Spezialausgabe März 2025

PRIVACY@WORK

FÜR DATENSCHUTZBEAUFTRAGTE

World Backup Day 2025 – so schaffen Sie Awareness

PRIVACY PERTS

ANDREAS WÜRTZ – IHR EXPERTE FÜR DATENSCHUTZ
ANDREAS WÜRTZ VERFÜGT ÜBER MEHR ALS 17 JAHRE BERUFSERFAHRUNG ALS VOLLZEIT-DATENSCHÜTZER IM UNTERNEHMEN. ER ZEIGT IHNEN, WIE SICH DATENSCHUTZ PRAGMATISCH UMSETZEN LÄSST.

„Das Leben ist wie eine Schachtel Pralinen …“

Liebe Leserin, lieber Leser,

genau, „und man weiß nie, was man kriegt“. Haben Sie diese Weisheit wiedererkannt? Sie stammt von Forrest Gump aus dem gleichnamigen Film. Die Weisheit passt bestens auch aufs Arbeitsleben. Wie eine Schachtel Pralinen steckt auch Ihr Job voller Überraschungen, sowohl positive als auch negative.

Doch auch Negatives ist meist weniger schlimm, als es auf den ersten Blick erscheint. Oftmals ist es der Anfang von etwas Positivem. Daher gilt: Machen Sie es auch im Arbeitsleben wie Forrest Gump. Stehen Sie den Dingen, Ideen und Menschen offen gegenüber und ergreifen Sie sich bietende Chancen.

Viele Grüße

Andreas Würtz, Rechtsanwalt und Chefredakteur des Ratgebers „Datenschutz aktuell“

WORLD BACKUP DAY 2025: SCHAFFEN SIE AWARENESS BEI DEN FÜHRUNGSKRÄFTEN

Vielleicht kennen Sie diesen Spruch: „No Backup, no mercy“, sprich „Keine Datensicherung, kein Mitleid“. Und vielleicht haben Sie auch schon mal selbst erfahren müssen, etwa im privaten Umfeld, dass da viel Wahres dran ist. Sind Daten weg und gibt es keine Sicherung, sind Gejammer und Schaden groß. Doch dem lässt sich vorbeugen. Und das ist besonders wichtig im Unternehmen.

Nutzen Sie den World Backup Day 2025

Versäumen es Unternehmen, (über)lebenswichtige Daten immer wieder abzusichern, braucht man sich nicht zu wundern, wenn diese für immer verloren sind. Doch meist sind nicht nur einfach Daten weg. Mehr oder weniger großer Schaden entsteht insgesamt beim „Business“, wenn man es mit dem Sichern von Daten nicht so genau nimmt.

Haben Sie den Eindruck, dass man das Thema Back-up hier und da zu sehr auf die leichte Schulter nimmt, sollten Sie der mangelnden Sensibilität den Kampf ansagen. Bestens als Aufhänger geeignet ist der World Backup Day, der Internationale Tag der Datensicherung. Dieser findet, wie jedes Jahr, am 31.3.2025 statt. Nutzen Sie diesen Tag als Aufhänger für eine kurze Awarenessaktion zum Start in die Arbeitswoche. So können Sie beispielsweise

- die Führungskräfte in einer E-Mail aufklären, warum Datensicherungen so wichtig sind,
- mit einer kurzen Info-Veranstaltung Interessierten die Möglichkeiten im Unternehmen vorstellen und
- das Thema in Ihre Beratungen oder Prüfungen integrieren.

Datensicherungen sind auch ein Datenschutzthema

Auch wenn mancher meint, dass Datensicherung doch in erster Linie ein technisches Thema sein dürfte, können Sie schnell aufzeigen, dass man hier leider falschliegt. Auch personenbezogene Daten müssen gesichert werden, und zwar aus folgenden Gründen:

- Die in Art. 5 Abs. 1 Datenschutz-Grundverordnung (DSGVO) enthaltenen Grundsätze gelten für alle Verarbeitungen personenbezogener Daten. Der Grundsatz der „Integrität und Vertraulichkeit“ (Art. 5 Abs. 1 Buchst. f DSGVO) sieht vor, dass personenbezogene Daten durch geeignete technische und organisatorische Maßnahmen vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung zu schützen sind.
- Das Sichern und Verfügbarhalten von personenbezogenen Daten sind technische und organisatorische Maßnahmen, um die Sicherheit der Verarbeitung personenbezogener Daten zu gewährleisten. Bei der Frage, ob eine Maßnahme angemessenen Schutz biete, müssen auch die Verfügbarkeit und Wiederherstellbarkeit von Daten bei einem Zwischenfall berücksichtigt werden (Art. 32 Abs. 1 Buchst. b und c DSGVO).
- Gehen personenbezogene Daten verloren oder werden sie zerstört, kann das ein Datenschutzverstoß und nach Art. 33 und 34 DSGVO zu melden sein, wenn dadurch die Sicherheit oder Vertraulichkeit der Daten beeinträchtigt wird.Das kann nicht nur wegen eines Verstoßes gegen Art. 5 oder Art. 32 DSGVO zu einem Bußgeld führen. Auch können Betroffene Schadensersatzforderungen geltend machen.

Machen Sie gemeinsame Sache

Geht es um Back-ups, ist das vor allem ein Thema, bei dem die IT-Abteilung eine große Rolle spielt. Daher sollten Sie diese einbinden, wenn Sie in Sachen Back-up sensibilisieren wollen. So können Sie nicht nur gemeinsam festlegen, bei welcher Zielgruppe besonderer Handlungsbedarf besteht. Sie können auch gemeinsam die Awarenessaktion durchführen.
Wollen Sie die Führungskräfte sensibilisieren, können Sie das mehrstufig machen. Informieren Sie zunächst per E-Mail über das Thema und dessen Wichtigkeit für das Unternehmen. Dann bieten Sie kurze gemeinsame Infoveranstaltungen an, etwa virtuell. Hier können Sie etwas zum Thema Datenschutz erzählen, die Kollegen von der IT-Abteilung zur Back-up-Strategie des Unternehmens und zu einzelnen Sicherungsmaßnahmen.

Muster: Information zum Thema Back-up

Sehr geehrte Führungskräfte,

wissen Sie, welcher Tag heute ist? Ganz genau, der 31.3.2025. Und das ist nicht irgendein Tag. Es ist jedes Jahr der Internationale Tag der Daten-

sicherung, der World Backup Day. Und diesen Tag gibt es nicht ohne Grund. Er soll unter anderem dazu beitragen, dass das wichtige Thema Datensicherung in den Fokus rückt.

Auch für unser Unternehmen sind Datensicherungen auf allen Ebenen und in allen Bereichen ein wichtiges Thema. Gehen Daten verloren oder werden sie vernichtet, haben wir nicht nur einfach ein Problem, das wir lösen müssen. Dieses Problem verursacht richtig viel Arbeit und kostet vor allem viel Geld.

Deshalb: Werden Sie als Führungskraft Ihrer Verantwortung gerecht. Es gibt zahlreiche Gründe, warum Sie sich in Ihrem Verantwortungsbereich des Themas annehmen sollten. Zehn Gründe finden Sie hier:

- **Schutz vor Cyberkriminellen**
  Cyberkriminelle sind eine große Gefahr, auch für unser Unternehmen. Doch den absoluten Schutz gibt es nicht. Umso wichtiger ist, dass wir auf den Fall der Fälle vorbereitet sind. Hierfür sind auch Back-ups von Systemen, Software und Daten unerlässlich. Werden etwa Daten von Cyberkriminellen verschlüsselt, um ein Lösegeld zu erpressen, kann ein Back-up die Rettung sein und das Weiterarbeiten ermöglichen.

- **Vorsorge für Katastrophenfälle**
  Egal ob ein Hochwasser, sintflutartige Regenfälle oder ein Feuer, solche Katastrophenfälle richten in der Regel erhebliche Schäden an. Auch unser Unternehmen kann es treffen. Damit solche Katastrophen nur begrenzten Schaden anrichten, ist es auch wichtig, dass Daten immer wieder gesichert werden. Dabei ist es unerlässlich, dass man auf die richtigen Methoden setzt, etwa das Vorhalten von Sicherungen an einem anderen Ort.

- **Schutz vor Pannen und menschlichem Versagen**
  Auch Profis kann das passieren. Im Eifer des Gefechts wird ein Dateiordner, ein Datensatz oder gar eine Datenbank gelöscht. Auch bei E-Mails kann schnell gerade das gelöscht werden, was doch so dringend gebraucht wird. Passiert so etwas, ist alles weniger schlimm, wenn es Datensicherungen gibt. Zumindest ist der tatsächliche Datenverlust meist erheblich geringer.

- **Aufrechterhalten des Geschäftsbetriebs**
  Fallen Systeme aus, gehen Datenträger kaputt oder werden Daten zerstört, heißt es für den Geschäftsbetrieb im betroffenen Bereich

erst einmal stopp! und nichts geht mehr. Damit die Ausfallzeiten gering sind, sind Back-ups ein wesentliches Element. So sind sie entscheidend, um den Geschäftsbetrieb im Schadensfall aufrechtzuerhalten oder schnell wieder arbeiten zu können.

- **Geringeres Risiko für technische Pannen**
  Vielleicht hatten Sie schon einmal solch ein Erlebnis, etwa im privaten Umfeld. Sie machen ein Update einer Software, z. B. des Betriebssystems, und plötzlich funktioniert nichts mehr. Und wenn es ganz blöd läuft, kommen Sie dauerhaft nicht mehr an Ihre Daten. Weil auch im betrieblichen Umfeld bei Updates von Systemen, Datenbanken und Software immer etwas schiefgehen kann, ist es unerlässlich, vorher Back-ups durchzuführen.
- **Schutz vor Imageschäden**
  Schutzwürdige Informationen, beispielsweise Geschäftsgeheimnisse oder personenbezogene Daten, dürfen nicht verloren gehen oder in falsche Hände geraten. Passiert das nämlich, können wir das unter Umständen nicht für uns behalten. Eventuell müssen wir Geschäftspartner oder auch Kunden bzw. andere Betroffene informieren. Klar, dass das an unserem Image und an unserer Reputation einige Kratzspuren hinterlassen kann.
- **Generelle Risikovorsorge**
  Jedes Unternehmen trifft die Pflicht, Risiken für das Unternehmen auszumachen und geeignete Gegenmaßnahmen zu ergreifen. Back-ups sind ein Baustein, um den sich beispielsweise im Zusammenhang mit der IT und dem Umgang mit Daten ergebenen Risiken zu begegnen.
- **Wettbewerbsvorteil**
  Im Fall der Fälle, etwa bei einem Hochwasser, kann es passieren, dass wir und auch unserer Konkurrenz in der näheren Umgebung mit größeren Problemen zu kämpfen haben. Mit Back-ups kann es uns gelingen, unsere Geschäftstätigkeit andernorts schnell wieder hochzufahren. Das kann ein Vorteil gegenüber unserer Konkurrenz sein.
- **Anforderungen aus dem Datenschutz**
  Back-ups sind auch nötig, damit wir im Bereich Datenschutz sauber unterwegs sind. Sie dienen als technisch-organisatorische Schutz-

maßnahmen dazu, die Sicherheit von Verarbeitungen und personenbezogenen Daten zu gewährleisten. Werden personenbezogene Daten gelöscht, obwohl dies nicht zulässig wäre, kann auch das zum Datenschutzproblem werden und ein Bußgeld nach sich ziehen.

- **Entspannteres Arbeiten**
  Back-ups sind eine Art Versicherung in Sachen stressfreies Arbeiten. Geht etwas schief, können Sie mit einem Back-up schneller wieder zur Tagesordnung zurückkehren. Das entspannt Sie und Ihre Mitarbeiter, wenn unnötiger Stress und Ärger vermieden werden.

Sie haben Fragen zum Thema Back-up? Dann schreiben Sie uns doch eine E-Mail. Nutzen Sie dazu einfach das Kontaktformular im Onlinebereich unter www.privacyxperts.de. Wir freuen uns auf Ihre Nachricht.

LANGE WARTEN IST NICHT DRIN: BINDEN SIE HIER DIE LEITUNG EIN

Damit im Datenschutz keine bösen Überraschungen auftauchen, gibt es auch Sie, den Datenschutzbeauftragten. Sie haben ein Auge darauf, dass man sorgsam und regelkonform mit personenbezogenen Daten umgeht. Doch nicht immer nimmt man sich Ihren Rat zu Herzen. Das kann es erforderlich machen, dass Sie die Leitung Ihres Unternehmens in die Sache einbinden.

Haben Sie Ihre Aufgaben im Blick

Die sind schnell zusammengefasst: Art. 39 Abs. 1 Datenschutz-Grundverordnung (DSGVO) sieht vor, dass Sie das Unternehmen und die Mitarbeiter in Datenschutzfragen beraten. Außerdem kontrollieren Sie die Umsetzung der geltenden Regelungen zum Datenschutz. Teil des Beratungs- und Kontrollauftrags ist auch, dass Sie Risiken ausmachen und diese an die zuständigen Stellen adressieren. Das können beispielsweise die jeweils für eine Verarbeitung personenbezogener Daten oder für die Beschäftigten verantwortlichen Führungskräfte sein. Doch daneben sollten Sie auch die Unternehmensleitung als Adressat nicht vergessen. Der Grund: Auch diese muss auf dem Laufenden sein, was im Unternehmen vor sich geht. Schließlich ist sie es, die in letzter Konsequenz die Entscheidungen zum Datenschutz trifft. Auch ist sie als Verantwortlicher dran, wenn beim Umgang mit personenbezogenen Daten etwas schiefgeht.

Sie sind keine „Datenschutz-Petze“

Wirft man Ihnen dies vor, machen Sie klar: Das Einbinden hat nichts mit Petzen und Anschwärzen zu tun. Sie kommen lediglich Ihren Aufgaben nach und informieren, wenn das aus Ihrer Sicht unerlässlich ist. Auch das ist Teil des Risikomanagements Ihres Unternehmens.

Informieren ist hier ein Muss

Es gibt Fälle, bei denen Sie nicht wirklich lange überlegen müssen. Diese sind von solcher Bedeutung für den Datenschutz bzw. für diejenigen, die die Verantwortung tragen, dass Sie unverzüglich informieren müssen.

Die folgende Checkliste enthält typische Fälle, in denen Sie mit der Unternehmensleitung sprechen sollten:

Checklist: Unverzügliche Information der Unternehmensleitung

Situation	Erläuterungen	Leitung eingebunden? ✔
Neue Verarbeitungen mit Datenschutz-Folgenabschätzung	Bestehen trotz Einhaltung der Datenschutzanforderungen hohe Risiken, muss eine Datenschutz-Folgenabschätzung durchgeführt werden (Art. 35 DSGVO). Werden diese Risiken nicht eingedämmt, muss die Aufsichtsbehörde eingebunden werden (Art. 36 Abs. 1 DSGVO).	○
Vorhaben mit erheblichen Datenschutzrisiken für Betroffene oder das Unternehmen	Auch wenn es keine Folgenabschätzung geben muss, können erhebliche Risiken bestehen. Die können ebenso aus Verträgen oder der Zusammenarbeit mit Dritten resultieren.	○
Verarbeitungen ohne risikoangemessene Schutzmaßnahmen	Solche Schutzmaßnahmen nach Art. 32 DSGVO müssen sein. Sind sie Ihrer Ansicht nach nicht ausreichend und will man nicht nachbessern, sollten Sie mit der Leitung sprechen.	○
Festgestellte erhebliche Datenschutzdefizite	Laufen die Dinge überhaupt nicht rund, sollten Sie die Unternehmensleitung einbinden, damit schnell alles Nötige veranlasst wird. Erhebliche Defizite dürfen kein Dauerzustand sein.	○
Gravierendes Fehlverhalten mit Datenschutzrelevanz	Wird der Datenschutz mit Füßen getreten, dürfen Sie nicht wegsehen. Gehen Ihre Hinweise ins Leere, bleibt Ihnen nur noch, die Leitung in Kenntnis zu setzen.	○
Erhebliche Datenschutzpannen	Kommt es zu Datenschutzpannen, Hackerangriffen und ähnlichen Vorfällen, dürfen Sie das nicht unter den Teppich kehren. Informieren Sie schnellstens das Management, denn durch Warten wird das Problem oder der Schaden meist noch größer.	○

Betroffenenanfragen mit Risikopotenzial	Gerade bei Auskunftsverlangen oder Löschaufforderungen kann es problematisch werden. Sehen Sie hier, dass es kritisch werden kann, sollten Sie mit der Leitung darüber sprechen.	●
Vorgänge mit Medienrelevanz oder Medienbeteiligung	Sind Vorgänge oder Vorfälle publik geworden, muss das Ihre Leitung wissen. Diese kann auch festlegen, wie damit umgegangen werden soll.	●
Rechtsprechung mit erheblicher Bedeutung	Etwa Urteile im Datenschutz können auch für Ihr Unternehmen erheblichen Einfluss auf die Geschäftstätigkeit haben.	●
Situationen mit ggf. erheblichen Folgen für Umsatz, Geschäftstätigkeit oder Image des Unternehmens	Mangelhafter Datenschutz kann sich schnell auf das „Business" auswirken. Sehen Sie hier Gefahren, informieren Sie die Unternehmensleitung.	●
Änderungen an der Datenschutzorganisation	Sollen hier Anpassungen vorgenommen werden, muss das nicht mit Ihnen oder der Leitung abgestimmt sein. Sprechen Sie das Thema an. Das gilt auch, wenn man Ihnen Aufgaben zuweisen will.	●
Beeinflussung oder Benachteiligung des Datenschutzbeauftragten	Gerade wenn man Druck auf Sie ausübt, sollten Sie das nicht einfach schlucken oder dem Druck nachgeben. Besprechen Sie das Problem mit der Leitung.	●
Aktivwerden der Datenschutzaufsicht	Meldet sich die Aufsichtsbehörde bei Ihrem Unternehmen, muss das bei der Leitung bekannt sein.	●
Einbinden der Datenschutzaufsichtsbehörde	Auch wenn man Fragen an die Aufsichtsbehörde stellen will, sollte die Unternehmensleitung Bescheid wissen. Diese entscheidet, ob es tatsächlich dazu kommt.	●

NEUE VERARBEITUNG AM START? DAS SIND IHRE 30 FRAGEN FÜR DIE ERSTBERATUNG

Jeder Datenschutzbeauftragte weiß: Vieles im Unternehmen funktioniert nur mit personenbezogenen Informationen, sei es im Hinblick auf die Kunden oder sei es im Hinblick auf die eigenen Beschäftigten. Und weil die Zeit nicht stehen bleibt, gibt es immer wieder neue Verarbeitungen. Hier ist Ihre Beratung als Datenschutzbeauftragter gefragt.

Werden Sie Ihrem Auftrag gerecht

Seit eh und je ist es Aufgabe eines Datenschutzbeauftragten, die Umsetzung der gesetzlichen und betrieblichen Anforderungen im Unternehmen zu fördern. Dazu gehört in erster Linie auch, dass Sie das Unternehmen und dessen Beschäftigte beraten. Das sieht Art. 39 Abs. 1 Buchst. a Datenschutz-Grundverordnung (DSGVO) vor. Beraten heißt dabei: Sie lassen sich die Dinge schildern, schätzen diese im Hinblick auf die datenschutzrechtlichen Rahmenbedingungen ein und geben die nötigen Hinweise. Orientiert man sich daran, ist in Sachen Datenschutz alles im grünen Bereich.

Sie sind Ermöglicher und nicht Verhinderer

Datenschutz ist wichtig – keine Frage! Doch Sie sollten Ihre Funktion nie so verstehen, dass Sie der einzige Beschützer der Daten sind und jedwede Verarbeitung personenbezogener Daten möglichst verhindern sollten. Verhindern Sie nämlich auch das, was eigentlich möglich wäre, kann das ziemlich schlecht für Ihr Unternehmen sein. Schließlich macht vielleicht die Konkurrenz das Mögliche möglich und Ihr Unternehmen hat das Nachsehen.

Also gilt: Sehen Sie sich nicht als Verhinderer, sondern als Ermöglicher. Spricht man Sie bezüglich einer neuen Verarbeitung an, können Sie zwar erläutern, warum die so nicht machbar ist. Zugleich sollten Sie jedoch Wege und Möglichkeiten aufzeigen, damit die Sache fliegt. Damit zeichnen Sie sich nicht nur als profunder Kenner der Datenschutzmaterie aus. Sie zeigen zugleich, dass Sie pragmatisch und lösungsorientiert im Interesse des Unternehmens tätig werden.

Arbeiten Sie nicht im stillen Kämmerlein

Gerade wenn es um neue Verarbeitungen geht, sollten Sie die zuständigen Kollegen frühzeitig zu einem ersten Gespräch einladen. Hier kann man Ihnen das Vorhaben präsentieren und Sie können erste Fragen zum Verständnis stellen. Zugleich können Sie erste Hinweise geben, worauf es im konkreten Fall ankommen dürfte. In einem solchen ersten Termin können Sie auch die folgende Checkliste einsetzen. Diese enthält einen Fragenkatalog, mit dem Sie alle wichtigen Punkte ansprechen können. Machen Sie sich zu den einzelnen Punkten Notizen. Sind diese länger, nutzen Sie zusätzliche Blätter und weisen Sie Ihrer Notiz die entsprechenden Nummern Ihres Fragenkatalogs zu.

Checkliste: 30 Fragen bei neuen Verarbeitungen

Nr.	Frage	Erläuterung	✔
1	Was ist konkret geplant? Was haben Sie vor?	Lassen Sie die Kollegen erläutern, welche Pläne man hat und wie weit die Planung fortgeschritten ist. Fragen Sie auch nach Konzepten, Übersichten oder Darstellungen zur beabsichtigten Umsetzung.	○
2	Wer ist für das Projekt und wer für den späteren Betrieb verantwortlich?	Das sollten Sie in Erfahrung bringen, um Ihrerseits die Ansprechpartner zu kennen, die Entscheidungen treffen können und auch die Verantwortung für den Datenschutz tragen.	○
3	Wie sieht der Zeitplan aus?	Lassen Sie sich einen Zeitplan erläutern. So können Sie besser abschätzen, wie dringend auch Ihre Beratung ist.	○
4	Werden personenbezogene Daten verarbeitet? Wenn ja, welche?	Belassen Sie es hier nicht bei allgemeinen Begriffen wie beispielsweise „Kundendaten“. Gehen Sie ins Detail und lassen Sie sich jeden Datentyp erläutern. So merken Sie meist schnell, ob bestimmte Informationen überhaupt erforderlich sind.	○
5	Um wessen personenbezogene Daten geht es?	Die Gruppe der „Betroffenen“ sollte klar beschrieben sein. Klären Sie auch, ob man sich im Bereich Verbraucher oder Geschäftskunden bewegt.	○
6	Woher stammen die personenbezogenen Daten bzw. wie werden diese erhoben?	Zwar sollten personenbezogene Daten grundsätzlich beim Betroffenen selbst erhoben werden. Das ist aber nicht zwingend. Auch die Form der Beschaffung kann für die weitere Beurteilung der Sache von erheblicher Bedeutung sein.	○
7	Für welchen Zweck werden die Daten verarbeitet?	Hinterfragen Sie das Ziel der Verarbeitung. Dies ist der Maßstab für die Prüfung der Rechtsgrundlage.	○
8	Wer soll mit den Daten arbeiten bzw. wer soll Daten erhalten?	Lassen Sie sich konkret erläutern, wer in Ihrem Unternehmen mit den Daten arbeiten soll. Auch eine Weitergabe an externe Stellen kann etwa für die Prüfung der Rechtsgrundlage wichtig sein. Diese Informationen sind zudem relevant, wenn es um Zugriffsrechte geht. Diese sollten auf das erforderliche Maß begrenzt sein.	○

Nr.	Frage	Erläuterung	✔
9	Auf welche Rechtsgrundlage wird die Verarbeitung gestützt?	Es gilt ein einfaches Prinzip: ohne Rechtsgrundlage keine Verarbeitung. Prüfen Sie mit den Kollegen, inwieweit sich die Verarbeitung auf eine Rechtsgrundlage in Art. 6 Abs. 1 DSGVO stützen lässt.	○
10	Wie wird die Verarbeitung technisch umgesetzt?	Hier sollten die Kollegen die technische Umsetzung schildern – idealerweise auf der Basis von grafischen Darstellungen. Hinterfragen Sie in diesem Zusammenhang, wie die Daten fließen und wo sie wie verarbeitet werden.	○
11	Besteht eine Verbindung ins Internet?	Ist das der Fall, besteht grundsätzlich auch das Risiko für einen Zugriff durch Cyberkriminelle. Hier sollten Sie erläutern, dass spezifische Schutzmaßnahmen nötig sind.	○
12	Welche technischen und organisatorischen Schutzmaßnahmen werden ergriffen?	Schauen Sie dazu mit den Kollegen in Art. 32 DSGVO. Machen Sie klar, dass risikoangemessene Schutzmaßnahmen unerlässlich sind. Dafür ist erforderlich, dass man zunächst Risiken ausmacht und diesen mit geeigneten Maßnahmen begegnet.	○
13	Auf welche Lösung welchen Anbieters wird gesetzt?	Lassen Sie sich diese Information geben, um beispielsweise im Internet recherchieren zu können. Auch der Blick auf die Webseite und in die Hinweise zum Datenschutz des Anbieters kann eine erste Einschätzung ermöglichen, wie dieser zum Datenschutz steht.	○
14	Wer ist intern an der Verarbeitung beteiligt?	Lassen Sie sich alle Stellen nennen. Auch hier muss in allen beteiligten Bereichen der Datenschutz passen.	○
15	Werden Dienstleister eingesetzt oder Dritte eingebunden?	Beim Betrieb oder bei der Verarbeitung können Dienstleister eingesetzt werden. Denken Sie etwa an ein Callcenter für die Kundenhotline. Hier müssen ggf. die Rahmenbedingungen aus Art. 28 DSGVO (Auftragsverarbeitung) oder nach Art. 26 DSGVO (gemeinsame Verantwortung) beachtet werden.	○
16	Wo sind Anbieter, Dienstleister oder Dritte ansässig?	Denken Sie hier an das Thema Drittstaatentransfer. Für Beteiligte in Drittstaaten muss Kapitel V der DSGVO umgesetzt werden.	○

Nr.	Frage	Erläuterung	✔
17	Gibt es Vorgaben zum Datenschutz?	Auch Dienstleister oder Anbieter können Vorgaben machen, etwa zu Informationspflichten.	○
18	Wird den Anforderungen an „Data Protection by Design and Default“ entsprochen?	Schauen Sie sich mit den Kollegen Art. 25 DSGVO an. Datenschutz muss schon bei der Konzeption von Verarbeitungen sowie bei Voreinstellungen für den Nutzer berücksichtigt werden.	○
19	Werden die Grundsätze der Verarbeitung personenbezogener Daten umgesetzt?	Die Anforderungen aus Art. 5 DSGVO sind immer gesetzt und müssen eingehalten werden. Auch hier sollten Sie mit den Kollegen den Wortlaut der Vorschrift durchgehen.	○
20	Wie wird die erforderliche Transparenz geschaffen?	Wie Transparenz zu schaffen ist, ergibt sich aus Art. 12 ff. DSGVO. Hinterfragen Sie, wie man die nötigen Informationen, etwa aus Art. 13 DSGVO, bei der Erhebung der Daten geben will.	○
21	Wie kann den Rechten der Betroffenen entsprochen werden?	Lassen Sie sich vor allem angedachte Prozesse und die technische Umsetzung erläutern, wenn etwa jemand Auskunft verlangt.	○
22	Wann werden personenbezogene Daten gelöscht?	Generell sollten vorab bereits Löschfristen festgelegt sein. Außerdem muss die technische Umsetzung der Löschung bedacht werden.	○
23	Wie wird ein sicherer Betrieb der Verarbeitung sichergestellt?	Die Gewährleistung der Sicherheit ist keine einmalige, sondern eine fortlaufende Aufgabe. Sprechen Sie an, wie eine Prüfung stattfindet und wie mit Anpassungsbedarf umgegangen wird.	○
24	Werden Daten aus Altsystemen übernommen?	Manchmal wird mit einer neuen eine alte Verarbeitung abgelöst. Bei der Übernahme von Daten darf es nicht zu Fehlern kommen.	○
25	Was passiert mit dem Altsystem bzw. den enthaltenen Daten?	Auch dazu muss man sich Gedanken machen. Soll das Altsystem abgeschaltet oder entsorgt werden, sollten Sie das Thema Datenlöschung ansprechen.	○
26	Ist der Betriebsrat informiert bzw. involviert?	Die Information ist meist nötig, damit der Betriebsrat prüfen kann, ob ein Mitbestimmungsrecht besteht.	○

Nr.	Frage	Erläuterung	✔
27	Besteht ein Mitbestimmungsrecht?	Das kann der Fall sein, wenn mit der Verarbeitung eine Leistungs- oder Verhaltenskontrolle der Arbeitnehmer möglich ist (§ 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz). Die zu schließende Betriebsvereinbarung kann die Verarbeitung erheblich beeinflussen.	○
28	Gibt es sonstige Festlegungen mit dem Betriebsrat?	Diese können für das Projekt bzw. für eine Erprobungsphase bestehen, gerade wenn es noch keine Betriebsvereinbarung gibt.	○
29	Ist eine Datenschutz-Folgenabschätzung erforderlich?	Bestehen bei Berücksichtigung aller Vorgaben und Maßnahmen zum Datenschutz hohe Risiken für die Rechte und Freiheiten natürlicher Personen, muss eine Folgenabschätzung gemäß Art. 35 DSGVO durchgeführt werden.	○
30	Wie verbleiben wir?	Wahrscheinlich ist manches offen geblieben, was die Kollegen nun klären müssen. Vereinbaren Sie am besten gleich einen Folgetermin.	○

Impressum:

PRIVACYXPERTS

PrivacyXperts, ein Unternehmensbereich der VNR Verlag für die Deutsche Wirtschaft AG, Theodor-Heuss-Straße 2–4, D-53177 Bonn; Großkundenpostleitzahl: D-53095 Bonn; Handelsregister: HRB 8165, Registergericht: Amtsgericht Bonn, Vertreten durch den Vorstand: Richard Rentrop, ISSN: 1614 – 5674; Kontakt: Telefon: 0228 – 9 55 01 60 (Kundendienst); Telefax: 0228 — 3 69 64 80, E-Mail: kundendienst@privacyxperts.de, Internet: https://www.privacyxperts.de, Umsatzsteuer: Umsatzsteuer-Identifikationsnummer gemäß §27a Umsatzsteuergesetz: DE 812639372, V.i.S.d.P.: Michael Jodda; Theodor-Heuss-Straße 2–4; D-53177 Bonn, Herausgeber: Michael Jodda, Bonn, Autor: Andreas Würtz, Freiberg am Neckar, Produktmanagement: Lisa Greiling, Bonn, Layout & Satz: Bettina Pour-Imani, BB-Design, Birken-Honigsessen,
Bildrechte Seite 1: SMUX, Seite 7 Murrstock, S. 11 stockmotion – alle Adobe.Stock.com,
Druck: Warlich Druck Meckenheim GmbH, Meckenheim
Erscheinungsweise: 16 mal im Jahr; im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer Frauen und Männer gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird. Alle Angaben in Privacy@Work wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.
Dieses Produkt besteht aus FSC®-zertifiziertem Papier.