im Schatten liegen", weil sie von Abteilungen oder Mitarbeitern ohne Wissen und Genehmigung der IT-Abteilung beschafft und eingesetzt werden. Ohne lange grübeln zu müssen, erkennen Sie ganz schnell, dass das früher oder später schiefgehen kann. Schließlich ist zu bedenken:

- Schatten-IT und Schatten-Software bringen häufig auch eine unklare Sicherheitssituation mit sich. Manchmal wird einfach beschafft, ohne zu wissen, wie es um die Sicherheit der Systeme oder Software bestellt ist. Denn nur weil etwas funktioniert und seinen primären Zweck erfüllt, heißt das nicht, dass damit verarbeitete Daten auch sicher sind.

- Gerade im Zusammenhang mit personenbezogenen Daten muss bei deren Verarbeitung auf die Sicherheit geachtet werden. Nach Art. 32 Datenschutz-Grundverordnung (DSGVO) müssen risikoangemessene Schutzmaßnahmen ergriffen werden. Und die treffen Ihr Unternehmen als Verantwortlicher und nicht etwa einen Hersteller eines Systems oder einer Software.

- Schatten-IT und Schatten-Software fliegen oft unter dem Radar der IT-Abteilung. Konkret heißt das: Die Profis bekommen überhaupt nicht mit, dass es bestimmte Systeme oder Software gibt, die in eine Update-Strategie einzubeziehen sind. Die Folge: Entsprechende Hard- und Software wird nicht mit den nötigen Updates versorgt. Über die möglicherweise aufkommenden Sicherheitslücken haben Hacker und Cyberkriminelle leichtes Spiel.

- Unbekannte Systeme und Software sind gerade im Zusammenhang mit personenbezogenen Daten ein großes Problem: So können nötige Datenschutzvereinbarungen fehlen, etwa im Rahmen einer Auftragsverarbeitung nach Art. 28 DSGVO. Unter Umständen verwendet der Hersteller personenbezogene Daten für eigene Zwecke, ohne dass es hierfür eine Rechtsgrundlage gibt. Auch kann es Probleme mit den Betroffenenrechten geben, etwa im Hinblick auf die nötige Transparenz sowie die Umsetzung der Rechte auf Auskunft oder Löschung. Und solche Datenschutzverstöße können bekanntlich viel Ärger nach sich ziehen und schlimmstenfalls auch ein schmerzhaftes Bußgeld, für das die Portokasse nicht ausreicht.

- Schatten-IT und Schatten-Software können Ihr Unternehmen finanziell ruinieren, etwa nach einem erfolgreichen Angriff von Cyberkriminellen. Denn selbst eine entsprechende Versicherung wird unter Umständen nicht zahlen, weil Ihr Unternehmen grob fahrlässig einen Schaden herbeigeführt hat. Schließlich hat es nicht dafür gesorgt, dass mögliche Risiken durch Schatten-IT und Schatten-Software ausgeschlossen werden.

Heben Sie die Hand

Als Datenschutzbeauftragter haben Sie nicht den Auftrag, die (Datenschutz-)Welt zu retten. Allerdings ist es Teil Ihres Beratungs- und Kontrollauftrags, dass Sie auf realistische Gefahren mit Datenschutzrelevanz hinweisen, und zwar für Ihr Unternehmen. Solche Risiken treten gerade im Zusammenhang mit unbekannter und unkontrolliert eingesetzter Hard- und Software auf. Dabei ist klar: Kommt es zu einer Datenpanne, ist es unerheblich, wer schlussendlich daran schuld ist. Ihr Unternehmen ist dafür verantwortlich. Auch das (Fehl-)Verhalten von Mitarbeitern wird ihm meist zugerechnet.

Sie wollen Schatten-IT und Schatten-Software aufspüren? Kein Problem. Sie brauchen hier nicht das Rad neu zu erfinden. Setzen Sie auf die folgende Schritt-für-Schritt-Anleitung:

Schritt 1: Sammeln Sie Einfälle und Ideen

Starten Sie zunächst damit, dass Sie sich Gedanken zu Ihrem Unternehmen, zur Geschäftstätigkeit und vor allem zu Bereichen machen, in denen Schatten-IT oder Schatten-Software zum Einsatz kommen könnten. Das kann z. B. in der Entwicklung sein. Schatten-Software finden Sie vielleicht im Bereich Vertrieb oder beim Marketing. Denken Sie hier auch an Ihre Beratungen, bei denen man sich mit den zur Verfügung stehenden Mitteln unzufrieden gezeigt hat. Auch unter Datenschutzaspekten Durchgefallenes wird vielleicht dennoch eingesetzt.

Schritt 2: Checken Sie das Verzeichnis von Verarbeitungstätigkeiten

Prüfen Sie die enthaltenen Verarbeitungstätigkeiten. Diese sollten vollständig erfasst sein. Achten Sie auch auf die Aktualität der Angaben. Finden Sie Angaben zu eingesetzten Systemen oder Software, sollten Sie auf Ihnen unbekannte Anbieter oder Produktnamen achten. Überlegen Sie außerdem, welche Verarbeitungstätigkeiten fehlen könnten oder welche Verarbeitungen ggf. nicht erfasst sind.

Schritt 3: Schauen Sie sich im Unternehmen um

Informieren Sie sich, was in Ihrem Unternehmen läuft. Wichtige Erkenntnisse kann es auch bringen, wenn Sie sich vor Ort umschauen oder mit Mitarbeitern sprechen. Sehen Sie beispielsweise Gerätschaften, die eher privater Natur sind, sollten Sie klären, was es damit auf sich hat. Denn: Auch private Geräte können gefährliche Schatten-IT sein. Nicht anders ist es mit privater Software oder privaten E-Mail- oder Cloud-Lösungen. Für die ist der Unternehmenseinsatz tabu.

Schritt 4: Tauschen Sie sich mit den IT-Kollegen aus

Besprechen Sie sich mit den Kollegen aus der IT-Abteilung. Machen Sie deutlich, dass Schatten-IT und Schatten-Software auch unter Datenschutzaspekten ein großes Problem sein können. So z. B., wenn es um die Sicherheit der Verarbeitung geht. Bitten Sie um die Einschätzung und Erfahrung der Kollegen zu diesem Thema. Hinterfragen Sie, was man unternimmt, um Schatten-IT und Schatten-Software nicht zum Problem werden zu lassen. Klären Sie, inwieweit verhindert wird, dass Hard- und Software abseits der Prozesse eingesetzt werden.

Schritt 5: Machen Sie ein gemeinsames Risiko-Brainstorming

Identifizieren Sie gemeinsam mit den IT-Kollegen einerseits die Bereiche, wo Schatten-IT und Schatten-Software ein Thema sein könnten. Überlegen Sie außerdem, welche praktischen Möglichkeiten es gibt, die Sache zu überprüfen.

Schritt 6: Ermitteln Sie die Situation

Hier empfiehlt sich ein mehrstufiger Ansatz. So kann zunächst eine Prüfung der Dokumentation erfolgen. Schauen Sie mit den Kollegen der IT-Abteilung gemeinsam vorhandene Inventarlisten durch. Finden Sie dort offensichtlich veraltete Technik oder veraltete Software, hat man vielleicht in der betreffenden Abteilung schon auf etwas Neueres gewechselt. Eventuell wird Software auch zentral inventarisiert. Hier können die Kollegen meist schnell sagen, ob sie hier Unbekanntes oder Ungenehmigtes vorgefunden haben.

Als nächste Stufe bietet es sich an, dass Sie mit den Kollegen vor Ort nach dem Rechten schauen. Statten Sie den Bereichen einen Besuch ab. Führen Sie dort auch Interviews mit den Führungskräften und Mitarbeitern. Zeigen Sie die Risiken durch Schatten-IT und Schatten-Software auf und hinterfragen Sie, inwieweit man hierauf setzt.

Schritt 7: Identifizieren Sie den Handlungsbedarf

Ist Schatten-IT oder Schatten-Software im Einsatz, ist schnelles Handeln geboten. Klären Sie mit den Kollegen der IT-Abteilung und den betroffenen Bereichen, wie man zügig einen ordnungsgemäßen und regelkonformen Zustand erreichen kann. Unter Umständen sollte die betreffende Hard- und Software zunächst einmal außer Betrieb genommen werden, um Risiken zu minimieren.

Schritt 8: Vereinbaren Sie die nötigen Maßnahmen

Achten Sie darauf, dass zügig gehandelt wird. Dabei ist klar: Über dieses Problem zu reden, reicht nicht aus. Es muss gelöst werden. Das geht nur mit den passenden Maßnahmen. Damit es keine Missverständnisse darüber gibt, wer verantwortlich ist und was zu tun ist, sollten die Maßnahmen konkret festgehalten und verbindlich vereinbart werden.

Schritt 9: Begleiten Sie die Umsetzung

Auch wenn es an das Umsetzen geht, kann Ihr Rat als Datenschutzbeauftragter gefragt sein. Wird das Thema „Schatten-IT und Schatten-Software“ bereinigt, müssen ggf. Daten umgezogen oder Datenträger entsorgt werden. Logisch, dass das sicher passieren muss.

Schritt 10: Kontrollieren Sie die Einhaltung

Als Datenschutzbeauftragter sollen Sie auch die Einhaltung der Vorschriften zum Datenschutz kontrollieren. Integrieren Sie hier den Punkt „Kontrolle von Schatten-IT und Schatten-Software“. Selbst wenn Sie nicht fündig werden, sollten Sie die Gelegenheit nutzen, um für die diesbezüglichen Gefahren zu sensibilisieren.

Besserer Datenschutz durch bessere Fehlerkultur? So können Sie das schaffen

Sie kennen den Spruch: Wo gehobelt wird, da fallen Späne. Klar, dass dort, wo gearbeitet wird, auch etwas schiefgehen kann. Passiert das beim Umgang mit personenbezogenen Daten, kann ein „Kann ja mal passieren" die Probleme und den Schaden noch vergrößern. Um dem vorzubeugen, ist es wichtig, eine gute Fehlerkultur zu etablieren.

Fördern Sie, dass man aus Fehlern lernt

Als Datenschutzbeauftragter können Sie sich nicht um alles kümmern. Das geht schon einfach aus Kapazitätsgründen nicht. Umso wichtiger ist, dass Sie Hilfe zur Selbsthilfe leisten. Die kann beispielsweise auch darin bestehen, dass Sie zunächst einmal den Boden für eine gute Fehlerkultur bereiten. Denn nichts ist schlimmer, als Fehler nicht auch als Chance zu sehen und die Dinge zukünftig besser zu machen. Dazu können Sie beispielsweise auf das folgende Muster setzen:

Beugen Sie Angst und Misstrauen vor
Bedenken Sie stets, dass Sie als Datenschutzbeauftragter von vielen Beschäftigten auch als Autoritätsperson wahrgenommen werden. Vielleicht misstraut auch mancher dem Umstand, dass man sich vertrauensvoll an Sie wenden kann, und zwar auch, wenn mal etwas schiefgegangen ist oder falsch gemacht wurde. Daher ist wichtig: Machen Sie bei jeder Gelegenheit deutlich, dass man sich bei Fragen, Problemen oder Pannen im Datenschutz an Sie wenden kann.

MUSTER: Info-Schreiben „Fehler haben auch etwas Gutes"

Liebe Kolleginnen und Kollegen,

Sie kennen bestimmt den Spruch „Aus Schaden wird man klug". Der mag stimmen und hier und da seine Berechtigung haben. Allerdings ist ein Schaden ein schwacher Trost, gerade im Datenschutz. Schließlich ist ein entstandener Schaden beim falschen Umgang mit personenbezogenen Daten oft ziemlich groß. Auch das Image unseres Unternehmens kann tiefe Kratzer davontragen. Also sollten wir uns alle an Folgendem orientieren: „Aus Fehlern wird man klug." Denn dann kommt es erst gar nicht zu weiteren Schäden.

Fehler können passieren
Seien wir ehrlich: Die Geschäfts- und Arbeitswelt wird immer herausfordernder. Auch der Umgang mit personenbezogenen Daten ist komplex. Selbst wenn wir uns anstrengen und große Sorgfalt walten lassen, kann es passieren, dass etwas nicht optimal läuft oder schiefgeht.

Fehler sind wichtig
Natürlich liegt auf der Hand: Jeder Fehler im Umgang mit personenbezogenen Daten ist ärgerlich. Doch die damit gemachte Erfahrung bietet zugleich die Chance, die Dinge in Zukunft besser zu machen. Manche Entwicklung hätte es nicht gegeben, wenn nicht etwas schiefgegangen wäre. Denken Sie nur an die gelben Klebezettel, die heutzutage in jedem Büro zu finden sind.

Helfen Sie, die Dinge besser zu machen
Sehen Sie beispielsweise, dass jemand Unterlagen mit schützenswertem Inhalt falsch entsorgt, sollten Sie nicht einfach wegschauen. Sprechen Sie den Kollegen an. Dabei ist wichtig: Schuldzuweisungen sind meist fehl am Platz. Fragen Sie lieber, ob sich der Kollege sicher ist, die richtige Vorgehensweise gewählt zu haben. Teilen Sie Ihre Sicht der Dinge. Erläutern Sie Ihre Einschätzung und geben Sie so Hilfestellung, das eigene Handeln zu überdenken.

Außerdem ist wichtig: Sprechen Sie Fehler im Kollegenkreis oder in der Abteilung offen an. Dabei müssen Sie niemanden an den Pranger stellen. Wichtig ist vielmehr, dass alle über die Situation, das Problem und die passende Lösung informiert sind und sich dazu austauschen. Setzen Sie beispielsweise in der Diskussion auf ein „Ich habe kürzlich bemerkt, dass Unterlagen falsch entsorgt wurden. Das sollte vermieden werden, indem wir ...".

Ihr Beitrag ist entscheidend
Gehen Sie offen mit Problemen und Fehlern um, leisten Sie Großes: Sie tragen dazu bei, eine positive Fehlerkultur zu etablieren. Dabei ist klar: Werden Probleme oder Fehler frühzeitig erkannt, können sie auch schnell angegangen werden. Zugleich tragen Ihr Wissen und Ihre Erfahrungen dazu bei, dass sich Fehler nicht wiederholen. Und davon profitieren alle: das Unternehmen, die Beschäftigten und diejenigen, die uns ihre Daten anvertrauen.

Mein Versprechen an Sie
Auch mir als Datenschutzbeauftragtem ist an einer guten Fehlerkultur gelegen. Es ist mir wichtig, dass alle mit Fehlern offen umgehen, gerade im Hinblick auf den Umgang mit personenbezogenen Daten. Brauchen Sie Unterstützung oder Rat? Melden Sie sich bei mir. Haben Sie etwas falsch gemacht oder läuft etwas im Unternehmen schief? Lassen Sie uns darüber reden. Dabei ist klar: Vertraulichkeit ist bei mir garantiert.

Ihr Datenschutzbeauftragter
Sepp Tember

So gehen Sie mit dem Thema NIS-2-Richtlinie um

Seit 2022 gibt es sie schon: die Richtlinie (EU) 2022/2555 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union, kurz NIS-2-Richtlinie (NIS-2-RL). Für viele Unternehmen bedeutet die NIS-2-RL viel Anpassungsbedarf, um etwa gut gegen Cyberkriminelle gewappnet zu sein. Doch welche Relevanz hat die Richtlinie für Sie als Datenschutzbeauftragten?

Darauf zielt die NIS-2-Richtlinie ab

Die Richtlinie macht den EU-Mitgliedstaaten Vorgaben, um die IT-Sicherheit in der EU vor allem bei wesentlichen und wichtigen Einrichtungen zu erhöhen. So sollen alle besser gegen aktuelle und zukünftige Risiken gewappnet sein. Weil es sich um eine Richtline handelt, bedarf es im Gegensatz zu einer Verordnung (z. B. wie bei der Datenschutz-Grundverordnung (DSGVO)) der Umsetzung in nationales Recht. Dazu hatten die Mitgliedstaaten bis Oktober 2024 Zeit.

Hier finden Sie das Regelwerk
Sie wollen sich ein eigenes Bild der NIS-2-RL machen? Die Richtlinie finden Sie auf den Seiten der EU in allen Amtssprachen, und zwar hier: https://t1p.de/txuvk.

In Deutschland noch nicht umgesetzt

Mit dem „NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG)“ sollen die Vorgaben der Richtlinie unter anderem in das BSI-Gesetz (BSIG) integriert werden. Wie schnell das Ganze geht, muss sich zeigen. Deutschland steht hier noch immer ziemlich am Anfang des Gesetzgebungsverfahrens. Inzwischen gibt es einen Regierungsentwurf vom 25.7.2025 (https://t1p.de/m7w6u). Ob es also zum Jahresende noch etwas wird, kann niemand vorhersagen. Über den Stand des Verfahrens können Sie sich beim Bundesinnenministerium informieren, und zwar hier: https://t1p.de/0z9vh.

Wie passt die NIS-2-RL zur DSGVO?

„Die NIS-2-RL hat mit Datenschutz nichts zu tun“ – diese Aussage ist an sich richtig, aber auch nicht so ganz. Zwar ist für den Umgang mit personenbezogenen Daten auch in Zukunft die DSGVO entscheidend. Ergreift ein Unternehmen Schutzmaßnahmen, um etwa den Anforderungen auf Basis der NIS-2-RL zu entsprechen, und werden dabei personenbezogene Daten verarbeitet, gelten hierfür jedoch die Rahmenbedingungen der DSGVO (Erwägungsgrund 14 zur NIS-2-RL).

Andererseits liegt auf der Hand: Viele Schutzmaßnahmen werden beide Bereiche abdecken, eben die Sicherstellung der IT-Sicherheit auf Basis der NIS-2-RL und zugleich die Gewährleistung der Umsetzung der DSGVO (z. B. Sicherheit der Verarbeitung nach Art. 32 DSGVO).

Entscheidende Frage: Ist Ihr Unternehmen betroffen?

Klar ist: Der Anwendungsbereich der NIS-2-RL bezieht mehr Unternehmen ein als die Vorgängerregelung. Unter Umständen wird der Anwendungsbereich in Deutschland mit dem NIS2UmsuCG ausgeweitet. Weil es aber nicht klug ist, auf dieses Gesetz zu warten, sollte Ihr Unternehmen prüfen, inwieweit es schon nach den Vorgaben der NIS-2-RL die kommenden Anforderungen erfüllen muss.

Und jetzt wird es kompliziert: Entscheidend ist, ob Ihr Unternehmen als wesentliche oder wichtige Einrichtung gilt. Hierfür sind Art. 3 NIS-2-RL, die Anlagen zur NIS-2-RL sowie der Anhang der Empfehlung 2003/361/EG (https://t1p.de/q84il) zu Unternehmensgrößen entscheidend. Außerdem wichtig: Im zukünftigen BSIG werden Festlegungen enthalten sein, was der deutsche Gesetzgeber unter besonders wichtigen Einrichtungen (entspricht dem Begriff der wesentlichen Einrichtung nach der NIS-2-RL) und wichtigen Einrichtungen versteht. Allerdings gibt es bislang nur einen Regierungsentwurf für eine Regelung in Deutschland. Zur Betroffenheit dürfte in Deutschland wohl gelten:

Voraussetzungen für die Einstufung als besonders wichtige (= wesentliche) Einrichtung:

- mindestens 250 Mitarbeiter oder
- ein Jahresumsatz von mehr als 50 Mio. € und eine Jahresbilanzsumme von mehr als 43 Mio. € und
- Geschäftstätigkeit in einem Sektor, der in Anhang I zur NIS-2-RL aufgeführt ist. Das sind beispielsweise die Sektoren Energie, Verkehr, Bankwesen, Gesundheitswesen oder digitale Infrastruktur. Nach deutschen Vorgaben dürften das zudem kritische Anlagen sein sowie Einrichtungsarten nach der Anlage 1 zum zukünftigen BSIG.

Achtung: Manche Einrichtungen gelten generell als besonders wichtige Einrichtungen. Schauen Sie hierzu in Art. 3 NIS-2-RL bzw. in § 28 des Entwurfs zum zukünftigen BSIG. Beispielsweise bei kritischen Einrichtungen kommt es auf Mitarbeiterzahl und Umsatzzahlen nicht an.

Voraussetzungen für die Einstufung als wichtige Einrichtung:

- mindestens 50 Mitarbeiter oder
- ein Jahresumsatz von mehr als 10 Mio. € und eine Jahresbilanzsumme von mehr als 10 Mio. € und
- eine Geschäftstätigkeit in einem Bereich, der in Anhang I und II zur NIS-2-RL aufgeführt ist, die Voraussetzungen für eine wesentliche Einrichtung jedoch nicht gegeben sind (Art. 3 Abs. 3 NIS-2-RL). Zudem kann die relevante Geschäftstätigkeit in Anlage 1 und 2 des zukünftigen BSIG aufgeführt sein.

Die Folgen sind weitreichend

Ist Ihr Unternehmen als besonders wichtige oder wichtige Einrichtung einzustufen, hat es viele Hausaufgaben zu erle-

digen, um die Sicherheit auf das nötige Niveau zu bringen. Das gilt erst recht, wenn Ihr Unternehmen bislang wenig in die IT-Sicherheit investiert hat. Typische Aktivitäten sind etwa der Aufbau eines IT-Sicherheits- und Risikomanagements, das Etablieren von Standards zur Bewältigung von Zwischenfällen oder die Absicherung der Lieferketten.

Vorsicht: Anwendung durch die „Hintertür“
Auch wenn Ihr Unternehmen an sich nicht als besonders wichtige oder wichtige Einrichtung gilt, können die NIS-2-RL bzw. die deutschen Vorgaben dennoch anzuwenden sein. Das kann passieren, wenn Ihr Unternehmen beispielsweise IT-Dienstleister ist und ein Auftraggeber als besonders wichtige oder wichtige Einrichtung gilt. Dann muss der Auftraggeber auch seine Lieferkette absichern. Das wiederum kann dazu führen, dass die Einhaltung der Vorgaben vertraglich vereinbart wird. Hier heißt es also: Bei Vereinbarungen mit anderen Unternehmen genau hinschauen. Müssen umfassende Maßnahmen ergriffen werden, kann das auch für den Dienstleister aufwendig und teuer werden.

Unterstützen Sie im Rahmen Ihrer Aufgaben

Als Datenschutzbeauftragter haben Sie Ihren Fokus weiterhin auf dem Umgang mit personenbezogenen Daten. Allerdings können Sie den zuständigen Kollegen oder der Unternehmensleitung Tipps geben, wie man an die Sache herangehen kann. Wie wäre es mit den folgenden Schritten?

CHECKLISTE: Schritt-für-Schritt-Anleitung NIS-2-Richtlinie

Ablauf	Achten Sie hierauf	Umgesetzt?
Schritt 1: Klären Sie, inwieweit Ihr Unternehmen betroffen ist.	› Prüfen Sie, ob die Festlegungen aus der NIS-2-RL dazu führen, dass Ihr Unternehmen aller Voraussicht nach die Anforderungen umsetzen muss. Diese werden sich insbesondere aus dem angepassten BSIG ergeben. › Schauen Sie, inwieweit Ihr Unternehmen indirekt betroffen ist. So kann Ihr Unternehmen ggf. nicht direkt den Anforderungen der NIS-2-RL und der deutschen Umsetzung unterliegen. Ggf. werden die Anforderungen an Ihr Unternehmen im Rahmen von Aufträgen weitergegeben.	☐ Ja ☐ Nein
Schritt 2: Verantwortliche festlegen und Projekt starten	› Steht fest, dass Ihr Unternehmen die Anforderungen umsetzen muss, ist es unumgänglich, die Sache anzugehen. Aussitzen ist nicht drin. › Ihr Unternehmen sollte ein Projektteam zusammenstellen, damit der nötige Handlungsbedarf ausgemacht wird. Zudem müssen Entscheidungen getroffen und Maßnahmen umgesetzt werden.	☐ Ja ☐ Nein
Schritt 3: Gefahren und Risiken analysieren und bewerten	› Ihr Unternehmen muss die Risiken an sich ausmachen, die sich aus der Geschäftstätigkeit bzw. etwa aus der Bedrohungssituation durch Cyberkriminelle ergeben. Risiken können sich aber auch aus Dienstleistungen ergeben, die man gegenüber anderen erbringt. › Auch die Umsetzung der Vorgaben an sich sollte unter Risikoaspekten betrachtet werden. Ggf. wird es keine oder nur kurze Übergangsfristen in Deutschland geben. › Es müssen Maßnahmen abgeleitet werden, um mit den Risiken angemessen umzugehen.	☐ Ja ☐ Nein
Schritt 4: Bestandsaufnahme durchführen	› Überblick zu gewinnen ist wichtig. Ggf. ist schon vieles in Ihrem Unternehmen vorhanden und manche Maßnahmen sind ausreichend. › Ideal ist ein Soll-Ist-Abgleich bzw. eine Analyse der Lücken (sogenannte Gap-Analyse). Passt das Ist noch nicht, müssen Maßnahmen festgelegt werden, um das Soll zu erreichen.	☐ Ja ☐ Nein
Schritt 5: Regelungen, Standards und Prozesse etablieren	› Diese Festlegungen sind entscheidend, damit die Sache insgesamt funktionieren kann. › Prozesse dürfen nicht nur auf dem Papier funktionieren. Hier ist die Praxis entscheidend.	☐ Ja ☐ Nein
Schritt 6: Beschäftigte sensibilisieren und qualifizieren	› Relevante Beschäftigte müssen über das erforderliche Know-how verfügen. Auch das ist nötig, um Risiken zu minimieren. Schulungen und Sensibilisierungsmaßnahmen sind unerlässlich. › IT-Sicherheit ist meist etwas für Spezialisten. Laienhafte Kenntnisse führen früher oder später zu Schäden. Hinterfragen Sie die Qualifikation der zuständigen Kollegen.	☐ Ja ☐ Nein
Schritt 7: Meldepflichten organisieren	› Zukünftig wird es besondere Meldepflichten geben, etwa zu IT-Sicherheitsvorfällen. Hierzu müssen Prozesse festgelegt und Verantwortliche benannt werden. › Empfehlen Sie, dass man die zukünftigen Regelungen des BSIG im Auge behält. Hier wird es Vorgaben zu Meldepflicht und Meldeweg geben.	☐ Ja ☐ Nein
Schritt 8: Dokumentation erstellen	› Die ergriffenen Maßnahmen müssen dokumentiert sein. Damit kann Ihr Unternehmen belegen, welche Umsetzungsmaßnahmen ergriffen wurden. › Die Dokumentation darf keine Lücken aufweisen. Außerdem ist Aktualität entscheidend.	☐ Ja ☐ Nein
Schritt 9: Prüfung der Umsetzung	› Dass Maßnahmen wirksam umgesetzt sind und funktionieren, muss durch Kollegen geprüft werden, die das fachlich gut beurteilen können. › Ggf. ist eine Prüfung durch externe Spezialisten oder eine Zertifizierung nötig, etwa weil ein Geschäftspartner eine unabhängige Bewertung fordert.	☐ Ja ☐ Nein
Schritt 10: Anpassungsbedarf fortlaufend ermitteln	› Es ist vieles noch im Fluss. Insofern muss fortlaufend geprüft werden, inwieweit aufgrund veränderter Rahmenbedingungen Anpassungsbedarf besteht. › Auch Risiken können sich verändern. Insofern müssen auch die Maßnahmen angepasst werden.	☐ Ja ☐ Nein

Das sind die typischen Hotspots fehlender Schutzmaßnahmen

Guter Datenschutz im Unternehmen hängt oft davon ab, dass die stattfindenden Verarbeitungen personenbezogener Daten sicher sind. Doch sicher ist nicht gleich sicher und viel hilft nicht automatisch viel. Ihr Unternehmen muss risikoangemessene technische und organisatorische Maßnahmen ergreifen. Vielleicht gibt es auch bei Ihnen Bereiche, wo das nicht so wirklich passt.

Schutz ist unerlässlich

Damit nichts durchs Raster fällt, sollten Sie immer wieder überlegen, wo es „unbekannte" Verarbeitungen geben könnte bzw. wo die Schutzmaßnahmen eventuell nicht passen, veraltet oder nicht mehr risikoangemessen sind. Gehen Sie in drei Schritten vor:

1. Schritt: Prüfen Sie das Verzeichnis von Verarbeitungstätigkeiten

Damit verschaffen Sie sich einen ersten Überblick. Schauen Sie, wo viele personenbezogene Daten verarbeitet werden oder wo sensible Informationen im Spiel sind. Dabei sollten Sie sich nicht allein darauf verlassen, was Sie an Einträgen vorfinden. Eventuell fehlt so einiges.

2. Schritt: Finden Sie Bereiche mit möglichen Lücken

Machen Sie ein kleines Brainstorming und notieren Sie sich alle Einfälle zu relevanten Fragen, wie z. B.:

- Wo gibt es weiße Flecken auf meiner Datenschutzlandkarte des Unternehmens?
- Welche Bereiche arbeiten viel mit personenbezogenen Daten?
- Wo gibt es große Veränderungen, etwa bei Verarbeitungen, Personal oder Technik?
- Bei welchen Bereichen habe ich als Datenschutzbeauftragter ein ungutes Gefühl?

Außerdem können Sie die unten stehende Checkliste mit Schwerpunkten nutzen, bei denen man als Datenschutzbeauftragter im Unternehmen oft fündig werden kann.

3. Schritt: Gehen Sie risikoorientiert auf die Suche

Bei Ihrer Suche werden Sie vielleicht so manches an bislang unbekannten Verarbeitungen finden. Notieren Sie jeden Fund. Bewerten Sie dann jedoch, wo Ihre Beratung bzw. der Handlungsbedarf für das Unternehmen am dringendsten ist. Orientieren Sie sich hier an folgenden Fragen:

- **Hat die Verarbeitung Außenwirkung?**
Gemeint sind hier alle Datenverarbeitungen, die nach draußen gerichtet und die für andere sichtbar sind. So z. B. ein Onlineshop oder ein auf künstlicher Intelligenz (KI) basierter Chatbot. Der Außenbezug an sich sorgt schon allein für ein erhöhtes Risiko. Da wären nicht nur die Betroffenen, Medien und die Datenschutzaufsicht. Denken Sie vor allem auch an Cyberkriminelle, die hier einen Angriffspunkt für ihre Machenschaften haben.

- **Birgt die Verarbeitung besondere oder höhere Risiken?**
Das kann der Fall sein, wenn etwa Profile gebildet oder besondere Kategorien personenbezogener Daten (Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO)) verarbeitet werden. Kommt es hier zu einer Verletzung des Schutzes, muss Ihr Unternehmen bei entsprechendem Risiko für die Betroffenen die Aufsichtsbehörde (Art. 33 DSGVO) und ggf. auch die Betroffenen (Art. 34 DSGVO) informieren.

CHECKLISTE: Typische Fundorte für Defizite bei Schutzmaßnahmen

Schwerpunkt	Erläuterung	Geprüft?
Internet, Online	Prüfen Sie die Webseite oder den Onlineshop Ihres Unternehmens. Gerade Webseiten sind schnell neu erstellt und ggf. wissen Sie nichts davon. Schauen Sie auf typische Schwachstellen. So z. B., ob eine aktuelle Verschlüsselung zum Einsatz kommt, Passwörter nicht im Klartext gespeichert werden und die eingesetzte Software auf aktuellem Stand ist. Hinterfragen Sie auch, wie man mit Zahlungsinformationen beim Onlineshop umgeht.	☐ Ja ☐ Nein
Apps	Auch hier sind angemessene Schutzmaßnahmen unerlässlich. Schauen Sie, wie man das bei Apps sicherstellt. Oft ist hier entscheidend, dass Sie die Probe aufs Exempel machen, um Unzulänglichkeiten zu entdecken.	☐ Ja ☐ Nein
KI	Werden in diesem Zusammenhang auch personenbezogene Daten verarbeitet, muss das volle Programm der DSGVO eingehalten werden. Auch die Schutzmaßnahmen müssen passen.	☐ Ja ☐ Nein
Marketing	Werbemaßnahmen können Datenschutzrisiken bergen: Prüfen Sie beispielsweise den E-Mail-Newsletter Ihres Unternehmens, und zwar von der Registrierung bis zur Abbestellung. Auch bei genutzter Software oder eingesetzten Dienstleistern muss die Sicherheit gewährleistet sein.	☐ Ja ☐ Nein
IT	Gern wird hier auf neue Technologien oder günstigere Anbieter bzw. Dienstleister gesetzt. Doch dabei darf die Sicherheit der Verarbeitung nicht auf der Strecke bleiben.	☐ Ja ☐ Nein
Personal	Hier wird viel mit personenbezogenen Daten gearbeitet und oft geht man dabei neue Wege. Denken Sie etwa an das Bewerber- und Personalmanagement, bei dem zunehmend auf moderne Systemlösungen und KI gesetzt wird.	☐ Ja ☐ Nein

KI-Beauftragter – passt das zu meiner Rolle als Datenschutzbeauftragter?

FRAGE: Ich bin Datenschutzbeauftragter in Teilzeit. Ab 2026 ist angedacht, dass ich meine Haupttätigkeit um weitere 15 % reduziere. Ich soll die Zeit aufwenden, um das für unser Unternehmen neue Thema künstliche Intelligenz (KI) zu begleiten und voranzubringen. Ich soll hier eine Art KI-Beauftragter werden, der eine ähnliche Funktion wie ein Datenschutzbeauftragter wahrnimmt. Ich frage mich in diesem Zusammenhang: Ist diese Aufgabe überhaupt mit meiner Rolle als Datenschutzbeauftragter kompatibel? Was ist in diesem Zusammenhang zu beachten?

ANTWORT: Zunächst ist es wichtig, dass Sie die Rahmenbedingungen klären. Bringen Sie in Erfahrung, was Ihrem Unternehmen hinsichtlich eines KI-Beauftragten vorschwebt. Das ist insofern von besonderer Bedeutung, weil ein KI-Beauftragter weder gesetzlich geregelt noch von der KI-Verordnung (KI-VO) gefordert ist. Die KI-VO fordert lediglich in Artikel 4 KI-Kompetenz. Das heißt, dass etwa Ihr Unternehmen diejenigen sensibilisieren und qualifizieren muss, die in seinem Auftrag mit dem Betrieb und der Nutzung von KI-Systemen befasst sind. Diese Personen müssen über ein ausreichendes Maß an KI-Kompetenz verfügen. Wie umfassend diese Kompetenz sein muss, hängt insbesondere von Art und Umfang des Einsatzes von KI ab bzw. was damit gemacht wird.

Klären Sie Rolle und Aufgaben

Natürlich ist es einem Unternehmen unbenommen, für bestimmte Themen oder Aufgaben einen Beauftragten zu benennen, um zentral eine kompetente Anlaufstelle für alle relevanten Fragen zu haben. Allerdings sollten Sie frühzeitig wissen, was es mit einer solchen Rolle auf sich hat. Je nachdem, was Ihr Unternehmen mit KI vorhat, müssen Sie adäquat ausgebildet und qualifiziert werden. Denn das ist Basis dafür, dass Sie die entsprechenden Aufgaben gut wahrnehmen können. Auch die angedachten Aufgaben sind wichtig, und zwar gerade vor dem Hintergrund Ihrer Rolle als Datenschutzbeauftragter. Sollen Sie im Bereich KI eine ähnliche Rolle wie ein Datenschutzbeauftragter wahrnehmen, dann würde auch beim Thema KI Ihr Fokus auf dem Beraten in KI-Fragen und dem Kontrollieren von relevanten Vorgaben liegen. Allerdings würden Entscheidungen zu KI anderswo getroffen werden müssen.

Achtung, Interessenkonflikt
Grundsätzlich dürfen Sie als Datenschutzbeauftragter auch andere Aufgaben wahrnehmen. Ihr Unternehmen darf Ihnen auch andere Aufgaben übertragen. Allerdings darf es mit der Wahrnehmung der anderen Aufgaben nicht zu einem Interessenkonflikt mit Ihrer Tätigkeit als Datenschutzbeauftragter kommen. Das wäre etwa dann der Fall, wenn Sie Entscheidungen über Zwecke und Mittel der Verarbeitung personenbezogener Daten übernehmen würden, sprich Aufgaben, die dem Verantwortlichen obliegen. Als Datenschutzbeauftragter müssten Sie Ihre eigenen Entscheidungen kontrollieren und bewerten, was jedoch objektiv bzw. unabhängig nicht mehr möglich sein dürfte.

Unabhängigkeit muss sichergestellt werden

Sprechen Sie mit den zuständigen Kollegen darüber, wie die Kompatibilität der Beauftragtenfunktionen sichergestellt werden kann. Das dürfte dann kein Problem sein, wenn man sich an Rolle und Funktion eines Datenschutzbeauftragten orientiert. Dieser berät und kontrolliert unabhängig. Allerdings trifft er keine Umsetzungsentscheidungen und er verantwortet auch nicht die Umsetzung. Wird das beim KI-Beauftragten ähnlich gehandhabt, sollten beide Funktionen vereinbar sein. Übrigens: Die Synergien können ein großer Vorteil sein.

Kann ein veralteter Eintrag im Verzeichnis gelöscht werden?

FRAGE: Bei uns führen wir das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 Abs. 1 Datenschutz-Grundverordnung elektronisch als Tabelle. Ich habe die Eintragungen durchgesehen. Dabei habe ich Verarbeitungstätigkeiten entdeckt, die es so nicht mehr gibt. Ich frage mich nun: Kann ein solcher Eintrag gelöscht werden, um das Verzeichnis wieder übersichtlicher zu machen?

ANTWORT: Mit dem Löschen sollten Sie vorsichtig sein. Unter Umständen hat ein solcher Eintrag noch seine Berechtigung, auch wenn die Verarbeitungstätigkeit so nicht mehr existiert. So kann ein Eintrag noch wichtig sein, wenn Daten zwar nicht mehr aktiv verarbeitet werden, jedoch etwa aufgrund von Aufbewahrungspflichten weiter vorgehalten werden müssen. Auch muss Ihr Unternehmen ggf. gegenüber der Datenschutzaufsicht auskunftsfähig sein. Verstöße können nämlich meist bis zu drei Jahre verfolgt werden. Insofern kann ein Eintrag für eine frühere Verarbeitungstätigkeit von großer Bedeutung sein. Um die Übersichtlichkeit zu erhöhen, können Sie verschiedene Maßnahmen ergreifen. Sie können die entsprechenden Verarbeitungstätigkeiten in eine Tabelle mit beendeten Verarbeitungen auslagern. Wollen Sie das nicht, können Sie bei gängigen Tabellenprogrammen die entsprechenden Bereiche ausblenden. Alternativ können Sie die Einträge auch einfach durchstreichen. Idealerweise vermerken Sie auch das Ende der Verarbeitungstätigkeit.

LAG Baden-Württemberg: Fehlende Datenschutzinfos bringen BEM zu Fall

BEM – diese Abkürzung steht für das Betriebliche Eingliederungsmanagement. Das müssen Arbeitgeber durchführen, wenn ein Arbeitnehmer innerhalb von zwölf Monaten mehr als sechs Wochen arbeitsunfähig erkrankt ist. Beim BEM spielt auch der Datenschutz eine Rolle. Und der kann eine Kündigung zu Fall bringen, wie ein Urteil des Landesarbeitsgerichts (LAG) Baden-Württemberg vom 14.1.2025 (Az. 15 Sa 22/24) zeigt.

Das führte zum Gerichtsverfahren

Ein Mann, der spätere Kläger, war seit 2014 als Transporteur bei einem Unternehmen, dem späteren Beklagten, beschäftigt. Seit Mitte 2018 war der Mann immer wieder erkrankt. Die Krankheitstage in zwölf Monaten beliefen sich jeweils auf 65 bis 121 Arbeitstage. Also wollte der Arbeitgeber des Mannes ein BEM-Verfahren durchführen.

Das BEM-Verfahren war in dem Unternehmen auch durch eine Betriebsvereinbarung geregelt. So war z. B. festgelegt, dass ein externer Dienstleister das BEM durchführt. Außerdem, dass das BEM mehrgliedrig aufgebaut ist, und zwar so, dass dem eigentlichen BEM ein Informationsgespräch vorausgeht.

Mann soll an BEM teilnehmen

Der Mann erhielt eine Einladung zum BEM. Darin wurde er über den Ablauf und das Ziel des BEM informiert. Auch wurde darauf hingewiesen, dass die Teilnahme freiwillig sei. Ferner wurde erwähnt, dass im BEM ggf. weitere Daten erhoben werden müssten. Was mit denen passieren würde, könne der Arbeitnehmer steuern. Zudem wurde über die dem Mann zustehenden Rechte nach Art. 13 ff. Datenschutz-Grundverordnung informiert. Zudem könne ihm im ersten Informationsgespräch die Datenschutzerklärung vorgelegt werden.

Der Mann erklärte sein Interesse an einem ersten Informationsgespräch und nahm hierzu als Vertrauensperson den Betriebsratsvorsitzenden mit. Das Informationsgespräch fand statt. Als Ergebnis wurde festgehalten, dass das BEM nicht gestartet werde, weil der Mann mit seinem Arbeitsplatz zufrieden wäre. Zudem könne er bei Krankheit ein BEM starten bzw. man werde ihn nach mehr als sechs Wochen erneuter Erkrankung neu einladen. Der Mann war in der Folge wiederum sieben Wochen krank. Das nahm das Unternehmen zum Anlass, dem Mann ordentlich zu kündigen.

Gegen die Kündigung zog der Mann vor das Arbeitsgericht. Dieses gab ihm recht. Die Kündigung war aus Sicht des Gerichts unwirksam. Das Unternehmen wurde verpflichtet, den Mann wie bisher zu beschäftigen. Doch das Unternehmen sah sich weiter im Recht und zog vor das LAG. Doch auch dort schloss man sich den Argumenten des Arbeitgebers nicht an.

So entschied das LAG

Die Kündigung des Arbeitsverhältnisses durch den Arbeitgeber ist unwirksam. Sie hat das Arbeitsverhältnis nicht beendet. Die Kündigung ist unverhältnismäßig, sozial ungerechtfertigt und folglich rechtsunwirksam.

Seitens des Arbeitgebers wurde nicht dargelegt, dass es keine zumutbare Möglichkeit mehr gab, durch mildere Maßnahmen eine Kündigung zu vermeiden. Musste aufgrund § 167 Abs. 2 Satz 1 Sozialgesetzbuch (SGB) IX ein BEM durchgeführt werden und ist dies nicht ordnungsgemäß erfolgt, muss der Arbeitgeber nachweisen, dass ein solches BEM nicht zu einer Verbesserung der Krankheitssituation hätte beitragen können. Ziel des BEM ist es nämlich, mildere Mittel als eine Beendigung des Arbeitsverhältnisses zu finden.

Datenschutzinformation muss sein

Generell muss ein Arbeitgeber die Initiative zum BEM ergreifen. Ob dies anzunehmen ist, hängt auch davon ab, ob der Arbeitnehmer nach § 167 Abs. 2 Satz 4 SGB IX auf die Ziele sowie Art und Umfang der Datenverarbeitung hingewiesen wurde. Das umfasst auch die Information, welche Krankheitsdaten verarbeitet und dem Arbeitgeber zugänglich gemacht werden.

BEM nicht regelkonform durchgeführt

Im vorliegenden Fall wurden schon bei der Einleitung des BEM wesentliche Fehler gemacht, sodass das BEM nicht ordnungsgemäß durchgeführt wurde. So wurden die in der Betriebsvereinbarung festgelegten Verfahrensschritte nicht eingehalten. Außerdem: Der Mann wurde nicht umfassend über die im Rahmen des BEM stattfindende Datenverarbeitung informiert. Die nötigen Informationen wurden weder in einem Infoflyer noch im Einladungsschreiben gegeben. Unter anderem ist unklar, wie sich das erwähnte BEM-Team zusammensetzt. Ferner, für welche Zwecke welche Daten dem Arbeitgeber zugänglich gemacht werden. Zudem wurde arbeitgeberseitig nicht vorgetragen, inwieweit eine entsprechende Aufklärung im Informationsgespräch vor dem eigentlichen BEM stattgefunden hat.

Das können Sie aus der Entscheidung folgern

- Beim BEM muss umfassend über die datenschutzrelevanten Aspekte informiert werden. Diese Anforderung ergibt sich ausdrücklich aus § 167 Abs. 2 Satz 4 SGB IX. Für den betreffenden Arbeitnehmer muss klar sein, was auf ihn zukommt und wer welche Daten für welchen Zweck verarbeitet oder erhält.
- Fehlt es an der nötigen Transparenz, kann das erhebliche Auswirkungen haben, denn die Durchführung des BEM ist nicht ordnungsgemäß erfolgt. Das kann dazu führen, dass eine personenbedingte Kündigung unwirksam ist.
- Vorsicht mit Betriebsvereinbarungen! Diese dürften die nötige Information des jeweiligen Mitarbeiters nicht ersetzen können.

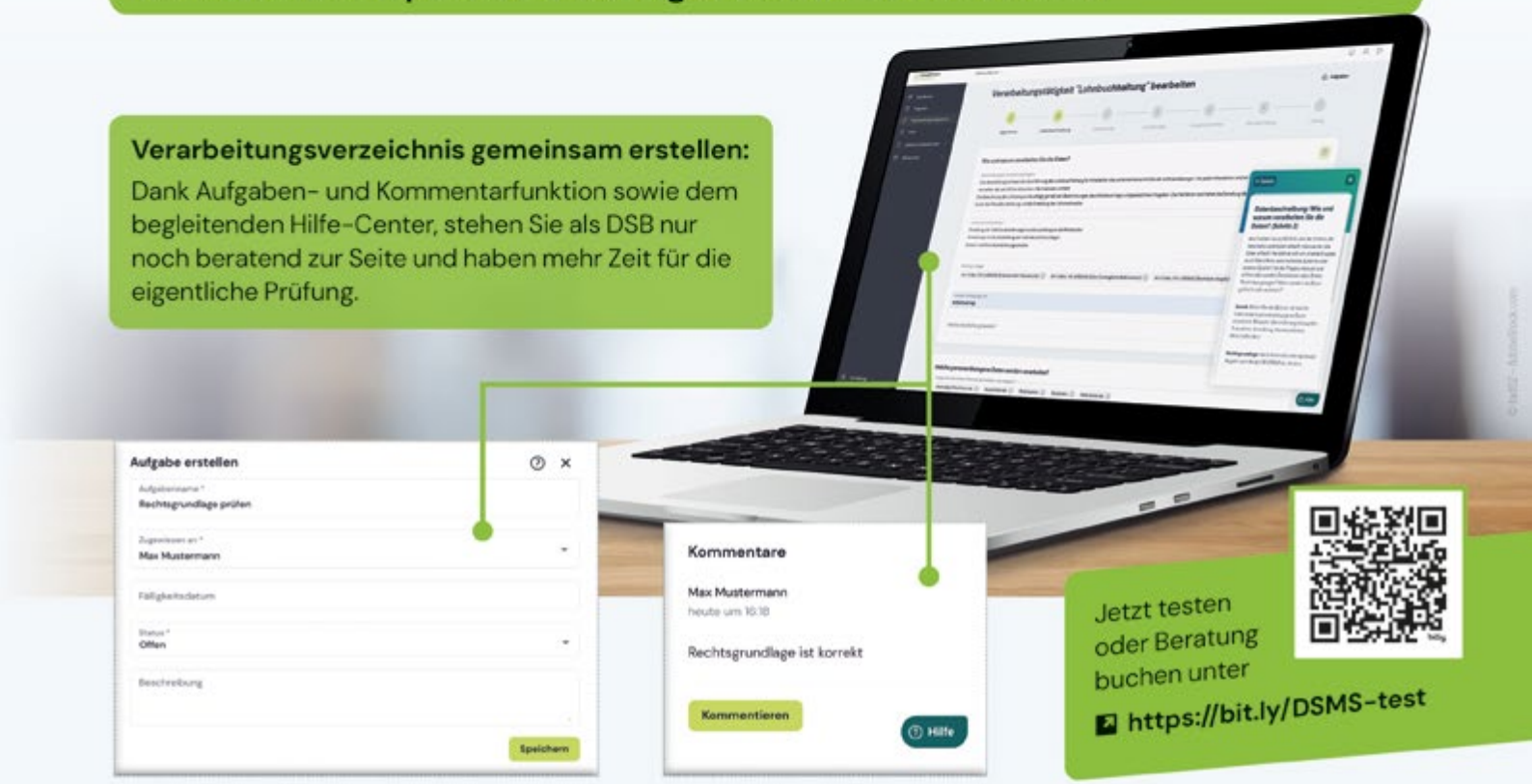
manageforwork | Datenschutz

REVOLUTION

für Ihre Datenschutzorganisation

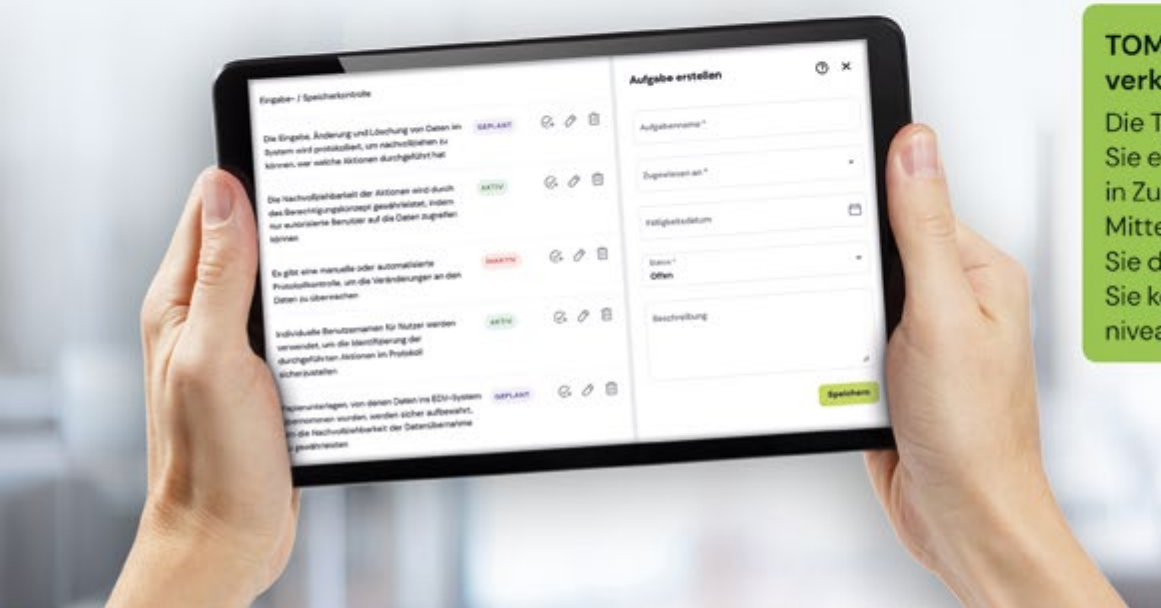
Minimieren Sie den Dokumentationsaufwand von Verarbeitungstätigkeiten und Co.: Kein Papierkram, nur Ergebnisse, mehr Sicherheit!

Verarbeitungsverzeichnis gemeinsam erstellen:
Dank Aufgaben- und Kommentarfunktion sowie dem begleitenden Hilfe-Center, stehen Sie als DSB nur noch beratend zur Seite und haben mehr Zeit für die eigentliche Prüfung.



Jetzt testen oder Beratung buchen unter
https://bit.ly/DSMS-test

1. Sie stellen einer Fachabteilung die Aufgabe zu, ihre Verarbeitungstätigkeit zu dokumentieren.
2. Verfolgen Sie den Fortschritt und reagieren auf Fragen und Unklarheiten.
3. Prüfen Sie das Risiko und definieren Sie TOMs.



TOM-Kataloge mit Audits verknüpfen:
Die TOM-Kataloge generieren Sie einfach per Vorlage oder in Zusammenarbeit mit der IT. Mittels Auditfunktion prüfen Sie die Maßnahmen. So stärken Sie kontinuierlich das Schutzniveau für Ihr Unternehmen.

PRIVACYXPERTS

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

Vorschau:

Awareness für die Personaler: Das sind Ihre Themen
Risiko Cybercrime: Zahlt die Versicherung?