DATENSCHUTZAKTUELL SEP I 2026

IMMERAKTUELL › IMMERRELEVANT › IMMERPRAXISNAH

NEUE PLÄNE: WERDEN SIE BALD NICHT MEHR GEBRAUCHT?

Reden Sie Tacheles!

Liebe Leserin, lieber Leser,

Ihre Tätigkeit als Datenschutzbeauftragter ist anspruchsvoll. Dazu braucht es nicht nur umfassendes Fachwissen. Sie brauchen auch Erfahrung, und zwar nicht nur in der Anwendung des Datenschutzes an sich. Die brauchen Sie auch im Umgang mit den Kollegen, die schließlich den Datenschutz verantworten oder umsetzen müssen. Denn manchmal müssen Sie auch Standpunkte vertreten, die manchem nicht so wirklich passen.

In einer solchen Situation hilft oftmals nur eines: Beschönigen und verharmlosen Sie nichts. Lassen Sie nichts unter den Tisch fallen. Reden Sie Klartext, und zwar freundlich, aber bestimmt.

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 im Unternehmen pragmatisch umsetzen lässt.

Inhalt

Zu Ihrem Onlinebereich:
https://www.privacyxperts.de

Live-Talk:
https://t1p.de/live-talk

E-Mail-Beratung:
https://t1p.de/andreas-wuertz

Impressum

PRIVACYXPERTS

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

ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Michael Schrader, Bonn

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

Produktmanagement: Franziska Rohrbach, Bonn

Verantwortlicher Chefredakteur:
RA Andreas Würtz, Freiberg am Neckar

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

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.

Werden die deutschen Regeln zum Datenschutzbeauftragten abgeschafft?

Neue Pläne: Werden Sie bald nicht mehr gebraucht?

Die Zukunft des Datenschutzes in Deutschland ist nicht so rosig – so lässt sich zusammenfassen, was etwa Datenschutzverbände oder Datenschutzaufsichtsbehörden von der Absicht der Bundesregierung halten, den Datenschutz in Deutschland zu „entbürokratisieren". Kurzum: Die Regierung will die deutschen Regelungen zusammenstreichen, etwa zur Benennungspflicht des Datenschutzbeauftragten.

Das hat die Bundesregierung vor

Die Regierungsparteien vereinbarten beim letzten Koalitionsausschuss ein Maßnahmenpapier. Unter dem Titel „Ein Programm für Aufschwung und Beschäftigung" finden sich auch Vorhaben, um den Datenschutz in Deutschland zu reformieren, sprich insbesondere die Vorgaben im Bundesdatenschutzgesetz. Beabsichtigt und für Unternehmen besonders relevant ist Folgendes:

- Datenschutz vereinfachen: Dort, wo die Datenschutz-Grundverordnung (DSGVO) Spielräume einräumt, sollen diese konsequent genutzt werden.
- Abschaffen der Benennungspflicht: Die deutschen Vorgaben zur Benennungspflicht, etwa die 20-Personen-Grenze, sollen gestrichen werden. Es soll nur noch ein Datenschutzbeauftragter in den Fällen erforderlich sein, wie sie sich aus Art. 37 DSGVO ergeben. Mit hohen Bußgeldern soll sichergestellt werden, dass Verantwortliche ihrer Verantwortung nachkommen. Klar ist dann auch: Wird Art. 38 DSGVO gestrichen, fällt auch der Verweis auf den besonderen Kündigungsschutz nach Art. 38 Abs. 2 DSGVO weg.
- Weniger „Datenschutzbürokratie" für Vereine und kleine bzw. mittelständische Unternehmen: Hier will man auf EU-Ebene erwirken, dass solche Verantwortliche vom Anwendungsbereich der DSGVO ausgenommen werden. Das soll auch für risikoarme Verarbeitungen personenbezogener Daten gelten.
- Stärkung der Datenschutzkonferenz und Konzentration von Zuständigkeiten beim Bundesbeauftragten für den Datenschutz: Hiervon verspricht man sich, dass es zu weniger unterschiedlichen Sichtweisen der Aufsichtsbehörden kommt, was sich positiv auf die Wirtschaft auswirken soll.
- Datengesetzbuch schaffen: Damit es mehr Rechtsklarheit und eine einheitliche Auslegung der Regeln gibt, soll das Datenrecht in einem Datengesetzbuch harmonisiert werden. So sollen der Datenschutz gesichert und zugleich die Datennutzung gefördert werden.

Hier finden Sie das Maßnahmenprogramm der Regierung

Die Bundesregierung hat sich viel vorgenommen, und zwar nicht nur im Datenschutz. Auch bei Arbeitsmarkt, Steuern und Rente will man den Reformturbo zünden. Das „Programm für Aufschwung und Beschäftigung" können Sie hier abrufen: https://t1p.de/djg6a.

Diese Folgen hat eine Abschaffung der deutschen Regeln zum Datenschutzbeauftragten

Machen die Regierungsparteien ernst und wird etwa die deutsche Regelung zur Benennungspflicht eines Datenschutzbeauftragten abgeschafft, droht Folgendes:

- Manche Verantwortliche, etwa kleine und mittelständische Unternehmen, brauchen ggf. zukünftig nicht mehr verpflichtend einen Datenschutzbeauftragten.
- Entfällt die Pflicht für einen Datenschutzbeauftragten, kann eine bestehende Benennung widerrufen oder in eine freiwillige Benennung umgewandelt werden. In beiden Fällen greift jedoch der besondere Kündigungsschutz nicht mehr.

Was gilt eigentlich, wenn es keine deutsche Sonderregel mehr gibt?

Wenn Sie oder Ihr Unternehmen auf diese Frage eine einfache und eindeutige Antwort erwarten, dürften Sie in den meisten Fällen enttäuscht werden. Wie so oft bei rechtlichen Fragen gilt auch hier: Es kommt auf den Einzelfall an. Denn auch die Vorgaben aus Art. 37 DSGVO zur Benennung eines Datenschutzbeauftragten sind nicht so eindeutig, wie es auf den ersten Blick erscheint.

Grundsätzlich gibt es 3 Fälle

Ein Verantwortlicher muss einen Datenschutzbeauftragten benennen, wenn

1. die Verarbeitung personenbezogener Daten durch eine **Behörde oder öffentliche Stelle** erfolgt. Dabei können auch nicht öffentliche Stellen erfasst werden, etwa wenn sie Aufgaben von Behörden übernehmen, etwa als sogenannte Beliehene, oder
2. die **Kerntätigkeit** eines Verantwortlichen oder Auftragsverarbeiters in Datenverarbeitungsvorgängen besteht, welche eine **regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang** erfordern,
3. die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters in der **umfangreichen Verarbeitung besonderer Kategorien von Daten oder** von personenbezogenen Daten über **strafrechtliche Verurteilungen und Straftaten** besteht.

Die Kernfrage: Was ist eine Kerntätigkeit?

Das klingt an sich nach einer einfachen Frage, ist es aber nicht. Schauen Sie in Erwägungsgrund 97 Satz 2 zur DSGVO, erfahren Sie zwar, dass Bezugspunkt die Haupttätigkeiten des Verantwortlichen oder Auftragsverarbeiters sind und nicht die Verarbeitung personenbezogener Daten als Nebentätigkeit. Gerade Verarbeitungen personenbezogener Daten, die untrennbarer Bestandteil der Tätigkeit des Verantwortlichen sind, sind für die Kerntätigkeit prägend.

Nicht relevant sind jedoch Verarbeitungen, die Kern- oder Haupttätigkeiten nur unterstützen oder einem Nebenzweck dienen. Daher: Auch wenn etwa ein Personalmanagementsystem oder eine Kundenverwaltung große Bedeutung haben, machen sie nicht den Kern der Tätigkeit aus.

Dass der Teufel im Detail stecken kann, zeigt dieses Beispiel: Ein Krankenhaus braucht einen Datenschutzbeauftragten, weil das Behandeln ohne das umfangreiche Verarbeiten besonderer Kategorien von Daten, also Gesundheitsdaten, nicht möglich ist. Ein Arzt braucht ihn unter Umständen nicht, weil seine Verarbeitung von Gesundheitsdaten nicht als umfangreich einzustufen ist.

Was gilt eigentlich bei einer freiwilligen Benennung?

Die DSGVO kennt auch die freiwillige Benennung eines Datenschutzbeauftragten (Art. 37 Abs. 4 Satz 1 DSGVO). Doch wenn ein Verantwortlicher freiwillig jemanden zum Datenschutzbeauftragten macht, kann man nicht einfach die Rahmenbedingungen setzen, wie man will. Gerade die Aufsichtsbehörden sind der Ansicht, dass auf freiwillig benannte Datenschutzbeauftragte die Artikel 37 bis 39 anzuwenden sind. Es gelten also die gleichen Rahmenbedingungen zu Stellung, Rolle und Aufgaben wie beim verpflichtend zu benennenden Datenschutzbeauftragten.

Will ein Verantwortlicher das nicht, kann er natürlich jemanden beschäftigen, der sich um den Datenschutz kümmert. Dann darf er einen Datenschützer aber nicht „Datenschutzbeauftragter" nennen. Bei „Datenschutzberater" oder „Datenschutzconsultant" dürfte es keine Verwechslungsgefahr geben.

Hier finden Sie die Sichtweise der Aufsichtsbehörden

Wollen Sie sich zu den Rahmenbedingungen der Benennungspflicht nach der DSGVO informieren? Dann können Sie die „Leitlinien in Bezug auf Datenschutzbeauftragte („DSB")" studieren. Zwar wurde dieses Arbeitspapier (Working Paper – WP) noch von der Art.-29-Arbeitsgruppe, dem Vorgängergremium des Europäischen Datenschutzausschusses (EDSA), im April 2017 verfasst. Allerdings hat der EDSA die Leitlinien bestätigt. Das WP 243 rev. 01 finden Sie hier: https://t1p.de/0dfdz.

Bereiten Sie sich auf alle Eventualitäten vor

Bislang ist es nur eine Planung der Bundesregierung, beim Datenschutz den Rotstift anzusetzen. Ob und wenn ja, was kommt, muss sich noch zeigen. Gerade Gesetzgebungsverfahren sorgen immer wieder für Überraschungen. Auch andere Prioritäten einer Regierung oder Neuwahlen können Gesetzgebungsvorhaben stoppen oder in eine ganz andere Richtung lenken.

Dennoch sollten Sie sich frühzeitig mit Ihrer Situation und derjenigen Ihres Unternehmens auseinandersetzen. So ist vielleicht auch nach der DSGVO ein Datenschutzbeauftragter erforderlich. Ist dem nicht so, ist Ihr Unternehmen gut beraten, auf Sie als freiwilligen Datenschutzbeauftragten zu setzen. Schließlich braucht es jemanden mit Know-how und Erfahrung, damit es mit dem Datenschutz im Unternehmen klappt.

Zur Einordnung gehen Sie folgendermaßen vor:

- Prüfen Sie, ob es eine generelle Pflicht gibt, etwa als Behörde. Dann ist immer ein Datenschutzbeauftragter erforderlich. Auch private Stellen, die öffentliche bzw. hoheitliche Aufgaben übernehmen, können verpflichtet sein.
- Klären Sie, worin die Kerntätigkeit des Verantwortlichen besteht. Ist Teil dessen ein systematisches Überwachen von Betroffenen oder das umfangreiche Verarbeiten besonderer Kategorien personenbezogener Daten, bedarf es eines Datenschutzbeauftragten.
- Prüfen Sie die Detailfragen. Nicht jede Verarbeitung ist prägend für die Kerntätigkeit. Eine Videoüberwachung im Unternehmen ist eher Nebentätigkeit. Bei einem Sicherheitsdienst kann sie Kerntätigkeit sein.
- Dokumentieren Sie Ihre Einschätzung. Halten Sie fest, welche Argumente für welche Einschätzung sprechen. Damit haben Sie auch eine gute Grundlage für ein Gespräch mit der Unternehmensleitung.

Zeiterfassung: Machen Sie diesen Schnellcheck

Entbürokratisierung ist derzeit das Ziel vieler Politiker, und zwar auch im Bereich Arbeit. So wird schon lange diskutiert, ob der Acht-Stunden-Arbeitstag fallen soll und nur eine Wochenhöchstarbeitszeit gilt. Dabei geht eine Diskussion unter, die auch viel Relevanz in Sachen Daten(schutz) hat. Die Rede ist von der Zeiterfassung. Die müsste in Deutschland schon längst neu geregelt sein.

Neue Regeln brauchen noch ein Weilchen

Schon 2019 urteilten der Europäische Gerichtshof und darauf basierend 2022 das Bundesarbeitsgericht, dass jeder Arbeitgeber die Arbeitszeit aller Arbeitnehmer erfassen muss. Doch die Überarbeitung der gesetzlichen Vorgaben steht noch immer aus. Es gibt nur einen Referentenentwurf, der noch einen langen Weg im Gesetzgebungsverfahren vor sich hat. Daher: Bis es so weit ist, sollten Sie nicht die Hände in den Schoß legen. Werfen Sie einen Blick auf die aktuelle Zeiterfassung. Dazu können Sie diese Checkliste nutzen.

Checkliste: Datenschutzaspekte bei der Zeiterfassung

Das können Sie prüfen	Hierauf sollten Sie achten	In Ordnung?
Worauf zielt die Verarbeitung welcher personenbezogenen Daten ab?	› Lassen Sie sich nicht mit dem Schlagwort „Zeiterfassung" abspeisen. Meist geht es um mehr als das reine Dokumentieren der Kommen- und Gehen-Zeiten. Ziel ist oft auch die Berechnung von Lohn oder Urlaubstagen bzw. das Dokumentieren von Dienstreisen, Freistellungen oder Arbeitsunfähigkeiten. › Klären Sie, welche Daten im Spiel sind. Kommt etwa Biometrie zum Einsatz, kann die Sache anspruchsvoll werden. Dann ist eine Datenschutz-Folgenabschätzung meist ein Muss.	○ Ja ○ Nein
Welche Formen der Zeiterfassung gibt es?	› Fordern Sie einen Überblick, wie Zeiten erfasst oder eingetragen werden können. Das geht vom Terminal über App oder manuelle Eintragungen bis hin zur biometrischen Erfassung. › Sollen Verbindungsprotokolle, Aktivitätsprofile oder Anmeldedaten ausgewertet werden, sollten Sie genau hinschauen. Hier kann es schnell zu einer unzulässigen Zweckänderung kommen. › Auch klassische Stechuhren kann es noch geben. Ebenfalls ist bei nicht digitalen Verarbeitungen der Datenschutz voll anzuwenden. Das ergibt sich aus § 26 Abs. 7 Bundesdatenschutzgesetz.	○ Ja ○ Nein
Gibt es eine Rechtsgrundlage für die Verarbeitung der betreffenden Beschäftigtendaten?	› Hinterfragen Sie, worauf man die Berechtigung zur Verarbeitung stützt. › Prüfen Sie besonders die Erforderlichkeit der konkreten Verarbeitung im Hinblick auf den verfolgten Zweck.	○ Ja ○ Nein
Werden gesetzliche, tarifliche und betriebliche Vorgaben eingehalten?	› Dreh- und Angelpunkt zur Arbeitszeitdokumentation ist aktuell § 16 Abs. 2 Arbeitszeitgesetz (ArbZG). Daneben können auch Tarifverträge Festlegungen treffen. › Betriebsvereinbarungen enthalten oft datenschutzrelevante Vorgaben, etwa zu Zwecken oder Auswertungen. Dabei ist wichtig: Betriebsvereinbarungen, die nicht mit Art. 88 Abs. 2 Datenschutz-Grundverordnung (DSGVO) in Einklang stehen, taugen nicht als Rechtsgrundlage.	○ Ja ○ Nein
Werden die Grundsätze der Verarbeitung nach Art. 5 Abs. 1 DSGVO eingehalten?	› Die Grundsätze müssen bei allen Verarbeitungen personenbezogener Daten eingehalten werden. › Gehen Sie die Grundsätze durch. Schauen Sie zudem in die daraus abgeleiteten Vorschriften, etwa zur Sicherheit der Verarbeitung (Art. 32 DSGVO) oder zur Transparenz (Art. 12 ff. DSGVO).	○ Ja ○ Nein
Bestehen Vorgaben für Korrekturen oder manuelle Eintragungen?	› Werfen Sie einen Blick in die internen Vorgaben. › Bewerten Sie in diesem Zusammenhang, wie die Richtigkeit von Daten gewährleistet wird.	○ Ja ○ Nein
Sind zuständige Personen (z. B. Zeiterfassungsbeauftragte) geschult?	› Zeiterfassung kann ein sensibles Thema sein. Schon von der Zahl der Urlaubstage kann sich eine Schwerbehinderung ableiten lassen, weil Schwerbehinderte im Jahr fünf zusätzliche Urlaubstage haben. › Vertraulichkeit und Wahrung des Datenschutzes sind wichtige Aspekte. Hinterfragen Sie, wie die entsprechende Sensibilisierung durchgeführt wird.	○ Ja ○ Nein
Sind Aufbewahrung und Löschung geregelt?	› Auch Zeiterfassungsdaten unterliegen Art. 17 DSGVO. Lassen Sie sich erläutern, wann entsprechende Daten gelöscht werden. › Ein Löschen ist nicht zulässig, wenn eine Pflicht zur Aufbewahrung besteht. § 16 Abs. 2 Satz 2 ArbZG sieht mindestens zwei Jahre vor. Ggf. gibt es weitere Vorgaben in Betriebsvereinbarungen oder Tarifverträgen.	○ Ja ○ Nein
Sind externe Dienstleister korrekt eingebunden?	› Sind Tools oder Apps von Dienstleistern im Einsatz, kann eine Auftragsverarbeitung vorliegen. Die Sache muss dann den Anforderungen aus Art. 28 DSGVO genügen. › Haben Sie ein besonderes Auge auf die Sicherheitsmaßnahmen. Die müssen auch beim Dienstleister risikoangemessen sein.	○ Ja ○ Nein
Sind die Angaben im Verarbeitungsverzeichnis vollständig und aktuell?	› Mit den erhaltenen Informationen sollten Sie einen kritischen Blick ins Verzeichnis nach Art. 30 Abs. 1 DSGVO werfen. › Passt das Ist nicht zum Soll, sollten die Kollegen entsprechend Hand anlegen.	○ Ja ○ Nein

Ist beim Besucherempfang alles im grünen Bereich?

Viele Unternehmen verfügen über einen Empfang. Dieser ist Anlaufstelle für Besucher und Lieferanten. Nicht selten wird dort aber auch Organisatorisches erledigt. Dabei ist klar: Ohne das Verarbeiten personenbezogener Daten funktioniert kein Empfang. Und weil es so einiges zu beachten gilt, sollten Sie Ihrem Empfang einen Besuch abstatten.

Verbinden Sie das Kontrollieren mit dem Beraten

Als Profi im Datenschutz wissen Sie: Ihr Auftrag als Datenschutzbeauftragter nach Art. 39 Abs. 1 Datenschutz-Grundverordnung (DSGVO) ist das Beraten in allen Datenschutzfragen.

Daneben sollen Sie auch die Einhaltung der Bestimmungen zum Datenschutz kontrollieren. Dabei ist es meistens von Vorteil, wenn Sie nicht gleich auf das Kontrollieren setzen und etwa ein Audit durchführen. Legen Sie den Fokus auf das Beraten. Vereinbaren Sie einen Termin mit den für den Empfang zuständigen Kollegen. Machen Sie vor Ort eine Begehung und widmen Sie sich dann gemeinsam den wichtigsten Fragen rund um den Datenschutz.

Verdeutlichen Sie die Notwendigkeit

Fragt Sie jemand, ob das wirklich notwendig sei, kann Ihre Antwort nur lauten: Ja! Und die guten Gründe können Sie gleich mitliefern.

Einerseits geht es darum, auch im Empfang im Einklang mit dem Datenschutz zu arbeiten, Risiken zu erkennen und Defizite rechtzeitig zu beheben.

Zugleich müssen bei jeder Verarbeitung personenbezogener Daten risikoangemessene Schutzmaßnahmen umgesetzt werden, und zwar technischer bzw. organisatorischer Natur. Hier gibt es für den Empfang keine Ausnahme.

Andererseits gilt gerade für den Empfang: Es gibt keine zweite Chance für einen guten ersten Eindruck. Geht es am Empfang im Datenschutz drunter und drüber, gibt Ihr Unternehmen bei den Ankommenden ein ziemlich schlechtes Bild ab. Und das kann vieles kaputt machen.

Hapert es schon bei einfachen Datenschutzmaßnahmen, kann das auch an der Professionalität zweifeln lassen. Und wer unprofessionell arbeitet, dem vertraut man lieber nichts an, schon gar nicht personenbezogene Daten.

Checkliste: Beratungsfragen zum Datenschutz am Empfang

Prüfpunkt	Darauf sollten Sie achten	Geprüft und in Ordnung?
Wie gestaltet sich die räumliche Situation?	› Lassen Sie sich vorab Pläne geben. So können Sie schon in der Vorbereitung mögliche Problembereiche ausmachen. › Machen Sie sich vor Ort ein Bild. Nicht selten passt das Vorgefundene nicht mehr zum eigentlich Geplanten, etwa weil es so praktischer ist. Das kann aber auch zu Datenschutzproblemen führen.	○ Ja ○ Nein
Können Unbefugte Bildschirme einsehen?	› Der Empfang nutzt in der Regel einen oder mehrere Bildschirme. Prüfen Sie, inwieweit diese so aufgestellt sind, dass eine Einsichtnahme für Unbefugte ausgeschlossen ist. › Unter Umständen sind Sichtschutzfilter für die Monitore das Mittel der Wahl. Ein Einblick von der Seite kann so ausgeschlossen werden.	○ Ja ○ Nein
Können schützenswerte Informationen an Tafeln, Pinnwänden, Theken oder Schreibtischen von Unbefugten zur Kenntnis genommen werden?	› Halten Sie Ausschau nach Aushängen, etwa zu Dienstplänen oder anderen internen bzw. schützenswerten Informationen. Diese gehen Dritte nichts an. › Ein Aushängen ist grundsätzlich nicht erforderlich. Diese können auch in einem Ordner „Organisatorisches Empfang" abgelegt werden. › Im Übrigen sollten Sie als Datenschutzbeauftragter prüfen, inwieweit vor Ort das Clean-Desk-Prinzip eingehalten wird.	○ Ja ○ Nein
Gibt es öffentliche schützenswerte Informationen?	› Das kann beispielsweise ein Empfangs- oder Willkommensbildschirm sein, auf dem Name und Firma des Besuchers sowie der besuchte Mitarbeiter zu sehen sind. Hierfür gibt es meist keine Rechtsgrundlage. Es fehlt regelmäßig an der Erforderlichkeit einer Bekanntgabe gegenüber Dritten (z. B. anderen Besuchern). › Prüfen Sie auch, inwieweit Besucher-, Teilnehmer- oder Anwesenheitslisten offen ausliegen. Erstens muss niemand wissen, wer sich zuvor eingetragen hat. Zweitens besteht für eine Bekanntgabe solcher personenbezogenen Informationen keine Rechtsgrundlage. Entsprechende Listen sind unter Verschluss zu halten. Voreintragungen sind abzudecken.	○ Ja ○ Nein
Welche Verarbeitungen personenbezogener Daten gibt es?	› Lassen Sie sich einen Überblick über stattfindende Verarbeitungen geben, etwa im Zusammenhang mit dem Management von Besuchern, Lieferanten, Handwerkern. › Denken Sie nicht nur an das Verarbeiten mit Computer & Co. Hinterfragen Sie auch manuelle Verarbeitungen, etwa das Führen von Listen oder das Beobachten über Videoüberwachungsmonitore.	○ Ja ○ Nein

Inwieweit sind alle Verarbeitungstätigkeiten im Verzeichnis von Verarbeitungstätigkeiten gelistet?	› Hier darf es keine Lücken geben. Achten Sie darauf, dass auch die Verarbeitungstätigkeiten am Empfang erfasst sind. › Prüfen Sie neben der inhaltlichen Vollständigkeit auch die Aktualität der Eintragungen. Manchmal entspricht die tatsächliche Handhabung nicht der vorgesehenen.	○ Ja ○ Nein
Wo arbeitet das Unternehmen mit externen Dienstleistern zusammen?	› Hier sind verschiedene Konstellationen denkbar, etwa beim Einsatz von Fremdservices (z. B. Sicherheitsdienst) oder von Empfangspersonal. Lassen Sie sich erläutern, wie die Zusammenarbeit aussieht. › Prüfen Sie gemeinsam, wie die Zusammenarbeit einzustufen ist. Meist ist eine Vereinbarung erforderlich, die auch datenschutzrechtliche Anforderungen abdeckt.	○ Ja ○ Nein
Ist garantiert, dass Telefonate vertraulich geführt werden?	› Vertraulichkeit ist oberstes Gebot. Am besten werden Gespräche so geführt, dass Unbefugte, etwa Besucher im Wartebereich, nicht mithören können. › Schlagen Sie vor, dass man für Vertrauliches einen geschützten Nebenraum nutzt oder auf Schützenswertes oder identifizierende Informationen verzichtet. Ggf. kann eine Anfrage auch per E-Mail gestellt bzw. beantwortet werden.	○ Ja ○ Nein
Werden Besucherwartebereiche überwacht?	› Auch das kann es geben. Schauen Sie sich den Wartebereich an. Manchmal wird hier Videoüberwachung eingesetzt, damit man vom Empfang aus alles im Blick hat. › Eine Rechtsgrundlage wird sich hier regelmäßig nicht finden, auch wenn man über die Videoüberwachung informiert. Schützenswerte Interessen von Wartenden werden ein berechtigtes Interesse Ihres Unternehmens überwiegen.	○ Ja ○ Nein
Gibt es vor Ort Transparenzinformationen?	› Am Empfang kommt es zu Verarbeitungen personenbezogener Daten. Diesbezüglich ist Art. 13 DSGVO einzuhalten. Die relevanten Informationen muss ein Betroffener zur Kenntnis nehmen können. › Prüfen Sie die Informationen hinsichtlich Vollständigkeit und Aktualität. Manchmal gibt es Neuerungen, die in den Informationen nicht nachgezogen wurden.	○ Ja ○ Nein
Bestehen für Unbefugte Zugriffsmöglichkeiten auf Ablagen, Postfächer, Drucker oder Faxgeräte?	› Machen Sie den Praxistest vor Ort. Prüfen Sie, inwieweit etwa Schränke mit Unterlagen tatsächlich verschlossen sind. › An Druckern & Co. sollte nichts Schützenswertes liegen bleiben, was Unbefugte an sich oder zur Kenntnis nehmen könnten.	○ Ja ○ Nein
Wie werden schützenswerte Dokumente, Ausweise oder Schlüssel verwahrt?	› Unter Umständen sind Schränke nicht ausreichend. So können im Einzelfall auch (Schlüssel-) Tresore notwendig sein. › Prüfen Sie auch das Positionieren von Schränken oder Tresoren. Diese sollten dort sein, wo Unbefugte nicht einfach hinkommen können.	○ Ja ○ Nein
Wie sind auf Geräten gespeicherte Daten geschützt? Welchen Diebstahlschutz gibt es für Geräte?	› Gelegenheit macht Diebe. Computer, Smartphones oder Tablets am Empfang sollten verschlüsselt sein, und zwar ohne Ausnahme. › Ggf. sind Kabelschlösser sinnvoll, um Langfingern spontanes Zulangen zu erschweren.	○ Ja ○ Nein
Wie erfolgt das Entsorgen von Unterlagen?	› Prüfen Sie die Umsetzung. Es darf nichts Schützenswertes im normalen Papiermüll landen. › Kommt ein Schredder zum Einsatz, sollten Sie auf den angemessenen Partikelschnitt achten. Eine Datenschutztonne muss abgeschlossen sein und darf nicht überquellen.	○ Ja ○ Nein
Können Unbefugte sich in unbeobachteten Momenten Zutritt verschaffen bzw. Schützenswertes entwenden oder zur Kenntnis nehmen?	› Wenn viel los ist am Empfang, darf es nicht passieren, dass sich jemand am Empfang vorbeimogelt. › Gibt es gesicherte Türen oder Drehkreuze, sollten Sie deren Funktion testen. Auch ein Mehrfachnutzen von ID-Karten sollte nicht funktionieren.	○ Ja ○ Nein
Wie werden Gepäckstücke oder Koffer verwahrt?	› Werden beispielsweise Trolleys von Besuchern aufbewahrt, sollte das in einem gesonderten gesicherten Raum mit beschränktem Zugang passieren. › Das Anbringen von Namen ist grundsätzlich nicht nötig. Nummern und Abholscheine reichen aus.	○ Ja ○ Nein
In welchen Situationen wird was als Pfand verlangt?	› Lassen Sie sich erläutern, inwieweit etwa Schlüssel oder Geräte gegen ein Pfand herausgegeben werden. › Werden Personalausweise als Pfand genutzt, sollte das schnellstens geändert werden. Das lässt sich nämlich nicht auf eine Rechtsgrundlage stützen.	○ Ja ○ Nein
Wie werden Post und Pakete verwahrt?	› Häufig werden auch Post oder Pakete über den Empfang abgewickelt. Idealerweise werden Pakete in einem verschlossenen Nebenraum aufbewahrt. › Postfächer für Mitarbeiter sollten nicht für Dritte einsehbar sein. Ein Zugriff muss ausgeschlossen werden. › Postbücher sollten sicher und für Dritte nicht einsehbar aufbewahrt werden.	○ Ja ○ Nein
Ist das Personal auf den Datenschutz verpflichtet und sensibilisiert?	› Mitarbeiter des Empfangs haben regelmäßig viel mit personenbezogenen Daten zu tun. Dementsprechend ist eine Verpflichtung obligatorisch. › Awareness ist ebenfalls ein Muss. Nur so wird der richtige Umgang mit personenbezogenen Daten organisatorisch gewährleistet. › Klären Sie, inwieweit das Personal über richtiges Verhalten bei datenschutzrelevanten Vorgängen oder Vorfällen Bescheid weiß.	○ Ja ○ Nein
Was passiert, wenn der Empfang nach Feierabend nicht mehr besetzt ist?	› Datenschutz und Datensicherheit müssen jederzeit gewährleistet sein, eben auch nach Feierabend am Empfang. › Machen Sie ggf. die Probe aufs Exempel und statten Sie dem Empfang einmal nach Feierabend einen Besuch ab, natürlich unangekündigt.	○ Ja ○ Nein

Mit diesen 5 Tipps finden Sie Verbündete im Datenschutz

Vielleicht kennen Sie das: Anscheinend sind Sie als Datenschutzbeauftragter der Einzige im Unternehmen, dem am Thema Datenschutz etwas liegt. Doch auch wenn Sie sich im Stich gelassen fühlen, ist das kein Zustand, den Sie hinnehmen und akzeptieren sollten. Im Gegenteil: Sie können viel dafür tun, damit Ihr Einzelkämpferdasein ein Ende hat.

Ändern Sie Ihr Mindset

Ihr Mindset zu Ihrer Situation, sprich Ihre innere Haltung, sollten Sie als Erstes anpassen. Sagen Sie sich nicht, dass Sie alles allein stemmen müssen. Im Gegenteil: Sie sind als Datenschutzbeauftragter nur Teil des Ganzen. Sie beraten und unterstützen bei der Umsetzung (Art. 39 Abs. 1 Datenschutz-Grundverordnung – DSGVO). Entscheiden müssen Sie nichts und erst recht nichts umsetzen. Das ist Sache des Verantwortlichen, wie sich aus Art. 24 Abs. 1 DSGVO ergibt. Daraus ergibt sich auch Ihr Hebel: Andere brauchen Sie, um ihrer Verantwortung im Datenschutz gerecht zu werden.

Verbündete finden ist kein Hexenwerk

Von nichts kommt nichts – damit Ihr Einzelkämpferdasein bald ein Ende hat, können Sie auf diese Tipps setzen:

Tipp Nr. 1: Machen Sie zunächst ein Brainstorming

Nehmen Sie sich Zeit und ein großes Blatt Papier. Überlegen Sie sich relevante Fragen, die Sie sich selbst stellen. Mit ausreichend Zeit zum Nachdenken notieren Sie sich alles, was Ihnen zum jeweiligen Aspekt einfällt. Dabei ist wichtig: Denken Sie auch an Aspekte, die Sie und Ihre Tätigkeit kritisch hinterfragen. Schauen Sie dann im nächsten Schritt, was von Ihren Einfällen besondere Relevanz hat und wie Sie die Sache angehen oder die Situation verbessern können. Impulsfragen können beispielsweise sein:

- Warum habe ich den Eindruck, Einzelkämpfer zu sein?
- Wie werde ich von anderen wahrgenommen?
- Was muss sich bzw. was muss ich ändern?
- Wer verfolgt ähnliche Ziele im Unternehmen wie ich?
- Wer kann mit bei der Erreichung meiner Zielen helfen?

Tipp Nr. 2: Kontaktieren Sie Partner

Auch hier kann ein Brainstorming sinnvoll sein. Denn unter Umständen ist Ihnen nicht klar, wer alles als Partner infrage kommt. Denn nicht alle sind auf den ersten Blick naheliegend. Typischerweise in Betracht kommen Abteilungen und Kollegen, die viel mit personenbezogenen Daten zu tun haben. So sollten Sie unbedingt die IT-Abteilung auf Ihrer Liste haben. Diese muss nämlich nicht einfach nur (personenbezogene) Daten verarbeiten. Sie hat auch ein großes Interesse an IT-Sicherheit. Die entsprechenden Maßnahmen sind auch oft im Interesse des Datenschutzes, sprich im Hinblick auf den Schutz der Verarbeitung nach Art. 32 DSGVO.

Denken Sie aber auch an andere Kontrollorgane im Unternehmen. Gibt es etwa einen Compliance Officer oder eine Unternehmensrevision, verfolgt man auch dort das gleiche Grundinteresse wie Sie: Gesetze und interne Vorschriften müssen eingehalten werden, und zwar ohne Ausnahme. Daneben kann auch die Rechtsabteilung wichtige Partner für Sie bereithalten.

Gehen Sie auf diese Stellen aktiv zu. Vereinbaren Sie Termine zum persönlichen Kennenlernen bzw. zum Austausch. In aller Regel stellt sich dann schnell heraus, wo man gemeinsame Sache machen kann. Das gilt gerade für gemeinsame Aktivitäten, etwa Prüfungen oder Awarenessmaßnahmen.

Tipp Nr. 3: Vermarkten Sie den Datenschutz positiv

Achten Sie immer darauf, dass Sie die Dinge positiv darstellen. Selbst wenn bei einer Beratung herauskommt, dass das Angedachte datenschutzrechtlich nicht zulässig ist, können Sie aufzeigen, wie man es doch noch hinbekommt. Nimmt man Sie als Möglichmacher, sprich Enabler, wahr, sind Sie ein gern gesehener Gesprächspartner und Berater im Datenschutz.

Daneben sollten Sie stets darauf achten, dass Sie den Nutzen des Datenschutzes herausstellen. Natürlich kosten Schutzmaßnahmen Geld. Doch das ist gut investiert, wenn dadurch noch größerer finanzieller Schaden vermieden wird.

Tipp Nr. 4: Bieten und nehmen Sie Hilfe an

Sie kennen die Weisheit „Eine Hand wäscht die andere"? Die sollten Sie aber nicht negativ verstehen. Vielmehr geht es um „Hilfst du mir, dann helfe ich dir". Unterstützen Sie einerseits die Kollegen im Datenschutz durch gute Tipps. Stehen Sie zudem mit Rat und Tat zur Seite. Geben Sie Hilfestellung, wo immer das möglich ist.

Doch auch außerhalb des Datenschutzes sollten Sie auf gegenseitige Hilfe setzen. Bestimmt haben Sie Know-how, was anderen im Unternehmen nutzt. Können Sie jemandem unter die Arme greifen, wird er sich revanchieren. Bietet man Ihnen Hilfe an, sollten Sie diese auch annehmen.

Tipp Nr. 5: Steigern Sie Ihren Bekanntheitswert

Unterschätzen Sie nicht, was Sympathie ausmachen und bewegen kann. Doch Sympathie baut sich nicht von selbst auf. Einerseits ist wichtig, dass Ihre Kollegen ein positives Bild von Ihnen haben. Andererseits ist unerlässlich, dass Sie den Kollegen die Chance geben, Sie kennenzulernen. Daher ist wichtig: Nehmen Sie jede Gelegenheit wahr, um mit den Kollegen ins Gespräch zu kommen. Lassen Sie nichts aus, wo man sich in lockerer Runde kennenlernen kann.

Welche Auswirkungen hat die Altersteilzeit auf meine Benennung?

FRAGE: Ich bin Datenschutzbeauftragter und nähere mich der Rente. Bei einer Betriebsversammlung war auch Thema, dass rentennahe Jahrgänge in Altersteilzeit gehen können. Ich überlege tatsächlich, ob das etwas für mich wäre. Dazu frage ich mich auch: Inwieweit hat Altersteilzeit Auswirkungen auf meine schon seit vielen Jahren bestehende Benennung zum Datenschutzbeauftragten?

ANTWORT: Bei Altersteilzeit gibt es regelmäßig unterschiedliche Modelle. Im sogenannten Blockmodell arbeiten Sie zu einem reduzierten Gehalt in der Arbeitsphase zunächst beispielsweise für zwei Jahre weiter. Danach kommt eine Freistellungsphase von zwei Jahren. Mit Ende der Freistellungsphase gehen Sie dann in Rente. Daneben kann es auch Teilzeitmodelle geben.

Betriebsrat kann Ihre erste Anlaufstelle sein

Oft gibt es tarifvertragliche oder betriebliche Besonderheiten zur Altersteilzeit. Um einen guten Überblick zu erhalten, können Sie sich vertrauensvoll an den Betriebsrat wenden. Dort gibt es meist auch einen Spezialisten, der tief im Thema steckt.

Klären Sie Ihre Rentenansprüche

Zwar werden auch in der Altersteilzeit weiter Rentenbeiträge eingezahlt. Allerdings sind diese geringer. Kommt es zudem zu einem vorzeitigen Renteneintritt, gibt es entsprechende Rentenabschläge. Je nach Umfang können die Abschläge erheblich sein. Lassen Sie sich daher vom Rentenversicherungsträger oder einer anderen unabhängigen Stelle beraten.

Sprechen Sie mit der Unternehmensleitung

Können Sie sich vorstellen, in Altersteilzeit zu gehen, sollten Sie das Gespräch mit der Unternehmensleitung und mit der Personalabteilung suchen. So kann gemeinsam auch für die Arbeitsphase einer Altersteilzeit ein Weg gefunden werden, um gut mit der neuen Situation umzugehen. Hier kann es auch attraktive Gestaltungsmöglichkeiten geben. So können Sie etwa beim Teilzeitmodell ausschließlich im Datenschutz tätig sein und eine andere Tätigkeit nicht mehr ausüben. Beim Blockmodell kann man den Übergang zu einem neuen Datenschutzbeauftragten fließend gestalten, sodass Sie viel Know-how an Ihren Nachfolger weitergeben können.

Müssen wir vertauschte Lieferscheine als Panne melden?

FRAGE: Wir haben nur Geschäftskunden. In der Logistik kam es kürzlich zu einer Panne. Es wurden in vier Pakete die falschen Lieferscheine gepackt. Auf diesen sind bei Lieferanweisungen auch personenbezogene Daten zu finden. Wir haben die Empfänger gebeten, die falsch erhaltenen Lieferscheine zu vernichten. Wir fragen uns noch: Müssen wir diese Panne nach Art. 33 Abs. 1 Datenschutz-Grundverordnung (DSGVO) melden?

ANTWORT: Drei Dinge sind im Zusammenhang mit der Meldung von Datenpannen entscheidend. Ihr Unternehmen muss

1. die Risiken bewerten, die sich aus der „Panne" für die Betroffenen ergeben: Dazu kann sich Ihr Unternehmen an Erwägungsgrund 85 zur DSGVO orientieren. Zu berücksichtigen sind etwa drohende (finanzielle) Schäden, Rufschädigung oder der Verlust der Kontrolle.
2. prüfen, welche Vorgaben die zuständige Aufsichtsbehörde macht: Schauen Sie auf die Webseite der für Ihr Unternehmen zuständigen Aufsichtsbehörde. Die Behörden geben Hinweise, wann eine Meldung erfolgen muss. Unter Umständen ist diese gerade nicht erforderlich, wenn nur ein niedriges Risiko für die Rechte und Freiheiten der Betroffenen besteht,
3. rechtzeitig mit den erforderlichen Informationen melden: Kommt Ihr Unternehmen zum Ergebnis, dass ein nicht nur niedriges Risiko besteht, muss die Meldung unverzüglich erfolgen, möglichst binnen 72 Stunden.

Risiken eher gering

Bei vernünftiger Betrachtung des Sachverhalts wird man in Ihrem Fall nicht von einem hohen Risiko ausgehen müssen. Es ging nur um eine kleine Zahl Betroffener. Die Daten waren eher unkritisch. Schäden aus der Kenntnisnahme der Daten dürften keine zu erwarten sein. Insofern dürfte eine Meldung nicht erforderlich sein, wenn die Aufsichtsbehörde diese bei niedrigen Risiken nicht fordert.

Gerichtsgutachter muss Auskunft nach DSGVO geben

Dass bei der Datenschutz-Grundverordnung (DSGVO) noch immer vieles unklar und auslegungsbedürftig ist, zeigt sich etwa am Recht auf Auskunft nach Art. 15 DSGVO. Das Oberlandesgericht (OLG) Stuttgart musste sich in diesem Zusammenhang mit der Frage auseinandersetzen, ob ein gerichtlicher Gutachter einem Kläger Auskunft über die im Zusammenhang mit der Gutachtenerstellung verarbeiteten Daten geben muss (Urteil vom 25.2.2026, Az. 4 U 342/25).

Das führte zum Rechtsstreit

Eine Frau, die spätere Klägerin, führte seit 2009 in zwei getrennten Verfahren Arzthaftungsprozesse gegen mehrere Zahnärzte. Im Rahmen der beiden Verfahren wurde vom Gericht ein Sachverständiger, der spätere Beklagte, beauftragt.

Anfang September 2024 forderte die Frau vom Gutachter Auskunft und Kopien der vom Gutachter verarbeiteten Daten. Erfasst sein sollte auch das nach Aussage des Gutachters bereits zu 90 % fertige Gutachten für eines der Gerichtsverfahren. Dieses Gerichtsverfahren wurde gegen die Klägerin entschieden, weil sie keinen weiteren Vorschuss auf die Gutachtenerstellung zahlen wollte und somit nicht den Beweis für ihre Ansprüche liefern konnte.

Gutachter erteilt keine Auskunft

Anstatt einer Auskunft leitete der Gutachter eine Stellungnahme an die Frau weiter. Diese stammte vom Gericht und führte aus, dass eine Auskunft nicht zu erteilen sei. So wäre der Gutachter selbst nicht datenschutzrechtlich verantwortlich. Zudem würde gegen Beweisregeln der Zivilprozessordnung (ZPO) verstoßen. Auch wäre ein Verstoß gegen das Urheberrecht gegeben.

Die Frau wollte das nicht akzeptieren und klagte auf Auskunft. Vor dem Landgericht hatte sie keinen Erfolg. Also zog sie vor das OLG. Das sah die Sache anders als die Vorinstanz.

So entschied das OLG

Die Klage der Frau auf Auskunft ist begründet. Ihr steht ein entsprechender Anspruch nach Art. 15 Abs. 1 und 3 DSGVO zu. Die DSGVO ist für die Tätigkeit eines gerichtlichen Sachverständigen anzuwenden. Es greift kein Ausnahmetatbestand nach Art. 2 Abs. 2 DSGVO. Daneben werden die Vorgaben der DSGVO zum Auskunftsrecht nicht durch verfahrensrechtliche Akteneinsichtsrechte verdrängt. Diese beziehen sich auf einen anderen Zweck, nämlich den Inhalt der Gerichtsakten.

Gutachter ist als Verantwortlicher anzusehen

Entscheidend ist nach Art. 4 Nr. 7 DSGVO, wer allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Zwar entscheidet im Wesentlichen das Gericht über den Zweck im Rahmen des Beweisbeschlusses. Die Entscheidung über die Mittel der Verarbeitung obliegt jedoch dem Sachverständigen. Er bestimmt die Art und Weise, wie das beabsichtigte Ergebnis erreicht werden soll. Er ist kein funktionaler Teil des Gerichts. Vielmehr entscheidet der Gutachter eigenverantwortlich, etwa über den Verarbeitungsumfang zur Erstellung des Gutachtens. Das Gericht hat keine Möglichkeiten zur Überwachung und Kontrolle der Datenverarbeitung.

Gutachter muss Auskunftspflicht nachkommen

Zwar kann das Auskunftsrecht gemäß Art. 23 Abs. 1 DSGVO durch EU-Gesetze oder Gesetze der Mitgliedstaaten beschränkt werden. Eine solche Beschränkung besteht in Deutschland jedoch nicht. Insbesondere enthält die ZPO keine solche Einschränkung. Auch allgemeine Erwägungen zum Schutz von Gerichtsverfahren führen nicht zu einer Beschränkung des Auskunftsrechts. Selbst der Grundsatz des fairen Verfahrens nach Art. 6 Abs. 1 Satz 1 der Europäischen Menschenrechtskonvention führt zu keiner Einschränkung des Rechts auf Auskunft.

Mit der begehrten Auskunft werden Rechte und Freiheiten anderer Personen genauso wenig beeinträchtigt wie ein eventuelles Urheberrecht des Gutachters. Gerade zum Urheberrecht hat der Gutachter nichts schlüssig vorgetragen. Doch selbst wenn das Urheberrecht bestehe, dürfe das nicht zu einer Beschneidung des Rechts auf Auskunft führen.

Gutachter muss voll Auskunft geben

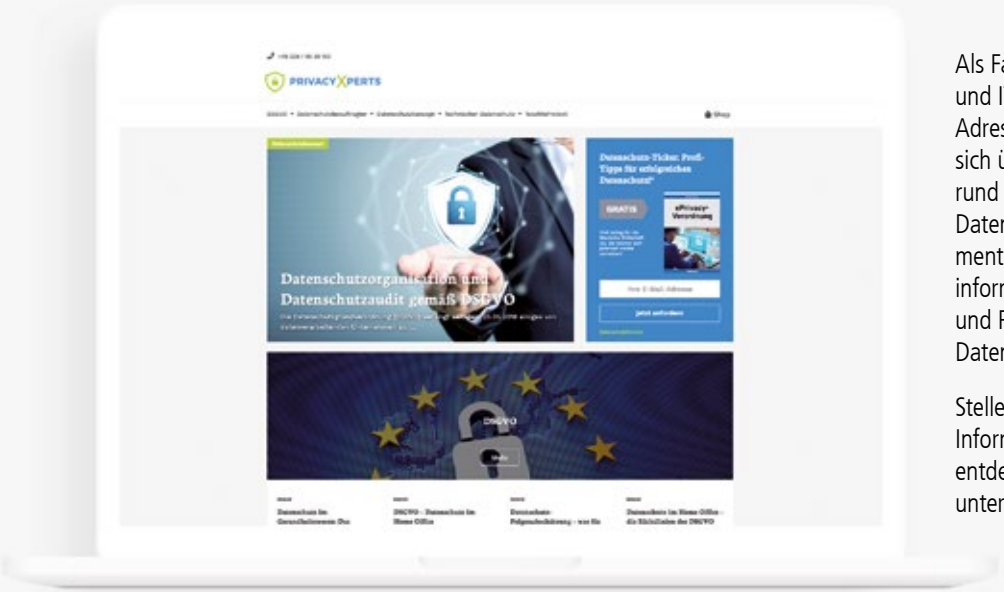
Vom Auskunftsanspruch und dem Recht auf Kopie nach Art. 15 Abs. 3 DSGVO ist das gesamte Gutachten erfasst. Dies gerade, wenn der Zusammenhang der verarbeiteten Daten erforderlich ist, um die Verständlichkeit sicherzustellen. Insofern ist eine originalgetreue Reproduktion notwendig. Erfasst sind alle Teile des Gutachtens, die in irgendeinem inhaltlichen Bezug zur Klägerin stehen. Auch allgemeine Ausführungen können erfasst sein, wenn sie für das Verständnis der weiteren Ausführungen erforderlich sind. Eine Zusammenfassung oder Zusammenstellung der personenbezogenen Daten der Klägerin reicht nicht aus, wenn damit das Verständnis oder die Überprüfung der Richtigkeit und Vollständigkeit der Daten erschwert würden.

§

Das können Sie folgern

Wer Verantwortlicher im Sinne des Art. 4 Nr. 7 DSGVO ist, der muss den Anforderungen der DSGVO nachkommen und auch die Rechte der Betroffenen erfüllen. Ein Gutachter ist eigenständig Verantwortlicher, selbst wenn er von einem Gericht beauftragt wird.

„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**

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:

So mindern Sie Datenschutzrisiken beim Chef

Planen Sie jetzt das 4. Quartal 2026