DATENSCHUTZAKTUELL Professional
OKT I 2025
IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

VORSICHT, MYTHEN: ENTZAUBERN SIE DIE CYBERVERSICHERUNG IHRES UNTERNEHMENS

AWARENESS ORGANISIEREN
Interne Schulungen einkaufen? Schauen Sie genau hin 1–2

VERÄNDERUNGSPROZESSE
Weisen Sie auf diese 7 Fallstricke bei Umstrukturierungen & Co. hin 3

Das Leben ist kein Ponyhof

Liebe Leserin, lieber Leser,

die Redewendung aus der Überschrift kennen Sie bestimmt. Und sie beschränkt sich nicht nur auf das Leben an sich, sondern gilt auch für Ihre Arbeit als Datenschutzbeauftragter. Gerade die Wahrnehmung Ihrer Aufgaben steckt voller Herausforderungen und Schwierigkeiten. Auch manche Enttäuschung kann es geben.

Doch auch wenn einiges eben nicht einfach oder angenehm ist, sollten Sie immer das Positive an Ihrer Arbeit sehen. Sie bewegen viel, auch im Interesse des Unternehmens. Machen Sie sich klar, was Sie leisten, und klopfen Sie sich mal selbst auf die Schulter. Dann kann Ihnen Negatives weniger anhaben.

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

Awareness organisieren
Interne Schulungen einkaufen? Schauen Sie genau hin
Seiten 1–2

Veränderungsprozesse
Weisen Sie auf diese 7 Fallstricke bei Umstrukturierungen & Co. hin
Seite 3

Risiken erkennen
Vorsicht, Mythen: Entzaubern Sie die Cyberversicherung Ihres Unternehmens
Seiten 4–5

Beratung
Daten auf Vorrat sammeln? So erläutern Sie Ihr „Besser nicht“
Seite 6

Fragen an die Redaktion
- *Müssen die Eltern einem Azubi-Steckbrief zustimmen?*
- *In welcher Sprache müssen die Datenschutzhinweise sein?*

Seite 7

Rechtsprechung
BAG: Daten für Systemtests dürfen auch personenbezogen sein
Seite 8

Zum neuen Onlinebereich!
www.privacyxperts.de/login

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

Bildnachweise:
Titel: Adobe Stock | Falko Matte
Seite 1: Adobe Stock | kasto

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)

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.

© 2025 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau

Nutzen Sie unsere Checkliste mit den Auswahlkriterien für den richtigen Anbieter.

Interne Schulungen einkaufen? Schauen Sie genau hin

Als Datenschutzbeauftragter haben Sie viel um die Ohren. Da wären nicht nur die tagtäglichen Fragen rund um den Datenschutz. Sie sind wahrscheinlich auch Ansprechpartner Nummer eins, wenn es um das Vermitteln von Datenschutzwissen geht. Vielleicht will Ihnen die Unternehmensleitung etwas unter die Arme greifen und Sie bei Schulungen entlasten. Gute Idee, aber schauen Sie genau hin.

Sehen Sie ein solches Angebot positiv

Alles, was Sie bei Ihrer Arbeit als Datenschutzbeauftragter entlasten kann, sollten Sie nie sofort ablehnen. Schauen Sie lieber, wie Sie den größten Nutzen ziehen können. Ein Beispiel: Sie können ein Training so ausrichten, dass die von einem externen Anbieter veranstaltete Schulung das Thema „Künstliche Intelligenz (KI) und Datenschutz“ abdeckt. Einerseits können Sie so wichtiges und aktuelles Wissen unter die Leute bringen, eben durch den externen Spezialisten. Andererseits können Sie selbst davon profitieren, falls Sie bei dem einen oder anderen Thema noch nicht sattelfest sind. Sie bekommen also Qualifikation ganz nebenbei.

Im Übrigen können eine gut abgestimmte Schulung und ein intensiver Austausch mit dem Referenten Ihre Situation als Datenschutzbeauftragter erheblich verbessern. Manchmal ist es sprichwörtlich so, dass der Prophet im eigenen Land nichts gilt. Sie können sich den Mund fusselig reden, doch erst wenn eine externe Kapazität die Dinge bestätigt, schenkt man dem Glauben.

Es gibt unzählige Anbieter, aber nicht jeder passt

Sollen Sie unterstützt werden, ist das zwar eine gute Nachricht. Doch zugleich beginnt für Sie und wahrscheinlich auch für die Personalabteilung die Suche nach einem passenden Angebot bzw. Anbieter oder Referenten. Suchen Sie mit der Suchmaschine Ihres Vertrauens nach Schulungen, finden Sie im Internet ganz schnell einige Anbieter. Und meist bieten diese an, eine Schulung speziell für Ihr Unternehmen zu konzipieren und auch im Unternehmen durchzuführen. Doch wie lässt sich bei all den Anbietern die Spreu vom Weizen trennen? Schließlich sollte Ihr Unternehmen nicht dem erstbesten Anbieter den Zuschlag geben. Setzen Sie auf die folgende Checkliste:

Keine Auftragsverarbeitung bei Schulungen
Eine Auftragsverarbeitung liegt meist nicht vor. Der Anbieter bzw. der Referent entscheidet einerseits meist selbst über Zwecke und Mittel der Verarbeitung personenbezogener Daten. Außerdem steht die Verarbeitung personenbezogener Daten nicht im Fokus der Leistung.

CHECKLISTE: Typische Auswahlkriterien bei Inhouse-Schulungen

Frage	Darauf kommt es besonders an	Geklärt?
Welche Inhalte müssen vermittelt werden und welche sind optional?	Überlegen Sie im Vorfeld, was thematisch vermittelt werden muss. Die Inhalte sollte auch Ihr Unternehmen vorgeben bzw. Schwerpunkte sollten angepasst werden können.	☐ Ja ☐ Nein
Wie setzt sich die Zielgruppe der Veranstaltung zusammen?	Prüfen Sie intensiv, wer an der Schulung teilnehmen soll. Das ist nicht nur für den Referenten wichtig. Ihr Unternehmen kann nur so beurteilen, ob das Vorgehen oder die Inhalte auch zielgruppengerecht gestaltet sind.	☐ Ja ☐ Nein

CHECKLISTE: Typische Auswahlkriterien bei Inhouse-Schulungen		
Welches Budget steht zur Verfügung?	Ohne Moos nix los. Klären Sie frühzeitig, welches Budget für die Inhouse-Schulungen zur Verfügung steht. Dabei sollten Sie umfassend über Kostenpositionen nachdenken, die das für die Schulung an sich bestehende Budget schmälern. Das sind auch Kosten für Räume oder Technik.	☐ Ja ☐ Nein
Welche Anbieter kommen in Betracht?	Prüfen Sie zunächst die Onlineangebote von speziellen Anbietern. Sprechen Sie ggf. auch mit Branchenverbänden bezüglich Empfehlungen und auch mit anderen Datenschutzbeauftragten. Vielleicht können Sie dort Erfahrungsberichte oder Empfehlungen erhalten.	☐ Ja ☐ Nein
Gibt es Referenzen für die Schulungen?	Klären Sie, inwieweit der Anbieter über Referenzen verfügt. Das können etwa andere Unternehmen sein, die zu den Kunden zählen.	☐ Ja ☐ Nein
Verfügt der Referent über nachgewiesene Fachkompetenz in den betreffenden Themen?	Eine Schulung lebt auch von der Qualifikation des Referenten. Lassen Sie sich erläutern, welche Qualifikation generell beim Referenten vorhanden ist und wie es bei für Ihr Unternehmen besonders relevanten Aspekten aussieht.	☐ Ja ☐ Nein
Hat der Referent einschlägige Branchenkenntnisse?	Das kann nötig sein, wenn Ihr Unternehmen in einem sehr spezifischen Bereich tätig ist. Kennt sich der Referent nicht aus, kann er nicht auf typische Aspekte eingehen.	☐ Ja ☐ Nein
Inwieweit besteht vorab die Möglichkeit, den Referenten persönlich kennenzulernen?	Bedenken Sie stets, dass die Chemie stimmen muss. Das ist nicht nur relevant für die Konzeption der Schulung. Auch muss der Referent eine gute Beziehung zu den Teilnehmern aufbauen können. Lassen Sie sich nicht damit abwimmeln, dass der Referent erst nach Vertragsschluss gesucht werden kann.	☐ Ja ☐ Nein
Können Schulungsinhalte spezifisch an die Bedürfnisse des Unternehmens angepasst werden?	Die Schulung muss zu Ihrem Unternehmen und dessen Anforderungen passen. Ansonsten verpufft der Trainingseffekt. Das wäre nicht nachhaltig.	☐ Ja ☐ Nein
Welche Materialien werden den Teilnehmern zur Verfügung gestellt?	Schauen Sie sich an bzw. besprechen Sie, was die Teilnehmer erhalten. Fragen Sie sich, wie gut die Unterlagen später im Alltag brauchbar sind, beispielsweise um etwas nachzuschlagen. Knappe Folien können zwar im Vortrag ausreichen. Als Hilfe nach der Schulung sind sie ohne Erläuterungen meist jedoch unbrauchbar.	☐ Ja ☐ Nein
Welche Urheberrechte bzw. Nutzungsrechte bestehen, etwa an Schulungsunterlagen?	Klären Sie, was Ihr Unternehmen mit den Unterlagen machen darf. Ist Ihr Unternehmen hier eingeschränkt, sinkt eventuell der zukünftige Nutzwert. Außerdem riskiert Ihr Unternehmen Ärger, wenn es sich nicht an die entsprechenden Vereinbarungen hält.	☐ Ja ☐ Nein
Wie soll das Wissen vermittelt werden?	Lassen Sie sich die in der Schulung eingesetzten Methoden erläutern. Ausschließlich ein Vortrag kann zu wenig sein, damit etwas bei den Teilnehmern hängen bleibt. Achten Sie hier insbesondere darauf, dass die angedachten Methoden ausgewogen und praxisnah sind. Sie müssen auch zum Bedarf und zu den Fähigkeiten der Teilnehmer passen.	☐ Ja ☐ Nein
Wie steht es um Teilnehmerzahl und Gruppengröße?	Auch das sollte angesprochen werden. Ggf. berechnet sich die Vergütung nach der Anzahl der Teilnehmer. Eine Pauschale ist hier meist besser. Zudem sollten Sie darauf achten, dass Teilnehmerzahl und Gruppengröße (z. B. zwecks Gruppenarbeit) zu Thema und Vorgehen passen.	☐ Ja ☐ Nein
Wie wird Praxisnähe hergestellt?	Haben Sie ein Auge darauf, welche Elemente hierzu eingebaut werden. Praxisnahe Beispiele sind eine Sache. Gruppenübungen oder Teamarbeit auf Basis von realen Situationen aus Ihrem Unternehmen können einen erheblich größeren Nutzen bringen.	☐ Ja ☐ Nein
Welche Kosten entstehen für die Erstellung der Schulung, von Schulungsunterlagen und pro durchgeführte Veranstaltung?	Lassen Sie sich erläutern, was kostenmäßig auf Ihr Unternehmen zukommt. Achten Sie hier insbesondere auch auf Kosten, die man zunächst nicht auf dem Radar hat. Das können Druckkosten für Unterlagen genauso sein wie Kosten für Anreise, Reisezeit, Unterkunft oder die Kosten für erforderliche Präsentationstechnik.	☐ Ja ☐ Nein
Inwieweit sind die zeitlichen Rahmenbedingungen und möglichen Termine rechtzeitig planbar?	Hier geht es darum, wie eine Schulung in den Jahresplan Ihres Unternehmens passt. Außerdem ist ein zeitlicher Vorlauf unerlässlich, um die Veranstaltung zu planen, zu organisieren und anzukündigen.	☐ Ja ☐ Nein
Welche Kosten entstehen, wenn eine Schulung verschoben werden muss?	Auch das kann passieren: Viele Teilnehmer sind krank und die Schulung ergibt an einem bestimmten Termin wenig Sinn. Dann sollte eine Schulung abgesagt und ein anderer Termin vereinbart werden können, am besten ohne weitere Kosten.	☐ Ja ☐ Nein
Wie sehen die vertraglichen Regelungen aus?	Es kann vieles besprochen werden und gut klingen. Entscheidend ist, was später im Vertrag stehen wird. Schauen Sie unbedingt mit den Kollegen über die Vereinbarung, ob das Besprochene tatsächlich enthalten ist. Zudem sollten Sie auf Kündigungsmöglichkeiten achten. Sind die Teilnehmer oder Sie unzufrieden, sollte die Sache schnell beendet werden können.	☐ Ja ☐ Nein

Weisen Sie auf diese 7 Fallstricke bei Umstrukturierungen & Co. hin

Manch ein Unternehmen wird derzeit umstrukturiert, beispielsweise um die aktuellen wirtschaftlichen Herausforderungen besser meistern zu können. Vielleicht ist das auch bei Ihrem Unternehmen der Fall. Und bei den meisten Veränderungen und Umstrukturierungen gibt es auch einen Bezug zu personenbezogenen Daten. Kein Wunder, dass es dabei so manchen Fallstrick gibt. Gut, wenn Sie frühzeitig darauf hinweisen.

Öffnen Sie die Augen

Bei Umstrukturierungen oder Veränderungen im Unternehmen haben die verantwortlichen Kollegen alles Mögliche im Kopf. Da kann es passieren, dass man das Thema Datenschutz vergisst oder dem nicht die nötige Relevanz beimisst. Dabei ist klar: Die Datenschutz-Grundverordnung (DSGVO) verzeiht keine Patzer. Schlimmstenfalls drohen viel Ärger und hohe Kosten, etwa für Bußgelder. Steuern Sie dem entgegen. Erläutern Sie beispielsweise in einem Gespräch die folgenden Fallstricke:

Fallstrick Nr. 1: Unklare Verantwortlichkeiten

Veränderungen, etwa der Neuzuschnitt von Abteilungen oder die Verlagerung von (Datenverarbeitungs-)Prozessen, können zu einer Art Verantwortungsvakuum führen. So fühlt sich der abgebende Bereich nicht mehr verantwortlich und der neue Bereich noch nicht verantwortlich. Hier sollten die Übergänge der Verantwortung vom einen zum anderen Bereich klar definiert und dokumentiert sein.

Fallstrick Nr. 2: Fehlende Rechtsgrundlage

Für jede Verarbeitung personenbezogener Daten bedarf es einer Rechtsgrundlage. Daneben muss schon bei der Erhebung der Zweck definiert sein. Sollen Daten ausgelagert werden, etwa an eine neue Tochtergesellschaft, wird das unter Umständen nicht von der bisherigen Rechtsgrundlage gedeckt sein. Insofern muss genau geprüft werden, unter welchen Umständen eine Übertragung von Prozessen und personenbezogenen Daten möglich ist, etwa auf Basis der Vorgaben von Art. 6 Abs. 4 DSGVO.

Fallstrick Nr. 3: Verletzung von Betriebsvereinbarungen

Betriebsvereinbarungen regeln oft, wie technische Einrichtungen, beispielsweise ein System, im Unternehmen eingesetzt werden dürfen. Auch wenn sie oft nicht als Rechtsgrundlage taugen, weil etwa die Anforderungen aus Art. 88 Abs. 2 DSGVO nicht umgesetzt sind, sind meist wichtige Rahmenbedingungen für die Verarbeitung personenbezogener Daten enthalten. So z. B., welche Daten für welchen Zweck verarbeitet werden dürfen, welche Auswertungen erlaubt sind oder an wen die Weitergabe von Daten möglich ist. Solche Einschränkungen spielen immer eine Rolle. Werden Rahmenbedingungen im Unternehmen verändert oder Prozesse ausgelagert, kann es schnell zum Verstoß gegen eine Betriebsvereinbarung kommen. Schlimmstenfalls kann dann der Betriebsrat die Verarbeitung gerichtlich stoppen lassen, weil der Arbeitgeber die gemeinsame Regelung nicht umsetzt.

Fallstrick Nr. 4: Reduzierte Schutzmaßnahmen

Werden Verarbeitungen oder Prozesse verändert oder andere Stellen im oder außerhalb des Unternehmens verlagert, muss das so passieren, dass auch während dieses Veränderungsprozesses die Sicherheit der Verarbeitung und der betreffenden Daten gewährleistet bleibt (Art. 32 DSGVO). Abstriche bei den Schutzmaßnahmen können grundsätzlich nicht gemacht werden. Denkt man hierüber nach, ist eine Risikobewertung unerlässlich. Denn nur auf deren Basis kann bewertet werden, inwieweit andere oder geringere Schutzmaßnahmen risikoangemessen sind.

Fallstrick Nr. 5: Cyberkriminelle haben leichteres Spiel

Veränderungen bringen Unsicherheiten mit sich. So erhalten Beschäftigte neue Aufgaben oder neue Vorgesetzte. Auch Berichtslinien können sich ändern. Gerade in der Übergangsphase steigt das Risiko, dass Cyberkriminelle die Situation ausnutzen und etwa mit Phishing-E-Mails leichteres Spiel haben. Umso wichtiger ist, dass Beschäftigte in Sachen Veränderungen auf dem Laufenden gehalten werden. Auch das Sensibilisieren für mögliche Gefahren ist in der Übergangszeit unerlässlich.

Fallstrick Nr. 6: Vergessene Datenschutzvereinbarungen

Werden Verarbeitungen verlagert oder Dienstleister mit der Verarbeitung beauftragt, muss geklärt werden, wie sich die Situation der Beteiligten unter Datenschutzaspekten darstellt. Bestimmt Ihr Unternehmen weiterhin allein über Mittel und Zwecke, kann eine Auftragsverarbeitung im Sinne von Art. 28 DSGVO vorliegen. Eventuell besteht auch eine gemeinsame Verantwortung (Art. 26 DSGVO). Doch auch bei einer Übermittlung von Daten zwischen Verantwortlichen kann Regelungsbedarf bezüglich der betreffenden personenbezogenen Daten bestehen. Und das muss erledigt sein, bevor es in die praktische Umsetzung geht.

Fallstrick Nr. 7: Unzureichende Datenschutzorganisation

Kommt es zu Veränderungen, kann das erhebliche Folgen für die Datenschutzorganisation haben. Da wären etwa Know-how-Träger, die das Unternehmen verlassen. Eventuell passen auch Strukturen oder Regelungen nicht mehr zum zukünftigen Zuschnitt. Was außerdem gerne vergessen wird: Wird eine Tochtergesellschaft gegründet, kann für diese ein Datenschutzbeauftragter erforderlich sein. Ob Sie das übernehmen können, ist meist auch eine Frage der Kapazität. Schließlich gibt es gerade bei neuen Unternehmen vieles zu erledigen. Zugleich ist der Beratungsbedarf oft ziemlich groß und die Fälle sind eher kein Standard.

Vorsicht, Mythen: Entzaubern Sie die Cyberversicherung Ihres Unternehmens

Hat Ihr Unternehmen eine Versicherung für Cybersicherheitsvorfälle, etwa für den Fall, dass Hacker zuschlagen, Cyberkriminelle Daten klauen bzw. zwecks Lösegelderpressung verschlüsseln? Wenn dem so ist, kann diese im Fall der Fälle hilfreich sein. Doch meist wiegt man sich in falscher Sicherheit. Gut, wenn Sie auf Stolperfallen hinweisen und mit Mythen rund um Cybersecurity-versicherungen aufräumen.

Eine Versicherung ist nur eine Säule in der Gesamtstrategie

Die Angst vor Cybersecurityvorfällen ist in vielen Unternehmen groß. Klar, dass man sich mit dem Abschluss einer entsprechenden Versicherung schnell etwas wohler fühlt. Und die „Rundum-sorglos-Versprechen" aus Gesprächen mit dem Versicherungsvertreter oder aus der Werbebroschüre klingen besonders beruhigend. Doch meist ist diese Wohlfühlatmosphäre schnell verflogen, wenn Sie auf einige typische Punkte hinweisen, die oftmals nicht bedacht und auch in keinem Verkaufsgespräch thematisiert werden. So z. B.:

- Entscheidend ist der tatsächlich vereinbarte Versicherungsumfang. Der ist meist nicht so umfassend, wie der Versicherungsnehmer meint. Viele Anforderungen, Auflagen oder Beschränkungen fallen erst auf, wenn der Vertrag und die Vertragsbedingungen intensiv geprüft werden.
- Das Unternehmen muss sich dennoch anstrengen. Ihr Unternehmen kommt aus der Verantwortung für risikoangemessene Schutzmaßnahmen nicht heraus. Das betrifft den Schutz aller Systeme, Computer und Daten im Unternehmen. Passen die Schutzmaßnahmen nicht oder nimmt man es etwa mit Updates nicht so genau, freut das die Versicherung. Sie muss meist nämlich nicht zahlen. Denn der Versicherungsnehmer hat gegen seine Obliegenheitspflichten verstoßen. Auch hier lohnt der Blick in die Versicherungsbedingungen.
- Versicherungen sind keine Wohlfahrtsvereine. Ganz im Gegenteil. Wie jedes Unternehmen sind sie verpflichtet, Gewinn zu erwirtschaften. Dazu dürfen sie keine Risiken eingehen, die zu ihren Lasten gehen. Also schauen sie vor dem Vertragsschluss genau hin bzw. stellen ganz konkrete Fragen. Die sollten auch zutreffend beantwortet werden, wenn Ihr Unternehmen seinen Versicherungsschutz nicht riskieren will.

Tragen Sie zum umfassenden Risikomanagement bei

Mit einer Versicherungspolice in der Schublade meint manch ein Unternehmen, für den Fall der Fälle gut gerüstet zu sein. Doch meist wiegt man sich in falscher Sicherheit. Umso wichtiger ist, dass Sie als Datenschutzbeauftragter ein Auge darauf haben, was Ihr Unternehmen in Sachen Cybersecurity unternimmt. Teil dessen kann es sein, dass Sie zwecks Risikobewertung auch eine Versicherung unter die Lupe nehmen.

Bei einem Gespräch mit den zuständigen Kollegen können Sie auch mit typischen Mythen aufräumen. Setzen Sie auf die folgende Checkliste:

Sprechen Sie mit dem Risk-Owner
Unter Umständen gibt es in Ihrem Unternehmen jemanden, der sich um das Risikomanagement kümmert. Führen Sie am besten zunächst mit diesen Personen ein Gespräch. Klären Sie, wie man mit den Risiken durch Cyberkriminelle umgeht und inwieweit eine Versicherung besteht. Sprechen Sie an, inwieweit geprüft wurde, ob der vereinbarte Versicherungsschutz zum tatsächlichen Bedarf und zu den tatsächlichen Gegebenheiten passt. Will man hier nicht mit Ihnen reden oder meint man, dass Sie das alles nichts angehe, können Sie auf Art. 32 Datenschutz-Grundverordnung verweisen. Abhängig von den vereinbarten Leistungen kann ein Versicherungsschutz auch eine organisatorische Maßnahme sein, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Und ob hier alles risikoangemessen ist, sollen Sie gemäß Ihrem gesetzlichen Auftrag eben auch kontrollieren. Beißen Sie auf Granit, sprechen Sie mit dem Risk-Owner. Das ist derjenige, der das Risiko verantwortet. Das ist schlussendlich die Unternehmensleitung.

CHECKLISTE: Mythen bei der Cybersecurityversicherung

Mythos	Das sollten Sie dazu erläutern	Besprochen?
Die Cyberversicherung deckt alles ab.	› „Alles" ist schon mal garantiert falsch und sollte Sie stutzig machen. Hinterfragen Sie, was die Kollegen genau damit meinen. Denn Sie wissen vielleicht auch aus privater Erfahrung: Geht es im Schadensfall darum, dass eine Versicherung zahlen soll, nimmt die es mit dem Versicherungsumfang meist ganz genau. › Schauen Sie gemeinsam in den konkreten Versicherungsschutz, aber auch in die Versicherungsbedingungen. Nicht selten enthalten Sie nur so ein umfassendes Bild des tatsächlichen Versicherungsschutzes.	☐ Ja ☐ Nein
Mit der Versicherung vermeiden wir Schlimmeres.	› Das ist zwar meist nicht falsch. Doch ganz richtig ist es auch nicht. Oft sind die Folgen von Cybersecurityvorfällen nicht vorher- und absehbar. Insofern passt ggf. die Versicherung auch nicht. › Folgeschäden werden oft nicht bedacht. Das können Schadensersatzforderungen von Geschäftspartnern oder Imageschäden sein. Auch das ist meist nicht abgesichert.	☐ Ja ☐ Nein

CHECKLISTE: Mythen bei der Cybersecurityversicherung		
Die Versicherung zahlt alle Schäden in voller Höhe.	› Eine Deckung für Schäden in unbegrenzter Schadenshöhe dürfte wohl kaum eine Versicherung zusichern. Schließlich können gerade durch Cybersecurityvorfälle erhebliche Schäden drohen. › Bringen Sie auch immer die Datenschutzkomponente ins Spiel. Cybersecurityvorfälle haben meist auch Datenschutzrelevanz. Geraten Daten in falsche Hände, können Betroffene Schadensersatz fordern. Auch Bußgelder in Millionenhöhe können drohen. Nicht selten sind gerade die vom Versicherungsschutz ausgenommen.	☐ Ja ☐ Nein
Mit den Angaben im Antrag für eine Versicherung muss man es nicht so genau nehmen.	› Wer so denkt, der kann sich das Geld für eine Versicherung auch sparen. Denn das ist der Grund Nummer eins, damit eine Versicherung nicht zahlen muss. Das Risiko für die Versicherung wird meist aufgrund der Angaben des Unternehmens bewertet. Flunkert Ihr Unternehmen beispielsweise bei Sicherheitsmaßnahmen und sind diese Ursache für den Schaden, wird man genau auf die falschen Angaben abstellen und weniger bzw. nicht zahlen. Der Vertrag kann von der Versicherung ggf. wegen arglistiger Täuschung angefochten werden. Schließlich hat Ihr Unternehmen böswillig über die Risikosituation getäuscht. › Lassen Sie sich doch einmal die Angaben aus dem Antrag nennen und machen Sie einen Realitätscheck. Eventuell sehen Sie schnell, dass das sich aus dem Antrag ergebende Soll nicht zum tatsächlichen Ist passt. Dann sollte schnellstens eine Anpassung erfolgen. › Das Ausfüllen und Bestätigen von Maßnahmen sind nicht Ihre Sache als Datenschutzbeauftragter. Das muss die IT-Abteilung bzw. die Unternehmensleitung erledigen und auch verantworten.	☐ Ja ☐ Nein
Dank der Versicherung müssen wir weniger Aufwand in Sachen Sicherheit treiben.	› Versicherungen drücken in der Regel kein Auge zu, weil Ihr Unternehmen schon ein langjähriger Kunde ist oder weil man Verständnis für die Situation hat. Es stehen die nackten Fakten im Vordergrund. Was vereinbart wurde, muss umgesetzt werden, damit die Versicherung im Fall der Fälle tatsächlich leistet. › Generell darf ein Unternehmen nicht die Hände in den Schoß legen, gerade in Sachen Schutzmaßnahmen. Die müssen risikoangemessen und wirksam umgesetzt sein. Selbst fehlende Awareness bei Mitarbeitern oder unpassende Notfallpläne können die Leistungspflicht der Versicherung zu Fall bringen. › Klären Sie für einzelne Leistungen oder Anforderungen, wie man im Unternehmen damit umgeht bzw. wie man diesen nachkommt. Insofern können Regelungen oder Prozesse erforderlich sein.	☐ Ja ☐ Nein
Im Fall der Fälle sind wir auf der sicheren Seite.	› Das ist Ihr Unternehmen garantiert nicht. Die Versicherung mag zwar finanziell einspringen oder bestimmte Tätigkeiten übernehmen. Das kann jedoch einige Zeit in Anspruch nehmen, auch wenn es eigentlich ziemlich schnell gehen sollte. › Gerade bei Cybersecurityvorfällen muss Ihr Unternehmen schnell handeln. Aber auch hier ist Vorsicht geboten. Ggf. macht die Versicherung auch hierzu Vorgaben. Eventuell legt sie fest, welche externen Spezialisten beauftragt werden dürfen. Hält sich Ihr Unternehmen nicht daran, bleibt es schlimmstenfalls auf den Kosten sitzen.	☐ Ja ☐ Nein
Die Versicherung zahlt schnell und unkompliziert.	› Wer hierauf hofft, hofft wahrscheinlich vergeblich. Bevor Versicherungen zahlen, prüfen diese, ob sie zahlen müssen. Das kann auch dazu führen, dass etwa Gutachter und IT-Spezialisten eingebunden werden, die die Sicherheitsmaßnahmen Ihres Unternehmens unter die Lupe nehmen. Das kann dauern. Stellt sich heraus, dass diese nicht passen oder dass Ihr Unternehmen grob fahrlässig gebotene Maßnahmen nicht ergriffen hat, gibt es ggf. keinen Cent. › Selbst wenn die Versicherung grundsätzlich zahlt, kann dies zunächst nur eine Abschlagszahlung sein. Die reicht ggf. nicht aus, um alles Nötige zu veranlassen.	☐ Ja ☐ Nein
Schadensersatzforderungen, Bußgelder und Lösegeldzahlungen werden von der Versicherung übernommen.	› Schauen Sie mit den Kollegen in den Versicherungsvertrag und die Versicherungsbedingungen. Oft werden solche Kosten nicht übernommen, sprich, Ihr Unternehmen bleibt darauf sitzen. › Eventuell wurde von den Kollegen ein solcher Kostenpunkt nicht bedacht. Hinterfragen Sie, wie man damit umgehen will. Dabei ist klar: Die Einstellung „Es wird schon irgendwie gut gehen“ ist schon allein unter Risikoaspekten für das Unternehmen nicht akzeptabel.	☐ Ja ☐ Nein
Die Versicherungssumme ist richtig bemessen und reicht vollkommen aus.	› Lassen Sie keinen Zweifel aufkommen: Alles wird teurer. Selbst wenn die Versicherungssumme automatisch angepasst wird, kann das dennoch schnell zu einer Unterversicherung führen, wenn Kosten schneller steigen als die Versicherungssumme. › Gerade wenn das Unternehmen wächst, muss die Versicherung entsprechend nachgezogen werden. Schauen Sie sich daher an, wann die letzte Bewertung bzw. Anpassung erfolgt ist.	☐ Ja ☐ Nein
Veränderungen im Unternehmen haben keinen Einfluss auf die Versicherung.	› Auch hierbei handelt es sich um einen gravierenden Denkfehler. Mit Veränderungen im Unternehmen verändern sich auch die Risiken. Und Versicherungen versichern immer nur die bekannten und vereinbarten Risiken. Setzt Ihr Unternehmen auf neue Technik oder spart es bei der IT-Sicherheit, kann sich die Risikosituation komplett ändern. Nicht anders ist es, wenn Ihr Unternehmen einen Onlineshop aufbaut, von dem die Versicherung bislang nichts weiß. › Machen Sie Veränderungen in der letzten Zeit aus. Lassen Sie sich erklären, wie sich das auf die Sicherheitssituation im Unternehmen ausgewirkt hat. Hinterfragen Sie auch, wie man sich hier mit der Versicherung bezüglich des Versicherungsschutzes abgestimmt hat.	☐ Ja ☐ Nein

Daten auf Vorrat sammeln? So erläutern Sie Ihr „Besser nicht“

Gerade in Zeiten von künstlicher Intelligenz (KI) kommen vielleicht auch in der einen oder anderen Abteilung Ihres Unternehmens Begehrlichkeiten auf. Man könnte doch bestimmt mehr personenbezogene Daten sammeln als erforderlich oder vorhandene Daten nicht löschen bzw. für andere Zwecke nutzen. KI macht zudem vieles möglich. Schieben Sie solchen Ideen einen Riegel vor.

Machbar ist vieles, zulässig aber nicht

Einfach personenbezogene Daten ohne Rechtsgrundlage oder konkreten Zweck zu verarbeiten ist nicht machbar. Das wissen Sie als Datenschutzprofi nur zu gut. Doch mancher will das vielleicht nicht so recht glauben. Schließlich ist das Thema KI in aller Munde und es muss doch einfach möglich sein, diese neue Technologie wertbringend einzusetzen. Also müssen Sie klarmachen, warum das alles nicht so einfach geht.

Erläutern Sie, was Sache ist

Wollen Sie darstellen, dass das Speichern von Daten auf Vorrat oder für einen nicht klar umrissenen Zweck nicht zulässig ist, sollten Sie mit Feingefühl vorgehen. Schließlich müssen Sie vielleicht bei einer persönlich als gut empfundenen Idee den Stecker ziehen. Zeigen Sie also nachvollziehbar auf, wo die Knack- oder Problempunkte liegen. Für Ihr Gespräch können Sie auf die folgende Checkliste setzen:

CHECKLISTE: Knackpunkte bei „Daten auf Vorrat“

Knackpunkt	Das ist wichtig	Besprochen?
Fehlende Rechtsgrundlage	› Sollen personenbezogene Daten verarbeitet werden, bedarf es für die gesamte Dauer, sprich von Anfang bis Ende der Verarbeitung, einer Rechtsgrundlage. › Werden Daten ohne eindeutigen und konkret umrissenen Zweck auf Vorrat gespeichert, wird es mit der Rechtsgrundlage schwierig. Es lässt sich nämlich nicht die Frage nach der Erforderlichkeit der Daten und der Verarbeitung im Hinblick auf den Zweck beurteilen.	☐ Ja ☐ Nein
Verstoß gegen den Grundsatz der Zweckbindung	› Aus Art. 5 Abs. 1 Buchst. b Datenschutz-Grundverordnung (DSGVO) ergibt sich die Zweckbindung. Damit ist gemeint, dass Daten eben bloß für den bei der Erhebung festgelegten Zweck verarbeitet werden dürfen. › Nur bei Einhaltung der Voraussetzungen des Art. 6 Abs. 4 DSGVO kann eine Weiterverarbeitung für einen anderen Zweck zulässig sein. Hierfür bedarf es jedoch der Prüfung, inwieweit der neue Zweck zum ursprünglichen Zweck passt, der sogenannten Kompatibilitätsprüfung. In diesem Zusammenhang müssen beispielsweise auch die Erwartungen der Betroffenen berücksichtigt werden. Und das kann die ganze Sache zu Fall bringen, wenn man als Betroffener gerade nicht mit einer Weiterverarbeitung rechnet. › Eine Zweckänderung ist auf Basis einer entsprechenden Einwilligung immer möglich. Das scheitert dann jedoch oft an der Praktikabilität oder der geringen Einwilligungsfreudigkeit der Betroffenen.	☐ Ja ☐ Nein
Verstoß gegen das Minimalprinzip	› Auch hierbei handelt es sich um ein wichtiges Grundprinzip der DSGVO. Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein. › Werden Daten für noch nicht festgelegte oder allgemeine Zwecke verarbeitet, lässt sich dieses Prinzip praktisch nicht einhalten. › Wie bei allen Prinzipien kann ein Verstoß erheblichen Ärger verursachen bis hin zu schmerzhaftem Bußgeld.	☐ Ja ☐ Nein
Unzureichende Transparenz	› Betroffene müssen wissen und nachvollziehen können, was mit ihren personenbezogenen Daten passiert. Entsprechend machen Art. 13, 14 DSGVO umfassende Vorgaben zu den Informationspflichten. Sind allerdings Informationen zum Zweck zu allgemein oder wird überhaupt kein Zweck genannt, ist das ein Verstoß gegen die Transparenzpflicht. › Prüfen Sie Datenschutzhinweise stets dahin gehend, ob klar wird, welche Daten für welchen Zweck für welchen Zeitraum verarbeitet werden.	☐ Ja ☐ Nein
Mangelhafte Umsetzung der Betroffenenrechte	› Denken Sie hier vor allem an das Recht auf Löschung personenbezogener Daten (Art. 17 DSGVO). Selbst wenn Daten berechtigterweise verarbeitet werden, müssen sie nach einer festgelegten Zeit (z. B. gemäß gesetzlicher Aufbewahrungspflicht) gelöscht werden. Sie dann weiterhin zu verarbeiten, weil man sie „vielleicht noch brauchen könnte“, ist ein Datenschutzverstoß. › Auch das Recht auf Auskunft (Art. 15 DSGVO) kann nur unvollständig umgesetzt werden, wenn Daten auf Vorrat gespeichert werden. So kann man ggf. den Zweck, die Empfänger oder die Speicherdauer nicht benennen. Auch eine falsche Auskunft kann Ihr Unternehmen teuer zu stehen kommen.	☐ Ja ☐ Nein
Die Verhältnismäßigkeit fehlt.	› Klar ist: Jede Verarbeitung personenbezogener Daten muss verhältnismäßig sein. › Fehlt es am konkreten Zweck, lassen sich Geeignetheit, Erforderlichkeit und Angemessenheit der Verarbeitung nicht beurteilen.	☐ Ja ☐ Nein

Müssen die Eltern einem Azubi-Steckbrief zustimmen?

FRAGE: In unserem Unternehmen gab es kürzlich einen Willkommensworkshop für die neuen Azubis. Dabei kam die Idee auf, dass man doch eine Vorlage entwickeln sollte, mit der sich die Azubis in ihren Bereichen oder im Intranet vorstellen können. Enthalten sein sollen Angaben zum Ausbildungsberuf, zur Abteilung und die internen Kontaktdaten. Auf freiwilliger Basis soll der Azubi etwa ein Foto von sich, Angaben zu Hobbys oder zu einem Motto machen können. Wer muss eigentlich für das Bild bzw. die privaten Infos im Steckbrief einwilligen?

ANTWORT: Bezüglich der Bildveröffentlichung und der entsprechenden Angaben bei einem solchen „Steckbrief" dürfte in der Regel die Einwilligung des Betroffenen ausreichen und das ist in diesem Fall der Azubi selbst. Es ist nicht nötig, dass ein Erziehungsberechtigter des Azubis zustimmt. Bedenken Sie in diesem Zusammenhang Folgendes:

- Im Gegensatz zu dienstlichen Informationen gilt für das Bild und die privaten Informationen: Eine Veröffentlichung ist für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich. Es geht auch ohne. Also fehlt es an einer Rechtsgrundlage, etwa nach Art. 6 Abs. 1 Satz 1 Buchst. b Datenschutz-Grundverordnung (DSGVO). Auch lässt sich das Ganze nicht auf ein überwiegendes berechtigtes Interesse stützen (Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO). Zwar mag es ein berechtigtes Interesse sein, schnell die neuen Azubis in der Belegschaft bekannt zu machen. Allerdings dürften hier die Interessen der Betroffenen überwiegen. So z. B., das Aussehen oder Privates für sich zu behalten und gerade nicht gegenüber einer großen Gruppe zu offenbaren. Also bleibt hier eigentlich nur die Einwilligung des Betroffenen.
- Bei der Einwilligung heißt es Vorsicht: Auch bei Azubis handelt es sich um Beschäftigte. Also müssen bei der Einwilligung eines Beschäftigten die Vorgaben aus § 26 Abs. 2 Bundesdatenschutzgesetz (BDSG) neben den allgemeinen Vorgaben aus Art. 7, 8, 4 Nr. 11 DSGVO beachtet werden. Genauerer Prüfung bedarf es hier beim Aspekt der Freiwilligkeit. Es gibt hier nicht nur das ggf. problematische Abhängigkeitsverhältnis im Beschäftigungsverhältnis. Eventuell wird also zugestimmt, weil man es sich mit seinem Arbeitgeber oder Vorgesetzten nicht verscherzen will. Auch kommt hinzu, dass es sich um Azubis und damit ggf. Minderjährige handelt. Diesen muss besonders vermittelt werden, dass sie in ihrer Entscheidung vollkommen frei sind und ein Nein keinerlei Konsequenzen hat.
- Ob ein minderjähriger Azubi selbst einwilligen kann, sollten Sie vor allem an folgendem Aspekt festmachen: Verfügt der Betroffene über die nötige Einsichtsfähigkeit, um die Folgen seines Handelns und damit seiner Entscheidung bezüglich der Datenverarbeitung erkennen und einordnen zu können? Meist wird hier gelten: Ein Azubi wird im Rahmen seiner Ausbildung eine Vielzahl eigenständiger Entscheidungen treffen müssen. Schließlich soll er zum eigenständig arbeitenden Kollegen ausgebildet werden. Insofern kann davon ausgegangen werden, dass ein Azubi mit einem Alter von 15 oder 16 Jahren über die Aufnahme eines Porträtfotos und persönlicher Informationen für eine Vorstellung selbst entscheiden kann.
- Eine Einwilligung sollte so gestaltet sein, dass sie wirksam erklärt werden kann. Sie muss also umfassende Transparenz hinsichtlich aller Umstände der Datenverarbeitung geben. Sinnvoll ist auch der Hinweis, dass ein Nein, sprich keine Einwilligung bzw. das Nichtbereitstellen eines Fotos oder von privaten Informationen, keine negativen Folgen hat. Denken Sie auch an die Schriftlichkeit der Einwilligung (§ 26 Abs. 2 Satz 3 BDSG). Schon aus Dokumentations- und Nachweiszwecken sollte diese Vorgehensweise gewählt werden (Art. 7 Abs. 1 DSGVO).

In welcher Sprache müssen die Datenschutzhinweise sein?

FRAGE: Als in Deutschland ansässiges Unternehmen überarbeiten wir gerade die Datenschutzhinweise für unsere Webseite und unseren Onlineshop. In diesem Zusammenhang haben wir nun diskutiert: In welchen Sprachen müssen diese Hinweise veröffentlicht werden?

ANTWORT: Zunächst einmal brauchen Sie die Hinweise und ggf. andere relevante Erklärungen (z. B. Allgemeine Geschäftsbedingungen, Nutzungsbedingungen, Einwilligungen) in deutscher Sprache. Einerseits haben Sie wahrscheinlich deutsche Kunden. Aber auch die Datenschutzaufsichtsbehörde oder Verbraucherschutzverbände dürften es schnell beanstanden, wenn es keine deutsche Version gibt. Zudem brauchen Sie Versionen für alle diejenigen Sprachen, die von denjenigen gesprochen werden, an die sich die Webseite oder der Onlineshop richtet. Für Letzteren können Sie die betreffenden Länder meist schnell ausmachen. Schauen Sie, in welche Länder Ihr Unternehmen liefert, sprich aus welchen Ländern man in Ihrem Shop einkaufen kann. Bei der Webseite können Sie ein Auge auf die auswählbaren Sprachversionen werfen. Ggf. werden Sie die zuständige Abteilung fragen müssen. Zumindest für die Fokusländer wird man die relevanten Dokumente und Informationen in der jeweiligen Landessprache bereithalten müssen.

BAG: Daten für Systemtests dürfen auch personenbezogen sein

Plant Ihr Unternehmen, neue Software anzuschaffen, mit der personenbezogene Daten verarbeitet werden soll, liegt es auf der Hand: Diese muss getestet werden. Idealerweise werden Daten verwendet, die sich auf fiktive Personen beziehen. Doch es müssen nicht immer „Dummy-Daten" verwendet werden. Das zeigt ein Urteil des Bundesarbeitsgerichts (BAG) vom 8.5.2025, Az. 8 AZR 209/21.

Diese Sache landete vor Gericht

Ein Mann war als Programmierer in einem Unternehmen beschäftigt. Zugleich war er Betriebsratsvorsitzender. Das Unternehmen gehörte zu einem Konzern mit Muttergesellschaft in den USA. Daten zu Beschäftigten wurden in einem Personalverwaltungssystem verarbeitet. 2017 wurden Aktivitäten gestartet, konzernweit das Personal-Informationsmanagementsystem Workday einzuführen. Im April und Mai 2017 wurden vom deutschen Unternehmen Daten aus dem bisherigen Personalverwaltungssystem an die Konzernmutter übertragen, um sie in Workday einzuspielen. Enthalten waren Name und dienstliche Kontaktdaten, aber auch Gehaltsdaten, private Anschrift, Familienstand, Sozialversicherungsnummer und Steuer-ID.

Betriebsvereinbarung sieht weniger Daten vor

Im Juli wurde eine Betriebsvereinbarung zur Duldung des Testbetriebs von Workday geschlossen. Enthalten war das Verbot, die Software bereits für die Personalverwaltung zu verwenden. In einer Anlage wurden die Daten aufgeführt, die für Testzwecke aus dem bisherigen Personalsystem an Workday übertragen werden dürfen. Das waren geschäftliche Informationen, etwa Personalnummer, Name, Kontaktdaten, Eintrittsdatum oder Arbeitsort. Private Informationen fehlten.

Mann fordert 3.000 € Schadensersatz

Weil aus seiner Sicht unzulässig personenbezogene Daten für Testzwecke übermittelt wurden, klagte der Mann gegen seinen Arbeitgeber. Unter anderem machte er einen Schadensersatz von 3.000 € geltend. Das Arbeitsgericht wies die Ansprüche zurück. Also zog der Mann vor das Landesarbeitsgericht. Nachdem auch hier der Erfolg ausblieb, führte er den Rechtsstreit vor dem BAG weiter. Das stellte dem Europäischen Gerichtshof (EuGH) Fragen. Nach deren Beantwortung entschied nun das BAG in der Sache. Das Gericht sprach dem Mann immateriellen Schadensersatz wegen einer unzulässigen Datenverarbeitung zu, allerdings nur in Höhe von 200 €.

So urteilte das BAG

Für den Kläger besteht ein Anspruch auf Ersatz eines immateriellen Schadens aus Art. 82 Abs. 1 Datenschutz-Grundverordnung (DSGVO). Das Unternehmen hat gegen die Vorgaben der DSGVO verstoßen.

§ 26 BDSG greift nicht mehr

Es liegt ein Verstoß gegen die DSGVO vor, indem von der Betriebsvereinbarung nicht erfasste Daten für die Software Workday übermittelt wurden, um diese dort zu verarbeiten. Die Daten dürften nicht nach Art. 88 Abs. 1 DSGVO i. V. m. § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG) zu Testzwecken verarbeitet werden. § 26 Abs. 1 BDSG darf nicht angewendet werden. Die Öffnungsklausel des Art. 88 DSGVO erlaubt zwar spezifischere nationale Regelungen. § 26 Abs. 1 Satz 1 BDSG erfüllt aber die vom EuGH umrissenen Vorgaben für eine spezifischere Regelung nicht. Insbesondere fehlen die Schutzmaßnahmen im Sinne von Art. 88 Abs. 2 DSGVO. Dementsprechend ist § 26 Abs. 1 BDSG keine Rechtsgrundlage im Sinne von Art. 6 Abs. 3 DSGVO. Die Zulässigkeit einer Verarbeitung im Beschäftigungsverhältnis bestimmt sich also durch die DSGVO selbst.

Rechtsgrundlage nicht gegeben

Die Verwendung der Daten ist nicht auf Basis von Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO zulässig. Zwar ist eine Verarbeitung personenbezogener Daten zwecks Tests einer Software nicht generell ausgeschlossen, etwa wenn „Dummy-Daten" nicht ausreichen. Allerdings geht im konkreten Fall die Verarbeitung über das hinaus, was die Betriebsvereinbarung zulässt. Durch die Beschränkung auf bestimmte Daten ist davon auszugehen, dass nur diese Daten erforderlich waren.

Die Verarbeitung lässt sich auch nicht auf Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO stützen. Die Daten dienten nicht mehr einer Verarbeitung zur Erfüllung des Arbeitsverhältnisses. Vielmehr handelte es sich um eine Weiterverarbeitung zu einem anderen Zweck im Sinne von Art. 5 Abs. 1 Buchst. b DSGVO.

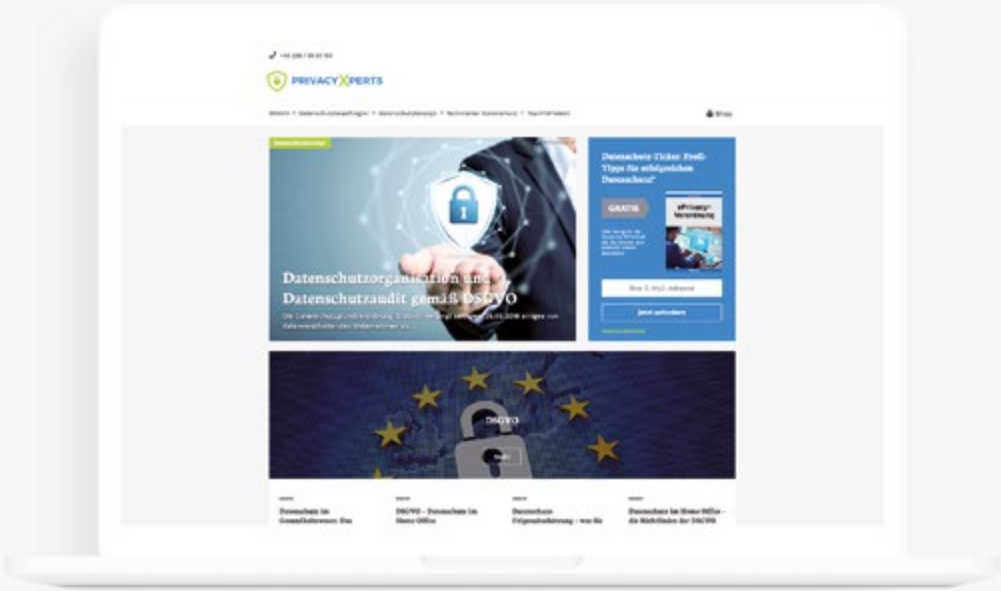
Durch den entstandenen Kontrollverlust ist von einem immateriellen Schaden auszugehen. Angemessen ist hier ein Betrag von 200 €. Relevant waren hierfür die geringe Sensibilität der Daten, der begrenzte Empfängerkreis im Konzern sowie die Dauer des Kontrollverlusts.

§

Das folgern Sie aus der Entscheidung

- Das BAG macht ausdrücklich klar: Die Anwendung von § 26 Abs. 1 Satz 1 BDSG ist für Datenverarbeitungen im Beschäftigungsverhältnis ausgeschlossen. Diese nationale Regelung ist nicht mit den Vorgaben aus Art. 88 DSGVO vereinbar. Insofern müssen sich die Rechtsgrundlagen aus der DSGVO selbst ergeben, sprich aus Art. 6 DSGVO.
- Bei Tests von Software kann es auch notwendig sein, dass personenbezogene Daten verwendet werden. Hierfür müssen eine Rechtsgrundlage und die Erforderlichkeit gegeben sein. Beschränkt eine Betriebsvereinbarung die personenbezogenen Daten, sind andere Daten für die Tests tabu.

„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

Automatisieren Sie Ihre Mitarbeiterschulung!

Jetzt Test-Account gratis aktivieren:

https://t1p.de/cyberxperts-gratis-test

Vorschau:

Notfallpläne: So können Sie prüfen
Mehr Effizienz: Diese 10 Tipps helfen

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