



VIDEOÜBERWACHUNG: DIESE PUNKTE SOLLTEN SIE CHECKEN

SICHERHEIT

Unternehmenssicherheitskonzept:
Haken Sie hier nach

1-2

WISSEN VERMITTELN

Wenn intern ermittelt werden soll:
Beugen Sie Pannen vor

3





Sicherheit muss sein

Liebe Leserin, lieber Leser,

es gibt Abteilungen im Unternehmen, die für Sie als Datenschutzbeauftragten von großer Bedeutung sind, etwa weil diese auch den Schutz personenbezogener Daten unterstützen. Die Rede ist von der Unternehmenssicherheit. Zwar mag der Datenschutz nicht deren primäres Anliegen sein. Jedoch werden dem Datenschutz gute Dienste erwiesen, wenn die Kollegen ihren Job gut machen.

Doch auch bei der Unternehmenssicherheit wird viel mit personenbezogenen Daten gearbeitet. Gleichwohl darf es am Datenschutz keine Abstriche geben. Grund genug für Sie, einmal genauer hinzuschauen bzw. nötiges Wissen zu vermitteln.

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

Sicherheit

Unternehmenssicherheitskonzept:
Haken Sie hier nach
[Seiten 1–2](#)

Wissen vermitteln

Wenn intern ermittelt werden soll:
Beugen Sie Pannen vor
[Seite 3](#)

Videoüberwachung

Videoüberwachung:
Diese Punkte sollten Sie checken
[Seiten 4–5](#)

Beratung

Bestandsaufnahme:
Das können Sie prüfen
[Seiten 6–7](#)

Kontrollen

Diese Punkte sind entscheidend für
Taschenkontrollen am Firmmentor
[Seite 8](#)



Zum neuen Onlinebereich!
www.privacyxperts.de/login



Expertensprechstunde:
www.privacyxperts.de/kontaktformular/

Bildnachweise:

Titel: Adobe Stock | Tiberius Gracchus

Seite 1: Adobe Stock | CrazyCloud

Impressum



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: 26-mal pro Jahr

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

(bei Rückfragen bitte Kundennummer angeben)

Dieses monothematische Supplement
„Unternehmenssicherheit“ liegt der Ausgabe Mai 2025 von
„Datenschutz aktuell“ bei.

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und
überprüft. Sie basieren jedoch auf der Richtigkeit uns erteil-
ter Auskünfte und unterliegen Veränderungen. Eine Gewähr
kann deshalb nicht übernommen werden.

Im Interesse der Lesbarkeit verzichten wir in unseren Beiträ-
gen auf geschlechtsbezogene Formulierungen. Selbstver-
ständlich 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



Unternehmenssicherheitskonzept: Haken Sie hier nach

Sie wissen vielleicht nur zu gut: Wenn man als Datenschutzbeauftragter wenig Zeit hat, muss man diese gut nutzen. Es ist wichtig, die Dinge clever und geschickt anzugehen. Eine Möglichkeit ist, im Unternehmen nach Verbindungen zu suchen, die beim Schutz persönlicher Daten helfen können. Vielleicht gibt es ein Team, das sich um die Unternehmenssicherheit kümmert. Und das bestimmt mit Konzept.

Gemeinsame Ziele

Zuerst könnte es scheinen, dass Sie als Datenschutzbeauftragter und das Sicherheitsteam grundverschiedene Ziele haben: Ihnen geht es in erster Linie um den Schutz persönlicher Daten, etwa von Kunden oder Mitarbeitern. Die Kollegen schützen Hab und Gut des Unternehmens und natürlich auch die Beschäftigten. Aber bei näherer Betrachtung arbeiten beide eigentlich für dasselbe Ziel. Beide wollen Schaden vom Unternehmen abwenden. Ein Beispiel ist, Unbefugte daran zu hindern, das Firmengelände zu betreten, um Straftaten zu begehen. Das kann der Diebstahl von Informationen sein, wie z. B. persönliche Daten, Geschäftsgeheimnisse oder Entwicklungsdaten.

Auch der Schutz von Werten ist für Sie relevant

Vielleicht denken Sie, dass Schutz vor Sabotage und Schäden nichts mit Datenschutz zu tun hat und eher in den Aufgabenbereich der Kollegen der Unternehmenssicherheit fällt. Aber das ist falsch. Wenn z. B. eine Trafostation ausfällt, kann das auch zum Problem für den Datenschutz werden. Schließlich können IT-Systeme oder Server Schaden nehmen, mit denen personenbezogene Daten verarbeitet werden. Der Schaden ist vielleicht gering, wenn Daten nur vorübergehend nicht verfügbar sind. Er ist immens, wenn Daten beschädigt wurden und für immer verloren sind. Und wird eine solche Panne in den Medien bekannt, wird der Schaden noch größer. Umso wichtiger ist also, dass Sie als Datenschutzbeauftragter auch ein Auge auf den passenden und risikoangemessenen Schutz haben.

Ihr Fokus: Datenschutz durch die richtigen Maßnahmen

Wollen Sie, dass die Unternehmenssicherheit mit Ihnen an einem Strang zieht? Nutzen Sie Datenschutz und Datensicherheit als Argument: Für das Verarbeiten von persönlichen Daten gilt es, viele Regeln zu beachten. Z. B. braucht man immer eine rechtliche Erlaubnis, die Rechtsgrundlage. Außerdem müssen persönliche Daten sicher verarbeitet werden. Hier lohnt der Blick in Art. 32 Datenschutz-Grundverordnung.

Überprüfen Sie die Schutzmaßnahmen

Die Kollegen machen sich bestimmt fortlaufend Gedanken, wie man das Firmengelände, die Gebäude und Werte sichern und die Firma vor Schaden schützen kann. Das Ergebnis ist meist ein umfassendes Sicherheitskonzept. Als Datenschutzbeauftragter sollten Sie sich das einmal genauer ansehen. So können Sie besser einschätzen, wie gut bestimmte technische und organisatorische Schutzmaßnahmen sind. Denn die können für das Datenschutzniveau entscheidend sein.



Gehen Sie mit Fingerspitzengefühl vor

Um die Kollegen nicht zu verprellen, sollten Sie Kritik geschickt formulieren. Sagen Sie nicht, dies oder jenes wäre schlecht oder falsch. Fragen Sie zunächst nach dem Warum, etwa „Warum ist diese Maßnahme aus Ihrer Sicht risikoangemessen?“ In Reaktion auf die Antwort der Kollegen können Sie dann Ihre Kritik oder den bestehenden Handlungsbedarf als „dringende Empfehlung des Datenschutzbeauftragten“ anbringen.




CHECKLISTE: Prüfen Sie das Unternehmenssicherheitskonzept


Fragestellung	Hintergrundinformationen	In Ordnung?
Inwieweit gibt es ein Sicherheitskonzept, um Unternehmen, Mitarbeiter, Betriebsgelände, Gebäude und Werte abzusichern?	- Das Konzept sollte nicht nur schriftlich verfasst sein. Es sollte auch von einem verantwortlichen Bereich bzw. von der Unternehmensleitung freigegeben sein. - Schauen Sie, worauf sich das Konzept erstreckt. Manchmal kommt es zu innerbetrieblichen Veränderungen (z. B. Umorganisationen des Betriebs, Anmietung von Räumlichkeiten außerhalb des eigentlichen Betriebsgeländes), sodass manches nicht erfasst ist.	☐ Ja ☐ Nein
Bestehen spezifische Konzepte für bestimmte Bereiche?	- Ein Konzept, mit dem alles Relevante erfasst und geregelt wird, kann dazu führen, dass es zu umfassend und unübersichtlich wird. Ggf. ist es sinnvoll, für bestimmte Bereiche spezifische Konzepte zu erstellen. - Denken Sie hier an die Unternehmensleitung bzw. die Führungsetage oder die Entwicklungsabteilung. Doch auch für den IT- und Serverbetrieb können Konzepte mit spezifischen Maßnahmen angebracht sein.	☐ Ja ☐ Nein
Wann wurde das Konzept erstellt und zuletzt überarbeitet?	- Der Blick auf Erstellungs- oder Überarbeitungsdatum kann schnell die Erkenntnis bringen, dass hier Handlungsbedarf besteht. Schließlich verändern sich Gefahren und Risiken fortlaufend, sodass regelmäßig geprüft werden sollte, inwieweit die Einschätzung und festgelegte Maßnahmen noch passen. - Haben Sie auch ein Auge darauf, wer das Dokument erstellt bzw. überarbeitet hat. Diese Person muss nicht automatisch geeignet oder qualifiziert sein.	☐ Ja ☐ Nein
Welche Stellen wurden in die Erstellung und Ausarbeitung des Konzepts einbezogen?	- Für umfassende Sicherheit bringt es meist wenig, wenn das Konzept im stillen Kämmerlein erarbeitet und beschlossen wird. Schließlich können viele andere Abteilungen Relevantes beitragen bzw. an der Festlegung bzw. Umsetzung von Maßnahmen zu beteiligen sein. - Typischerweise sind folgende Abteilungen relevant: Personalabteilung, IT-Abteilung, Gebäudemanagement.	☐ Ja ☐ Nein
Wie wurden Gefahren, Bedrohungen und Schwachstellen analysiert?	- Hier geht es vor allem darum, dass die Risikoanalyse Hand und Fuß hat. Denn einfach drauflosplanen ist für ein gutes Sicherheitskonzept der falsche Ansatz. Vorab müssen Gefahren (etwa räumliche Lage des Betriebsgeländes), aber auch problematische Rahmenbedingungen (z. B. Verbot baulicher Veränderungen am Mietgebäude) analysiert und bewertet werden. - Achten Sie darauf, dass Sie das typische Vorgehen wiederfinden: Es werden Gefahren ausgemacht. Dann wird der mögliche Schaden bewertet. Schließlich muss die Wahrscheinlichkeit des Schadens Eintritts bewertet werden. Erst jetzt hat man ein Risiko, das je nach Bewertung unterschiedlich ausfallen kann.	☐ Ja ☐ Nein
Wurden unternehmens- oder geschäftstätigkeitsbezogene Bedrohungen berücksichtigt?	- Hier kann ein Brainstorming gute Dienste leisten. Überlegen Sie, was gerade für Ihr Unternehmen von Bedeutung sein kann, welche (Angriffs-)Szenarien oder Schadensereignisse es geben kann. - Denken Sie auch an Aspekte wie Sabotage, das Ausspähen von Informationen oder Social Engineering.	☐ Ja ☐ Nein
Welche Maßnahmen sind zur Risikobehandlung festgelegt?	- Risiken ausmachen und bewerten ist eine Sache. Eine ganz andere jedoch, wie man damit umgeht. Idealerweise findet man Gegenmaßnahmen, die ein Risiko auf nahezu null reduzieren. - Finden Sie Risiken, denen man mit einer Übertragung (z. B. auf eine Versicherung) begegnen oder die man akzeptieren will, sollten Sie in die Detailprüfung gehen. Gerade ein „Mit dem Risiko müssen wir eben leben“ ist kein Argument dafür, jegliche Maßnahmen zur Risikoreduktion zu unterlassen. - Machen Sie deutlich, dass es nicht nur technische Maßnahmen zur Behandlung von Risiken geben kann. Unter Umständen bringen auch organisatorische Maßnahmen viel. Meist ist die Kombination aus beiden die beste Wahl.	☐ Ja ☐ Nein
Inwieweit passen die organisatorischen Maßnahmen?	- Technik allein reicht in der Regel nicht aus. Auch organisatorische Maßnahmen sind notwendig, so beispielsweise Arbeitsanweisungen, Richtlinien und Prozessbeschreibungen zur Umsetzung. - Theorie und Praxis müssen zusammenpassen. Die beste Regelung bringt nichts, wenn sie im Arbeitsalltag nicht gelebt und umgesetzt werden kann. Dazu müssen Regelungen auch den Mitarbeitern bekannt sein. - Besteht Datenschutzrelevanz, können Sie prüfen, inwieweit man Sie als Datenschutzbeauftragten eingebunden hat.	☐ Ja ☐ Nein
Sind Zuständigkeiten und Verantwortlichkeiten klar definiert?	- Einerseits müssen diese Zuweisungen der Maßnahmen vorgenommen sein. Andererseits müssen die entsprechend Benannten auch tatsächlich in der Lage sein, die an sie gerichtete Anforderung zu erfüllen. - Sprechen Sie mit den Verantwortlichen, inwieweit sie aus deren Sicht überhaupt die Verantwortung wahrnehmen können.	☐ Ja ☐ Nein

Wenn intern ermittelt werden soll: Beugen Sie Pannen vor

Läuft etwas im Unternehmen schief oder kommt es beispielsweise zu Diebstählen, schlägt vielleicht die Stunde der Unternehmenssicherheit. Diese soll dann ggf. im Auftrag der Unternehmensleitung der Sache auf den Grund gehen. Was auf den ersten Blick nach einem folgerichtigen Vorgehen aussieht, kann sich schnell als Datenschutzproblem entpuppen.

Klären Sie geschickt auf

Gerade im Hinblick auf Ermittlungen gibt es einige Knackpunkte im Datenschutz. Diese sollten die Kollegen kennen, um Probleme erst gar nicht entstehen zu lassen. Weisen Sie auf die fünf wichtigsten hin:

Knackpunkt 1: Es bedarf immer einer Rechtsgrundlage

Sollen personenbezogene Daten im Zusammenhang mit präventiven (= vorbeugenden) oder repressiven (= strafverfolgenden) Zwecken verarbeitet werden, muss vorab immer die Rechtsgrundlage geklärt werden. Diese kann sich vor allem aus Art. 6 Abs. 1 Satz 1 Datenschutz-Grundverordnung (DSGVO) ergeben. Zu nennen ist etwa die Verarbeitung auf Basis der Einwilligung des Betroffenen (Art. 6 Abs. 1 Satz 1 Buchst. a DSGVO), zur Vorbereitung oder Durchführung eines Vertrags mit ihm (Art. 6 Abs. 1 Satz 1 Buchst. b DSGVO) oder zur Wahrnehmung eines überwiegenden berechtigten Interesses (Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO).

Soll beispielsweise erkannt werden können, wer als Externer zu oft die Entwicklung besucht, kann die entsprechende Verarbeitung personenbezogener Daten ggf. auf ein überwiegendes berechtigtes Interesse gestützt werden. Allerdings müssen hier viele Rahmenbedingungen berücksichtigt werden und die Abwägung muss zugunsten des berechtigten Interesses des Unternehmens ausfallen.

Knackpunkt 2: Zweckänderungen sind nicht problemlos möglich

Werden personenbezogene Daten verarbeitet, muss schon bei der Erhebung bzw. Beschaffung der Daten der Zweck konkret festgelegt sein. Eine Verarbeitung personenbezogener Daten auf Vorrat oder ohne konkret definierten Zweck ist unzulässig und wäre an sich bereits ein Datenschutzverstoß.

Jedoch ist das Verarbeiten für einen anderen Zweck nicht immer verboten. Es gibt mit Art. 6 Abs. 4 DSGVO eine Vorschrift, die eine Verarbeitung für einen anderen Zweck erlauben kann. Dazu muss der neue Zweck mit dem bisherigen Zweck kompatibel sein. Ob das der Fall ist, bedarf einer genauen Prüfung der Rahmenbedingungen.

Auch sind andere Vorschriften einzubeziehen, etwa § 24 Bundesdatenschutzgesetz (BDSG). Danach kann eine Verarbeitung personenbezogener Daten zu einem anderen Zweck zulässig sein, wenn dies für die Verfolgung von Straftaten erforderlich ist. Auch wenn die zweckändernde Verarbeitung für die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, kann sie auf Art. 6 Abs. 4 DSGVO

i. V. m. § 24 Abs. 1 Nr. 2 BDSG gestützt werden. Aber Achtung! Auch in diesen Fällen dürfen die Interessen der betroffenen Person am Ausschluss der Verarbeitung nicht überwiegen.

Knackpunkt 3: Bei Beschäftigten gelten Besonderheiten

Geht es um personenbezogene Daten zu Beschäftigten, müssen Sie die Rahmenbedingungen aus § 26 BDSG beachten. Dieser macht beispielsweise besondere Vorgaben, wenn es um die Ermittlungen bei Straftaten geht. Dabei ist wichtig: Alle in § 26 Abs. 1 Satz 2 BDSG genannten Voraussetzungen müssen eingehalten werden. Passiert das nicht, kann es schlimmstenfalls bei einem arbeitsgerichtlichen Rechtsstreit zu einem Beweisverwertungsverbot kommen. Außerdem kann wegen einer unzulässigen Verarbeitung ein Bußgeld drohen. Zudem kann ein Betroffener Schadensersatz fordern, wenn ihm ein Schaden entstanden ist. Der kann auch immaterieller Natur sein.

Auch ist wichtig: Eventuell bestehen Betriebsvereinbarungen. Sehen diese strengere (Datenschutz-)Maßstäbe vor, sind diese einzuhalten. Dagegen können Betriebsvereinbarungen den Standard der DSGVO nicht absenken. Er muss etwa hinsichtlich Rechtsgrundlage, Erforderlichkeitsprinzip, Schutzmaßnahmen oder Betroffenenrechten eingehalten werden.

Knackpunkt 4: Transparenz ist (fast immer) ein Muss

Sollen personenbezogene Daten verarbeitet werden, muss das transparent passieren, sprich, der Betroffene muss über die Rahmenbedingungen informiert werden, und zwar egal, ob sie bei ihm erhoben werden oder bei Dritten. Ein heimliches Verarbeiten ist grundsätzlich nicht mit der Zielsetzung der DSGVO vereinbar. Allerdings kann es Ausnahmen geben, etwa für Kontrollmaßnahmen ohne Kenntnis des Betroffenen.

In bestimmten Fällen greifen die Ausnahmen des Art. 14 Abs. 5 DSGVO bzw. des § 33 Abs. 1 Nr. 2 BDSG, sodass eine Verarbeitung auch ohne Kenntnis des Betroffenen zulässig sein kann.

Knackpunkt 5: Erforderlichkeit und Verhältnismäßigkeit müssen gegeben sein

Die Zulässigkeit einer Verarbeitung ist entscheidend von der Erforderlichkeit bzw. von der Verhältnismäßigkeit der Verarbeitung abhängig. Hierzu müssen mehrere Aspekte erfüllt sein. So muss nicht nur ein legitimer Zweck verfolgt werden. Die konkrete Verarbeitung der Daten muss geeignet (= der Zweck lässt sich damit erreichen), erforderlich (= es gibt keine alternative Vorgehensweise, die die Betroffenen weniger beeinträchtigt) und angemessen (= die Verarbeitung darf insgesamt nicht außer Verhältnis zum Zweck stehen) sein.



Videoüberwachung:

Diese Punkte sollten Sie checken

Geht es um die Absicherung von Betriebsgelände oder Gebäuden, fällt diese Aufgabe meist in den Zuständigkeitsbereich der Unternehmenssicherheit oder des Werkschutzes. Weil Videoüberwachung oft auch auf eine Verarbeitung personenbezogener Daten hinausläuft, muss die für die Verarbeitung verantwortliche Abteilung so manchen Datenschutzaspekt berücksichtigen.

Damit Sie nichts vergessen

Sie wollen in Sachen Videoüberwachung beraten? Oder wollen Sie vielleicht eine bereits stattfindende Videoüberwachung auf Herz und Nieren prüfen? Kein Problem!

Setzen Sie sich dazu mit den zuständigen Kollegen zusammen und klären Sie insbesondere die Fragen in folgender Checkliste. Passt es irgendwo nicht, sollten Sie mit den Kollegen die zu ergreifenden Maßnahmen vereinbaren und die Umsetzung terminieren.

 CHECKLISTE: Typische Prüfaspekte bei Videoüberwachung 		
Aspekt	Hierauf können Sie eingehen	Geklärt und in Ordnung?
Wie gestaltet sich die geplante bzw. eingesetzte Videoüberwachung?	➤ Am besten lassen Sie sich entsprechende Unterlagen und Pläne vorlegen. Haben Sie ein Auge darauf, wann die Unterlagen erstellt wurden. Sind diese schon in die Jahre gekommen, stimmen Soll und Ist manchmal nicht mehr überein. ➤ Lassen Sie sich auch Vereinbarungen oder Verträge vorlegen. Nicht nur eine Vereinbarung zum Datenschutz kann wichtig sein. Haben Sie auch ein Auge auf Leistungsbeschreibungen für eingekaufte Services oder Wartungsdienstleistungen. ➤ Hinterfragen Sie, wer wofür zuständig ist und wer worüber entscheidet. Manchmal entscheidet bei einer Videoüberwachung der Dienstleister mehr als derjenige, der es am Ende datenschutzrechtlich zu verantworten hat, nämlich Ihr Unternehmen.	☐ Ja ☐ Nein
Wie steht es um die Eintragung im Verzeichnis von Verarbeitungstätigkeiten?	➤ Schauen Sie, was Sie bezüglich der Verarbeitungstätigkeit „Videoüberwachung“ vorfinden. Ggf. ist die Beschreibung zu allgemein und gibt die Rahmenbedingungen für die einzelnen Überwachungssituationen nicht wieder. ➤ Manchmal sind die Eintragungen unvollständig, veraltet oder fehlen ganz. Adressieren Sie den entsprechenden Handlungsbedarf.	☐ Ja ☐ Nein
Wie gestalten sich die Rahmenbedingungen vor Ort?	➤ Ein Plan ist gut, die Dinge mit eigenen Augen zu sehen, aber oft viel besser. Denn nicht selten sieht die Realität anders aus, als es der Plan vorsieht. Machen Sie sich also ein Bild vor Ort. ➤ Werfen Sie auch einen Blick auf den von den Kameras gelieferten Bildausschnitt. ➤ Haben Sie vor Ort ein Auge auf das Drumherum. Schauen Sie sich an, wo Grundstücksgrenzen verlaufen. Eventuell gibt es Bereiche, die nicht überwacht werden dürfen. ➤ Manchmal wird auch erst beim Vor-Ort-Besuch klar, dass eine Kamera eher einer Attrappe ähnelt, weil sie verschmutzt oder defekt ist.	☐ Ja ☐ Nein
Warum gibt es die Videoüberwachung überhaupt bzw. warum gibt es eine Überwachung an der betreffenden Stelle?	➤ Die Gründe, also die verfolgten Zwecke, muss man Ihnen nennen können. Akzeptieren Sie nicht pauschale Antworten wie „Das machen wir zur Sicherheit“. ➤ Vorsicht vor Bewertungen des großen Ganzen. Der Zweck muss für jede Überwachungssituation bzw. jede Kamera festgelegt sein und passen.	☐ Ja ☐ Nein
Welche Technik wird eingesetzt?	➤ Zwar gibt es hier und da noch ganz klassische Überwachungssysteme mit Bandaufzeichnung. Allerdings gehören die meist schon eher ins Museum. Doch auch bei solchen „Uralt-Systemen“ muss den Anforderungen der Datenschutz-Grundverordnung (DSGVO) entsprochen werden. Es gibt keinen Bestandsschutz für alte Technik. ➤ Nutzt man moderne Systeme, etwa über WLAN oder gar mit einem Cloud-Speicher, sollten Sie sich das ganz genau erklären lassen. Schauen Sie ganz besonders nach der Sicherheit der entsprechenden Lösung bzw. auch nach nötigen Datenschutzvereinbarungen. Schließlich ist und bleibt Ihr Unternehmen für die eingesetzte Technik verantwortlich.	☐ Ja ☐ Nein
Inwieweit findet eine inhaltliche Bildanalyse durch die Technik statt?	➤ Klären Sie, was die Technik macht und wie es beispielsweise zu einer Alarmmeldung kommt. Eventuell ist die Kamera „intelligent“ und kann eigenständig Veränderungen im Bild oder Personen als Objekte im Bild erkennen. ➤ Schauen Sie, inwieweit es Verfolgungsmöglichkeiten gibt, sodass „Objekte“ vom System zur Nachverfolgung von einer zur anderen Kamera weitergegeben werden. Dieses Tracking kann zum Datenschutzproblem werden.	☐ Ja ☐ Nein



CHECKLISTE: Typische Prüfaspekte bei Videoüberwachung

Wird auf künstliche Intelligenz (KI) gesetzt?	› Stellen Sie die Frage an die Zuständigen. Lassen Sie sich erklären, was stattfindet, und besprechen Sie, inwieweit Datenschutzrelevanz besteht. › Geben Sie den Hinweis, dass je nach Szenario auch die KI-Verordnung umzusetzen ist. Im Bedarfsfall sollten die hierfür zuständigen Stellen im Unternehmen eingebunden werden.	☐ Ja ☐ Nein
Warum ist die Videoüberwachung am jeweiligen Einsatzort rechtlich erlaubt?	› Generell gilt: ohne Rechtsgrundlage keine Verarbeitung personenbezogener Daten. › Maßstab für die Zulässigkeit einer Videoüberwachung ist meist Art. 6 Abs. 1 Satz 1 Buchst. f DSGVO. Hier muss eine Interessenabwägung stattfinden. › Das berechnigte Interesse des Verantwortlichen muss die Interessen der Betroffenen überwiegen. Dabei spielen Erforderlichkeit und Verhältnismäßigkeit oft die entscheidende Rolle. Nicht selten ist die Videoüberwachung nicht geeignet, es gibt mildere Mittel oder es fehlt an der Angemessenheit mit Blick auf das verfolgte Ziel.	☐ Ja ☐ Nein
Inwieweit bestehen betriebliche Regelungen, etwa in einer Betriebsvereinbarung?	› Sind Arbeitnehmer betroffen, bedarf es aufgrund der zwingenden Mitbestimmung aus § 87 Abs. 1 Nr. 6 Betriebsverfassungsgesetz einer Betriebsvereinbarung. Diese enthält oft Vorgaben und Verbote. › Existiert eine Vereinbarung, sollten Sie klären, ob die Festlegungen in der Praxis umgesetzt sind. › Achten Sie darauf, dass der Mindeststandard der DSGVO gewahrt ist. Ist dies nicht der Fall, hat die Betriebsvereinbarung keine Regelungswirkung.	☐ Ja ☐ Nein
Welche Bereiche sind von der Erfassung ausgenommen?	› Generell darf Ihr Unternehmen nur innerhalb der eigenen Grundstücksgrenzen überwachen. Der öffentliche Raum (z. B. Straße) darf maximal 1 m über die Grenze hinaus erfasst werden. Dieser „Grenzgebiet“ wird von Aufsichtsbehörden meist nicht beanstandet. › Gerade Nachbargrundstücke sind generell tabu. Ggf. muss mit technischen Lösungen (z. B. montierten Sichtblenden) dafür gesorgt werden, dass eine entsprechende Überwachung unmöglich ist. › Eventuell kann es ausreichen, wenn Bereiche verpixelt oder geschwärzt werden. Allerdings muss das in der Kamera passieren, sodass der entsprechende Bildinhalt fehlt.	☐ Ja ☐ Nein
Wann findet eine Aufzeichnung statt?	› Schauen Sie sich das am System für jede Kamera an. Das lässt sich in der Regel individuell steuern. Insofern sollten Sie auf die Umsetzung des Erforderlichkeitsgrundsatzes achten. › Je nach Bereich kann die Aufzeichnung nur außerhalb der Arbeits- und Geschäftszeiten zulässig sein. Hier sind die Interessen von Besuchern, Kunden und Beschäftigten zu berücksichtigen.	☐ Ja ☐ Nein
Wie und wo werden die Bilddaten gespeichert?	› Schauen Sie, wo die Daten landen. Diese können lokal oder in einer Cloud gespeichert werden. Ist Letzteres der Fall, muss auch hier für Sicherheit gesorgt werden, etwa bei der Datenübertragung. Eventuell ist eine Vereinbarung zur Auftragsverarbeitung nötig. › Auch Videoüberwachungssysteme sind vor Dieben nicht sicher. Hinterfragen Sie die Unterbringung und die Verschlüsselung der Daten.	☐ Ja ☐ Nein
Für welchen Zeitraum werden Bilddaten gespeichert? Was passiert danach?	› Hier muss dem Grundsatz der Speicherbegrenzung Rechnung getragen werden (vgl. Art. 5 Abs. 1 Buchst. e DSGVO). Ist die Kenntnis der Daten für den verfolgten Zweck nicht mehr erforderlich, müssen sie gelöscht werden. Das ergibt sich auch aus Art. 17 Abs. 1 Buchst. a DSGVO. Ob auf einem Datenspeicher noch viel freier Platz ist, spielt keine Rolle. Standardmäßig dürfte eine Speicherdauer von 48 bis 72 Stunden ausreichen. › Fragen Sie nach, wie der Prozess zur Löschung von Daten ausgestaltet ist. Prüfen Sie, ob dieser aus Ihrer Sicht in der Praxis so passt.	☐ Ja ☐ Nein
Wie wird die nötige Transparenz gegenüber Betroffenen hergestellt?	› Transparenz ist ein Muss. Schauen Sie vor Ort, ob Betroffene rechtzeitig problemlos erkennen können, dass sie sich auf einen Bereich mit Videoüberwachung zubewegen. › Ein Hinweisschild oder Piktogramm reicht in aller Regel nicht aus. Zumindest Basisangaben (z. B. Verantwortlicher, Kontaktdaten, weitere Informationsmöglichkeit) müssen angegeben werden. Orientieren Sie sich an den Informationspflichten aus Art. 13 DSGVO.	☐ Ja ☐ Nein
Wer kann wie auf die Videoüberwachung bzw. auf gespeicherte Daten zugreifen?	› Es muss festgelegt sein, wer für welchen Zweck auf die aufgezeichneten Daten zugreifen darf. Achten Sie hier darauf, dass man sich auf das Erforderliche beschränkt, sprich das „Need-to-know-Prinzip“ beachtet. › Machen Sie den Check, wenn Überwachungsdaten in der Cloud liegen. Vielleicht haben hier mehr Personen Zugriff als erforderlich.	☐ Ja ☐ Nein
Wie wird die Sicherheit der Verarbeitung gewährleistet?	› Technische bzw. organisatorische Schutzmaßnahmen im Sinne von Art. 32 DSGVO sind unerlässlich. Dazu müssen zunächst die Risiken ausgemacht werden, damit die passenden Maßnahmen festgelegt und umgesetzt werden können. Denken Sie hier insbesondere auch an die Themen Zugriffsschutz und Verschlüsselung. › Gibt es eine Verbindung ins Internet, sollten Sie die Datenübertragung hinterfragen. › Denken Sie auch an die Themen Updates und Wartung. Diese sind wichtige Sicherheitsbausteine.	☐ Ja ☐ Nein
Inwieweit sind andere Stellen an der Verarbeitung beteiligt?	› Eventuell werden Dienste von Dritten genutzt, die sich im Alarmfall aufschalten können. Auch wenn Speicher im Internet genutzt werden, kann das eine Auftragsverarbeitung sein. Dann ist Art. 28 DSGVO zu beachten. › Sitzt der Dienstleister in einem Drittstaat, greifen die Anforderungen aus Kapitel V der DSGVO. Insbesondere muss Ihr Unternehmen für ein angemessenes Datenschutzniveau sorgen.	☐ Ja ☐ Nein



Bestandsaufnahme: Das können Sie prüfen

Je nach Unternehmensgröße wird die Unternehmenssicherheit bzw. der Werkschutz entsprechend aufgestellt sein. Insofern können der Aufgabenzuschnitt und die damit einhergehende Verarbeitung personenbezogener Daten ganz unterschiedlich ausfallen.

Klären Sie, was Sache ist

Hatten Sie bislang eher kein Auge auf diesen Bereich im Unternehmen, lohnt es sich umso mehr, wenn Sie etwas Licht ins Dunkel bringen. Klären Sie mit den zuständigen Kollegen, welche Verarbeitungssituationen es gibt und inwieweit personenbezogene Daten eine Rolle spielen. Damit Sie Ihrem Beratungsauftrag aus Art. 39 Abs. 1 Datenschutz-Grundverordnung

(DSGVO) umfassend nachkommen können, finden Sie in der folgenden Checkliste viele Themen und Verarbeitungssituationen, die Sie adressieren können. Gibt es eine der erwähnten Situationen, können Sie nach der ersten Bestandsaufnahme in weiteren Gesprächen in die Tiefe gehen. Übrigens: Checken Sie auch, inwieweit Sie die betreffenden Verarbeitungen im Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) wiederfinden.

 CHECKLISTE: Bestandsaufnahme Unternehmenssicherheit 		
Aspekt	Hintergrund	Besprochen bzw. geklärt?
Zutrittskontrollsysteme	› Es gibt verschiedene Zutrittskontrollsysteme. Häufig anzutreffen sind in Unternehmen Chipkarten, mit denen der jeweilige Mitarbeiter Zutritt gemäß den für ihn vorgesehenen Zutrittsberechtigungen erhält. › Lassen Sie sich das System umfassend erklären. Idealerweise stellen die Kollegen Ihnen Konzepte, Beschreibungen und Übersichten zur Verfügung. › Klären Sie, welche personenbezogenen Daten für die Steuerung des Zutritts verarbeitet werden. Sind biometrische Informationen im Spiel, müssen Sie hellhörig werden. Dabei handelt es sich um Daten nach Art. 9 Abs. 1 DSGVO, sodass besondere Rahmenbedingungen gelten, etwa zur Rechtsgrundlage. › Hinterfragen Sie auch das Vorgehen, wenn das System ausfällt oder jemand eine Zutrittsberechtigung fordert. Hier müssen die Prozesse passen.	☐ Ja ☐ Nein
Ausweismanagement	› Beispielsweise um schnell zu erkennen, wer Mitarbeiter ist und wer nicht, setzen viele Unternehmen auf Ausweise. › Klären Sie, für welche Personengruppen es welche Ausweise bzw. Ersatzausweise gibt, etwa für Mitarbeiter, Aushilfen, Besucher, Handwerker. › Gerade bei Ausweisen für Nichtmitarbeiter sollten Sie klären, welche Berechtigungen hinterlegt sind. Vor allem bei (Tages-)Ausweisen für Handwerker oder Ersatzausweisen dürfen die Zutrittsberechtigungen nicht zu weitreichend sein. Idealerweise werden sie individuell vergeben, damit sie auf den konkreten Fall passen. › Haben Sie ein Auge auf die relevanten Prozesse zur Beantragung, Ausgabe und Rückgabe von Ausweisen. Von Relevanz ist auch der Prozess bei Verlust eines Ausweises. Hier müssen nicht nur Meldungen schnell möglich sein. Die Berechtigungen müssen schnellstens entzogen werden.	☐ Ja ☐ Nein
Schlüsselverwaltung	› Schlüssel wirken zwar manchmal schon etwas antiquiert. Es gibt sie aber noch so gut wie in jedem Unternehmen. Insofern ist auch eine Verwaltung der Schlüssel unerlässlich. Hinterfragen Sie, was passiert, wenn ein Schlüssel verloren geht. Passiert nichts, kann das auch zum Sicherheitsrisiko werden, nicht zuletzt für den Datenschutz. › Schauen Sie, inwieweit es inzwischen digitale Formen gibt, wie beispielsweise Dongles. › Lassen Sie sich erläutern, welche personenbezogene Daten verarbeitet werden. Das gilt auch für klassische Schlüssellisten in Papierform.	☐ Ja ☐ Nein
Empfang	› Gerade in großen Unternehmen wird der Empfang oft durch die Unternehmenssicherheit gesteuert. › Prüfen Sie, inwieweit relevante Verarbeitungen bzw. Verarbeitungstätigkeiten im Verzeichnis von Verarbeitungstätigkeiten enthalten sind. Fehlen diese oder sind sie veraltet bzw. unvollständig, besteht für die Kollegen Handlungsbedarf. › Häufig kommen am Empfang viele Lösungen zum Einsatz, mit denen personenbezogene Daten verarbeitet werden. So z. B. Systeme, mit denen etwas verwaltet wird. Denken Sie aber auch an Papierlisten, die noch geführt werden. Auch hier darf Datenschutz nicht auf die leichte Schulter genommen werden. › Beim Empfang bietet sich stets ein Vor-Ort-Besuch an. Auch wenn vieles in der Theorie geregelt ist und seine Ordnung hat, kann das im Tagesgeschäft ganz anders aussehen.	☐ Ja ☐ Nein


CHECKLISTE: Bestandsaufnahme Unternehmenssicherheit

Besuchermanagement	› Nicht selten werden hier Softwarelösungen eingesetzt. Schauen Sie, welche personenbezogenen Daten von Besuchern verarbeitet werden. Klären Sie den verfolgten Zweck und die entsprechende Rechtsgrundlage. › Legen Sie ferner einen Fokus auf die Erforderlichkeit der erfassten Daten. Nicht selten werden mehr Daten erfasst als nötig. Das können auch Kopien von Ausweisen oder Führerscheinen sein. › Haben Sie ein Auge auf das Alter der Daten. Meist fällt der Zweck der Verarbeitung schnell weg, sodass kein Grund mehr für eine weitere Verarbeitung besteht. Die Daten müssen dann gelöscht werden.	☐ Ja ☐ Nein
Verwaltung von Lieferanten, Handwerkern und Fremdbeschäftigten	› Hierbei handelt es sich um eine Besuchergruppe mit Besonderheiten. Eventuell nimmt man es hier etwa im Hinblick auf Zutrittsberechtigungen oder Begleitung und Beaufsichtigung nicht so genau. › Sprechen Sie kritische Bereiche an und wie man hier sicherstellt, dass Unbefugte keinen Zutritt haben. So muss etwa ein Servicetechniker für die Kaffeemaschine keinen Zutritt zu sicherheitsrelevanten Bereichen, etwa zur „Chefetage“, zur Entwicklungsabteilung oder zum Serverraum, haben.	☐ Ja ☐ Nein
Einbindung von Dienstleistern im Bereich Personal- und Securitydienstleistungen	› Klären Sie, inwieweit Aufgaben ausgelagert wurden. So kann ggf. der Empfang oder die Pforte mit dem Personal eines Sicherheitsdienstleisters besetzt sein. Doch auch in diesem Fall ist und bleibt Ihr Unternehmen für den Datenschutz bzw. für die Sicherheit der von ihm verantworteten Verarbeitungen personenbezogener Daten datenschutzrechtlich verantwortlich. › Lassen Sie sich Vereinbarungen zum Datenschutz vorlegen. Wurde zum Thema Datenschutz überhaupt nichts vereinbart, muss hier nachgesteuert werden. › Gerade bei eingesetztem Fremdpersonal muss sichergestellt sein, dass dieses dennoch Bescheid weiß, wie der Datenschutz in Ihrem Unternehmen organisiert ist, welche Regeln gelten und was beachtet werden muss.	☐ Ja ☐ Nein
Einbruchschutz	› Hier können Sie sich die verwendete Technik erklären lassen. Schauen Sie, inwieweit sie noch auf der Höhe der Zeit ist und auch tatsächlichen Schutz bietet. So bringen gesicherte Fenster wenig, wenn sich das Türschloss mit einer Büroklammer öffnen lässt. › Gerade bei modernen Einbruchmeldesystemen kann es zu Verarbeitungen personenbezogener Daten kommen, die nicht auf Anhieb erkennbar sind. So kann es Raumpläne, Notfall- und Kontaktlisten geben, die meist auch Personenbezug aufweisen.	☐ Ja ☐ Nein
Einsatz von Videoüberwachung	› Der Einsatz von Überwachungskameras ist typischerweise Thema der Unternehmenssicherheit. Klären Sie hier die Rahmenbedingungen für deren Einsatz sowie die datenschutzrechtliche Zulässigkeit. › Schauen Sie sich konkret an, was überwacht wird. Nicht selten kommt es zu einem Datenschutzverstoß, weil zu viel erfasst wird oder Bilddaten zu lange gespeichert werden.	☐ Ja ☐ Nein
Parkraummanagement	› Eventuell ist diese Aufgabe den Kollegen zugewiesen. Klären Sie, welche Verarbeitungen mit personenbezogenen Daten es gibt. Machen Sie deutlich, dass auch personenbeziehbare Daten von Bedeutung sind, beispielsweise Kfz-Kennzeichen. Möglicherweise setzt man auf eine automatisierte Zufahrtskontrolle, bei der Kennzeichen erfasst werden. › Hinterfragen Sie hier insbesondere, welche Daten für welchen Zweck erfasst werden, warum dies erlaubt ist und wann die Daten gelöscht werden.	☐ Ja ☐ Nein
Besonderer Schutz von Sachwerten	› Eventuell wird bei der Unternehmenssicherheit so manches verwahrt, was besonderen Schutzes bedarf. Denken Sie etwa an Unterlagen oder Datenträger. Ggf. verfügt man über besonders gesicherte Räume oder Tresore. Doch auch hier müssen Sicherheit und Zutrittschutz gewährleistet sein. › Schauen Sie sich etwa Listen mit Berechtigungen an. Finden Sie Personen, die nicht mehr im Unternehmen sind, sollten Sie einen Aktualitätscheck empfehlen.	☐ Ja ☐ Nein
Kontrollmaßnahmen	› Denken Sie hier beispielsweise an Taschen- und Torkontrollen, die meist von der Unternehmenssicherheit verantwortet werden. Klären Sie, wie man vorgeht und wie man eine unzumutbare Beeinträchtigung des Persönlichkeitsrechts bei kontrollierten Personen vermeidet. › Für Kontrollmaßnahmen bestehen häufig Betriebsvereinbarungen, weil Fragen der betrieblichen Ordnung mitbestimmungspflichtig sind. Schauen Sie einerseits, ob etwa Beschränkungen umgesetzt sind. Andererseits darf die Betriebsvereinbarung selbst nicht hinter dem Mindeststandard der DSGVO zurückbleiben, wenn es um die Verarbeitung personenbezogener Daten geht.	☐ Ja ☐ Nein
Notfall- und Katastrophenmanagement	› Nicht selten finden sich bei Unternehmenssicherheit oder Empfang entsprechende Pläne oder Listen für den Fall der Fälle. Diese umfassen oft auch personenbezogene Daten. › Prüfen Sie, wie man die entsprechenden Dokumente sicher verwahrt.	☐ Ja ☐ Nein



Diese Punkte sind entscheidend für Taschenkontrollen am Firmmentor

Viele Unternehmen können ein Lied davon singen: Manche Mitarbeiter nehmen es mit dem Eigentum nicht so genau. Und schnell stellt man im Warenbestand fest, dass wohl der eine oder andere Mitarbeiter zum Langfinger wurde. Um dem Einhalt zu gebieten, kommen vielleicht auch die Kollegen in Ihrem Unternehmen auf die Idee, Taschen und Ähnliches am Firmmentor zu kontrollieren.

Machen Sie den Check

Egal, ob die Kollegen Sie um Ihren Rat fragen oder ob Sie eine Kontrolle durchführen wollen: Weil es bei Taschenkontrollen einiges zu beachten gilt, können Sie auf die folgende Checkliste setzen.

 CHECKLISTE: Relevante Fragen bei Taschenkontrollen		
Zu klären	Erläuterungen	Geklärt und in Ordnung?
Welche Festlegungen gibt es bereits?	Bestehen Sie auf die Vorlage entsprechender Unterlagen. Gibt es noch keine, sollten diese unverzüglich erstellt werden. Das Geregelte ist auch Maßstab für Ihre Bewertung als Datenschutzbeauftragter.	☐ Ja ☐ Nein
Wer ist für die Kontrollen verantwortlich, wer ist für sie zuständig?	Wenn das etwa aus einer Arbeitsanweisung nicht hervorgeht, muss hier unbedingt eine Festlegung getroffen werden. Nur wer verantwortlich ist, wird schon im Eigeninteresse ein Auge darauf haben, dass geltende Regeln eingehalten werden.	☐ Ja ☐ Nein
Sind die betreffenden Mitarbeiter für das richtige Vorgehen sensibilisiert bzw. geschult?	Lassen Sie sich erläutern, wie die kontrollierenden Kollegen damit vertraut gemacht wurden, wie sie vorgehen dürfen und was sie keinesfalls tun dürfen. Meist ist eine praxisnahe Schulung am besten. Klären Sie auch, wie sichergestellt wird, dass die Kontrollen vertraulich behandelt werden.	☐ Ja ☐ Nein
Inwieweit ist der Betriebsrat involviert?	Solche Kontrollen sind regelmäßig mitbestimmungspflichtig (§ 87 Abs. 1 Nr. 1 Betriebsverfassungsgesetz (BetrVG)). Es muss also vor Beginn der Kontrollen eine Betriebsvereinbarung geschlossen werden. Hier muss dann der Arbeitgeber dafür sorgen, dass das Festgelegte umgesetzt wird (§ 77 Abs. 1 BetrVG). Das ist nicht Sache des Datenschutzbeauftragten.	☐ Ja ☐ Nein
Auf welche rechtliche Basis soll die Kontrollmaßnahme gestützt werden?	Hinterfragen Sie die Rechtsgrundlage. Die sollte man Ihnen nennen können. Geht es etwa um Beschäftigte und sind allgemeine Kontrollen nach dem Zufallsprinzip angedacht, ist § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG) die richtige Hausnummer. Geht es um das konkrete Aufdecken einer von einem Mitarbeiter begangenen Straftat, liegen Sie mit § 26 Abs. 1 Satz 2 BDSG richtig.	☐ Ja ☐ Nein
Wie werden die Persönlichkeitsrechte der zu kontrollierenden Personen möglichst gering beeinträchtigt?	Lassen Sie sich erklären, wie man konkret die Kontrolle gestalten will. Das beginnt schon mit der Auswahl nach dem Zufallsprinzip. Ferner müssen die Kontrollen so durchgeführt werden, dass es zu keiner Stigmatisierung kommt, wenn etwa der Tascheninhalt geprüft wird. Dazu ist die Kontrolle in einem Nebenraum durchzuführen.	☐ Ja ☐ Nein
Inwieweit sind körpernahe Kontrollen vorgesehen?	Ein Abtasten lässt sich meist nicht rechtfertigen. Auch auf Basis einer Einwilligung klappt das nicht, weil diese eher unfreiwillig gegeben wird, sodass sie unwirksam erklärt worden wäre. Besteht ein konkreter Verdacht, dass etwas am Körper versteckt wird, sollte die Polizei hinzugezogen werden.	☐ Ja ☐ Nein
Wie geht man weiter vor, wenn sich ein Verdacht bestätigt bzw. nicht bestätigt?	Idealerweise gibt es konkrete Festlegungen zum weiteren Vorgehen. Achten Sie hier darauf, inwieweit das Vorgehen unter Vertraulichkeitsaspekten „schlank“ ist. So sollte intern das „Need-to-know-Prinzip“ konsequent umgesetzt werden.	☐ Ja ☐ Nein
Warum sind die Kontrollen bzw. ist das beabsichtigte Vorgehen insgesamt verhältnismäßig?	Bewerten Sie aus Sicht des Datenschutzbeauftragten, inwieweit das Vorgehen und die damit einhergehende Beeinträchtigung des Persönlichkeitsrechts von kontrollierten Personen verhältnismäßig sind. Hierzu muss das Vorgehen im Hinblick auf den Zweck geeignet, erforderlich und angemessen sein. Das gilt auch, wenn es zur Verarbeitung personenbezogener Daten kommt.	☐ Ja ☐ Nein
Wie werden Betroffenenrechte erfüllt?	Besondere Relevanz hat hier der Aspekt Transparenz. Die Mitarbeiter müssen vorab informiert werden, was es mit den Kontrollen auf sich hat. Gibt es Regelungen oder eine Betriebsvereinbarung, müssen diese kommuniziert werden. Bezüglich der Verarbeitungen ist Art. 13 Datenschutz-Grundverordnung zu beachten.	☐ Ja ☐ Nein

„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



DATENSCHUTZ LEICHT GEMACHT: IHRE ONLINE-WEITERBILDUNG 2025

REFERENTEN

Kristin Benedikt: Datenschutzexpertin und Richterin am Verwaltungsgericht Regensburg

Dr. Jens Eckhardt: Rechtsanwalt und Fachanwalt für Informationstechnologierecht

Bernd Fuhlert: TÜV-zertifizierter Datenschutzbeauftragter

Michael Rohrlisch: Rechtsanwalt, Fachautor, Dozent und Video-Trainer

WEBINARE

VON 10:00 BIS 11:00 UHR

24.04.2025 "Praxis-Guide Verfahrensübersicht: Direkt anwendbare Strategien für Datenschutzbeauftragte"
mit Bernd Fuhlert

21.05.2025 "Arbeitszeiterfassung und Datenschutz: Rechtssicher beraten – praxisnah umsetzen"
mit Kristin Benedikt

26.06.2025 "DSGVO-Grundsätze – warum Art. 5 DSGVO die zentrale Datenschutz-Norm ist"
mit Michael Rohrlisch

Sichern Sie sich jetzt Ihre Teilnahme unter:
<https://www.privacyxperts.de/shop/>





Telefon: 02 28 95 50 150

Fax: 02 28 36 96 480

E-Mail: kundendienst@privacyxperts.de

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