Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT

November 2020

Bild: iStock.com/NicoElNino

Mittlerweile liegen einige Äußerungen von Datenschutzaufsichtsbehörden zu Schrems II vor. Wirklich konkret werden die wenigsten.

Nicht erfüllbare Forderungen des EuGH?

„Zusätzliche Maßnahmen" bei Standardvertragsklauseln

In der Entscheidung „Schrems II" hält der EuGH Datenübermittlungen in die USA auf Basis der EU-Standardvertragsklauseln weiterhin für möglich. Allerdings fordert er „zusätzliche Maßnahmen". Der Beitrag diskutiert, was das Gericht damit meinen könnte.

Für Datenübermittlungen in die USA scheint „Schrems II" zumindest einen rechtlichen Hoffnungsschimmer zu bieten. Völlig verworfen hat der EuGH nur den Privacy Shield (Urteil des Europäischen Gerichtshofs (EuGH) vom 16.7.2020 – C-311/18, abrufbar unter https://ogy.de/eugh-entscheidung-schremsII). Er war ein Regelungswerk speziell für Datenübermittlungen in die USA.

1. Was ist die Besonderheit der Standardvertragsklauseln?

Gegen die Standardvertragsklauseln der Europäischen Kommission hat der EuGH dagegen vom Grundsatz her nichts einzuwenden. So der amtliche Leitsatz 4 der Entscheidung „Schrems II": „Die Prüfung … hat nichts ergeben, was [ihre] Gültigkeit berühren könnte."

Die Klauseln sind enthalten im Beschluss 2010/87/EU vom 5.2.2010 (abrufbar unter https://ogy.de/standardvertragsklauseln).

Ihre Besonderheit: Sie sind nicht speziell für Datenübermittlungen in die USA konzipiert. Vielmehr bieten sie eine mögliche Rechtsgrundlage für Datenübermittlungen in alle Drittländer außerhalb der EU. Sie können ein unzureichendes Datenschutzniveau im Zielland einer Datenübermittlung ausgleichen.

Damit scheinen sie wie dafür gemacht, als Rechtsgrundlage für Datenübermittlungen in die USA zu dienen. →

TITEL
01 „Zusätzliche Maßnahmen" bei Standardvertragsklauseln

SCHULEN & SENSIBILISIEREN
05 Datenschutz bei Zoom

BEST PRACTICE
07 Datenschutz im BGM

NEWS & TIPPS
11 Datenschutzaufsicht in Deutschland
12 Ersetzendes Scannen
12 Schrems II und die Folgen
12 Erklärvideo „Recht am eigenen Bild"
12 „Mitarbeiter-Exzess" bei Abfragen am Arbeitsplatz

BERATEN & ÜBERWACHEN
13 Fehlzeiten datenschutzkonform erfassen (Beispiele)
15 Bring your own Device
18 BVerfG: Hürden für Eingriffe in die Privatsphäre zu niedrig

DATEN-SCHLUSS
20 Wenn die Polizei schneller als „der Datenschutz" ist …

Editorial

Ricarda Veidt,
Chefredakteurin

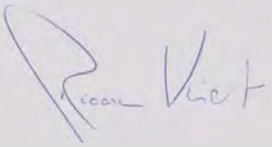
Erste Ausblicke

Liebe Leserin, lieber Leser! Auch wenn seit März alles anders läuft, als man es sich einmal gedacht hat: Weihnachten kommt bestimmt, und auch das neue Jahr. Der digitale Herbstkongress des BvD e.V. gab einigen Aufsichtsbehörden die Gelegenheit, einen Ausblick auf 2021 zu geben.

Danach stehen der Ausbau der Abstimmungsprozesse sowie eine einheitlichere Sanktionspraxis auf EU-Ebene auf der Agenda, ebenso der Start bei Zertifizierungsverfahren. Wohl eher nicht in die Gänge kommen wird die ePrivacy-Verordnung. Das Bayerische Landesamt für Datenschutzaufsicht sieht Schwerpunkte u.a. darin, Lösungen für Alltagsthemen wie Office 365 und Videokonferenztools zu finden, aber auch zu prüfen, wie es um das dauerhafte Datenschutz-Management steht: Aktualisieren Unternehmen z.B. ihre Datenschutz-Folgenabschätzungen regelmäßig?

Darüber hinaus ließ eine Zahl aus Baden-Württemberg aufhorchen: 2020 haben sich dort die Geldbußen um 50 % im Vergleich zum Vorjahreszeitraum erhöht. Ob sich diese Tendenz fortsetzt?

Bleiben Sie gesund!
Ihre Ricarda Veidt



2. Welche Tücken ergeben sich bei näherem Hinsehen?

Den Privacy Shield ließ der EuGH aus zwei Gründen scheitern (siehe Ehmann, Datenschutz PRAXIS 8/2020, Seite 1, Frage Nr. 8):

- Die Überwachungsprogramme der USA für das Internet nehmen keine Rücksicht darauf, ob die Überwachung im konkreten Einzelfall verhältnismäßig ist oder nicht.
- Betroffene Personen haben im Ergebnis keine Möglichkeit des Rechtsschutzes gegen eine solche Überwachung – es sei denn, sie sind US-Bürger.

Diese beiden Argumente zielen auf die Befugnisse von US-Behörden und auf den fehlenden Rechtsschutz gegen ihre Maßnahmen. Damit lassen sie sich auch nicht einfach ausblenden, wenn ein Verantwortlicher die Standardvertragsklauseln verwenden will. Denn wie der Begriff „Vertragsklauseln" nahelegt, bilden diese Klauseln den wesentlichen Inhalt eines Vertrags zwischen einem Datenexporteur in der EU und einem Datenimporteur in einem Drittland (beispielsweise in den USA).

Regelungen eines Vertrags binden jedoch immer nur die Vertragsparteien, hier also den Datenexporteur und den Datenimporteur. Sie sind kein geeignetes Instrument, um Befugnisse von Behörden einzuschränken oder Möglichkeiten des Rechtsschutzes gegenüber Behörden herzustellen. Diese Behörden sind schlicht und einfach keine Parteien des Vertrags (so Schrems II, Rn 125). Er berührt ihre Befugnisse nicht.

Damit war für den EuGH klar, dass Standardvertragsklauseln allein eine Datenübermittlung in die USA nicht legitimieren können. Da sie an der rechtlichen Situation in den USA nichts ändern, können sie kein angemessenes Schutzniveau für die betroffenen Personen herstellen.

Die logische Konsequenz: Wer auf der Basis der Standardvertragsklauseln Daten in die USA übermittelt, muss als Verantwortlicher „zusätzliche Maßnahmen" ergreifen. Nur die Vertragsklauseln plus solche zusätzlichen Maßnahmen führen zum gebotenen Datenschutzniveau (Schrems II, Rn 139). Siehe dazu schon ausführlich Ehmann, Datenschutz PRAXIS 8/2020, Seite 1, Fragen Nr. 6 bis Nr. 9.

3. Wie erläutert der EuGH die Formulierung „zusätzliche Maßnahmen"?

Im Ergebnis überhaupt nicht! Der EuGH nimmt zwar dazu Stellung, was ein in der EU ansässiger Verantwortlicher tun muss, wenn er solche „zusätzlichen Maßnahmen" nicht ergreifen kann (Aussetzung oder Beendigung der Übermittlung in den Drittstaat, also etwa in die USA – siehe Schrems II, Rn 135).

Auch erwartet der EuGH von einem Verantwortlichen, der Daten in ein Drittland wie die USA übermitteln will, dass er die Datenschutzgesetze dieses Landes zuvor genau analysiert. Dabei muss sich der Verantwortliche „vergewissern, dass das Recht des … [Drittlands] es dem Empfänger [der Daten] erlaubt, die Standarddatenschutzklauseln … einzuhalten" (Schrems II, Rn 141). Mit welchen konkreten „zusätzlichen Maßnahmen" der Ver-

antwortliche sicherstellen könnte, dass sie zusammen mit den Standardvertragsklauseln ein ausreichendes Schutzniveau für die übermittelten Daten herstellen, verrät der Europäische Gerichtshof aber nicht.

4. Ist Hilfe von den Aufsichtsbehörden zu erwarten?

Ein Überblick dazu, was bisher an Äußerungen der Datenschutzaufsichtsbehörden vorliegt, fällt ernüchternd aus:

- Die deutsche Datenschutzkonferenz (DSK) hat bereits am 28.7.2020 eine Pressemitteilung veröffentlicht, die den Inhalt der Entscheidung knapp zusammenfasst. Sie ist abrufbar unter https://ogy.de/dsk-schrems2. Zu den Standardvertragsklauseln enthält sie unter Nr. 2 wenige Sätze.
- Der Europäische Datenschutzausschuss (European Data Protection Board) geht in seinen „Häufigen Fragen" zu Schrems II (veröffentlicht am 23. Juli 2020) unter Frage 10 mit vier Sätzen auf das Thema „zusätzliche Maßnahmen" ein. Der Text ist in der offiziellen englischen Fassung abrufbar unter https://ogy.de/edpb-faq-schrems. Die DSK hat eine deutsche Übersetzung erstellt. Sie findet sich hier: https://ogy.de/edpb-faq-schrems-deutsch.
- In seiner 37. Sitzung am 2. September 2020 hat der Europäische Datenschutzausschuss eine Task Force eingerichtet. Sie soll Empfehlungen ausarbeiten, die Verantwortliche und Auftragsverarbeiter bei der Umsetzung von „zusätzlichen Maßnahmen" unterstützen (siehe https://ogy.de/edpb-task-force). Ergebnisse liegen bisher nicht vor.
- Der Landesbeauftragte für den Datenschutz Baden-Württemberg hat eine Orientierungshilfe zu Schrems II vorgelegt. Die aktuelle Fassung („2. Auflage" mit Stand 7. September 2020) ist abrufbar unter https://ogy.de/oh-lfdi-bw. Auf Seite 11 bis 13 gibt das Dokument einige Hinweise zum Thema „zusätzliche Maßnahmen". Eine Abstimmung mit anderen Aufsichtsbehörden scheint nicht erfolgt zu sein.

5. Hilft es, ausschließlich anonymisierte Daten in die USA zu übermitteln?

Anonymisierte Daten fallen nicht in den Anwendungsbereich der Datenschutz-Grundverordnung (DSGVO). Gemäß Erwägungsgrund 26 Satz 5 zur DSGVO gelten die Grundsätze des Datenschutzes nicht für personenbezogene Daten, „die in einer Weise anonymisiert worden sind, dass die betroffene Person nicht oder nicht mehr identifiziert werden kann." Sie unterliegen daher auch nicht den Vorgaben der DSGVO für die Übermittlung von personenbezogenen Daten in ein Drittland wie die USA.

In der Regel wertlos

Daten sind jedoch nur dann anonymisiert, wenn weder der Verantwortliche selbst noch eine andere Person einen Personenbezug (wieder)herstellen können. Dies hebt Erwägungsgrund 26 Satz 3 zur DSGVO hervor. Auch wenn ausschließlich der Verantwortliche selbst den Personenbezug (wieder)herstellen könnte, sind Daten nicht anonymisiert, sondern nach wie vor personenbezogen.

Die Übermittlung von derart anonymisierten Daten in die USA ist für Unternehmen meist sinnlos. Sie sind für die Abwicklung von Geschäftsprozessen ohne Wert.

6. Hilft es, nur pseudonymisierte Daten zu übermitteln?

Daten sind nur unter folgenden Voraussetzungen als pseudonymisiert anzusehen (Art. 4 Nr. 5 DSGVO):

- Die Daten müssen so verarbeitet sein, dass sie „ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können".
- Diese zusätzlichen Informationen müssen gesondert aufbewahrt werden.
- Die zusätzlichen Informationen müssen außerdem „technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht →

einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden".

Pseudonymisierte Daten weiter personenbezogen

Pseudonymisierte Daten sind weiterhin personenbezogen, so sehr deutlich Erwägungsgrund 26 Satz 2 zur DSGVO. Wer keinen Zugriff auf die „zusätzlichen Informationen" hat, kann die pseudonymisierten Daten mit hoher Wahrscheinlichkeit keiner bestimmten Person zuordnen. Völlig ausgeschlossen ist eine solche Zuordnung aber nicht. Außenstehende können nicht abschätzen, über welche Mittel US-Behörden wie die National Security Agency (NSA) verfügen, um pseudonymisierte Daten doch einer bestimmten Person zuzuordnen.

Herausgabepflichten

Hinzu kommt, dass US-Behörden nach US-Recht sehr oft die Herausgabe der „zusätzlichen Informationen" verlangen können, mit deren Hilfe sie die Pseudonymisierung aufheben können. Solche Herausgabepflichten beziehen sich nach den Vorgaben des „CLOUD-Act" auch auf Daten innerhalb der EU, sofern US-Unternehmen in irgendeiner Art und Weise legal auf sie zugreifen können. Dazu genügt es, dass sie vertragliche Zugriffsrechte haben (zum „CLOUD-Act" siehe Ehmann, Datenschutz PRAXIS 9/2019, Seiten 13–15).

Auch keine sinnvolle Lösung

Die Pseudonymisierung allein stellt vor diesem Hintergrund wohl kaum eine ausreichende „zusätzliche Maßnahme" zu den Standardvertragsklauseln dar. Zudem ist eine Pseudonymisierung mit beträchtlichem Aufwand verbunden. Das macht sie für Unternehmen wenig attraktiv.

7. Hilft es, die Daten zu verschlüsseln?

Oft würde eine Verschlüsselung den Geschäftspartner in den USA gerade an dem hindern, was er laut Vertrag mit den Daten tun soll. Klassisches Beispiel ist die Nutzung eines Cloud-Dienstes für maschinelles Lernen in den USA. Hier soll der US-Geschäftspartner die übermittelten Daten auswerten, um den individuellen Lernfortschritt festzustellen. Das kann er nicht, wenn ihm eine Verschlüsselung den Zugriff auf den Dateninhalt verwehrt.

Ansonsten gilt für eine Verschlüsselung das, was oben zur Pseudonymisierung gesagt wurde. Verschlüsselte Daten sind rechtlich gesehen nämlich pseudonymisierte Daten. „Zusätzliche Informationen" im Sinn der Pseudonymisierung sind die Informationen, mit deren Hilfe eine Entschlüsselung möglich ist.

8. Hilft es, die Standardvertragsklauseln abzuändern?

Diesen Ansatz favorisiert der Landesbeauftragte Baden-Württemberg in seiner Orientierungshilfe (Seite 11–13). Das Vorgehen ist kompliziert und mit erheblichen Risiken verbunden. Das gilt auch dann, wenn die Klauseln „nur" um einen Anhang ergänzt werden. Unternehmen ohne erfahrene Rechtsabteilung und ohne Datenschutz-Anwalt sollten davon schlicht die Finger lassen. Der Text aus Baden-Württemberg ist keine „abschreibefertige Vorlage", die juristische Laien benutzen könnten. Jede Veränderung an einem komplexen Vertragstext wie den Standardvertragsklauseln kann im konkreten Fall Fernwirkungen nach sich ziehen, die unerwartet gefährlich sind. Dieses Risiko ist ohne qualifizierte juristische Unterstützung nicht beherrschbar.

Die Klauseln bleiben ein Vertrag

Alle Modifizierungen und Ergänzungen der Standardvertragsklauseln ändern im Übrigen nichts daran, dass sie als vertragliche Vereinbarung nur die am Vertrag beteiligten Parteien binden. Das Ziel, die hoheitlichen Befugnisse von US-Behörden durch die Änderung von Vertragsklauseln auszubremsen, ist deshalb von vornherein zum Scheitern verurteilt.

9. Hilft es, US-Geschäftspartner zu verpflichten, über behördliche Zugriffe zu informieren?

Das schlägt z.B. der Landesbeauftragte Baden-Württemberg bei der Ergänzung der Standardvertragsklauseln vor (siehe Seiten 11/12: „Ergänzung Anhang Klausel 5d i"). Ein solcher Ansatz mag aus deutscher Sicht sinnvoll wirken. Er blendet jedoch wichtige Besonderheiten des US-Rechts aus. Sie lassen sich an dem Begriff „gag order" festmachen.

Auch das ist keine Lösung

„Gag" bedeutet in diesem Zusammenhang nicht „Scherz" oder etwas Ähnliches, sondern „Knebel". Eine „gag order" ist also eine behördliche „Knebelverfügung", die den Adressaten zum Schweigen zwingt. Das bedeutet grob skizziert:

Bestimmte US-Behörden können mit einem „National Security Letter" die Herausgabe von Daten anordnen. Rechtsgrundlage hierfür ist häufig „Section 702 FISA Act". Darauf geht der EuGH in „Schrems II" mehrfach ein (siehe dort etwa Rn 178–181). Eine solche Anordnung wird regelmäßig mit einer „gag order" verbunden. Sie untersagt es dem Adressaten der Anordnung, ihre Existenz nach außen zu erwähnen. Verstößt er gegen die „gag order", hat er mit erheblichen Konsequenzen zu rechnen. Unter Umständen ist sogar eine Haftstrafe denkbar.

National Security Letters, verbunden mit einer „gag order", ergehen in den USA jedes Jahr viele tausendmal. Kein Geschäftspartner in den USA wird es wagen, gegen eine „gag order" zu verstoßen. Informationspflichten vertraglich zu vereinbaren, läuft deshalb ins Leere.

10. Wie geht es weiter?

Von zentraler Bedeutung ist es, wie sich die erwähnte Taskforce des Europäischen Datenschutzausschusses äußern wird. Zu hohe Erwartungen sollte man dabei nicht haben. Die Vorgaben des EuGH in „Schrems II" sind eng und lassen nur wenig Spielräume. Einfache Lösungen „zum Abschreiben" sind nicht zu erwarten.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken und dem Datenschutz in Unternehmen und Behörden seit Jahren verbunden.

Bild: iStock.com/Andrei Stanescu

Eine wichtige Sicherheitsmaßnahme: Auf den Endgeräten sollte immer der aktuellste Zoom-Client zum Einsatz kommen, zu finden unter zoom.us/download.

Videokonferenz-Tools

So lässt sich der Datenschutz bei Zoom verbessern

Webdienste für Videokonferenzen und Teamarbeit sind besonders anfällig für mehr oder weniger große Lücken bei Datenschutz und Datensicherheit. Lesen Sie Tipps, wie sich der Datenschutz bei Zoom optimieren lässt, und geben Sie sie in Schulungen weiter.

Derzeit lässt sich weder mit Zoom noch mit einem anderen bekannten Anbieter für Videokonferenzen ein hundertprozentiger Datenschutz erreichen. Das gilt für Zoom genauso wie für Google Meet, GoToMeeting, Blizz, Cisco WebEx, Microsoft Teams und Skype. Generell ist lediglich Cisco WebEx halbwegs datenschutzkonform zu nutzen – allerdings nur dann, wenn die Buchung über die Deutsche Telekom läuft.

Die Situation hat sich mit dem Schrems-II-Urteil des Europäischen Gerichtshofs (EuGH) nicht verbessert. Denn ohne das Privacy Shield, das der EuGH gekippt hat, ist in den meisten Fällen eine Datenübermittlung in die USA schlicht unzulässig.

Kritik der Datenschützer

Schon vor dem EuGH-Urteil hatte der Bundesdatenschutzbeauftragte Ulrich Kelber davor gewarnt, Zoom einzusetzen. Er kritisierte v.a. die Verschlüsselung des Dienstes. Erst nach einigem Druck hat Zoom nachgegeben und will sicherstellen, dass alle Anwender in Zoom eine Ende-zu-Ende-Verschlüsselung nutzen können.

Auch die Berliner Datenschutzbeauftragte kritisiert den Datenschutz bei Zoom und anderen Plattformen. Die Landesdatenschutzbeauftragten empfehlen derzeit Plattformen wie Jitsi Meet, Tixeo Cloud, BigBlueButton, Wire oder sichere-videokonferenz.de. Wie gut diese Lösungen die eigenen Anforderungen abdecken, muss jeder Verantwortliche für sich entscheiden.

Grundlegende Sicherheitseinstellungen

Wer trotzdem aus verschiedenen Gründen – u.a. mangels leistungsfähiger Alternativen – auf Zoom setzt, sollte einige grundlegende Sicherheitseinstellungen beachten, um keine unnötigen zusätzlichen Sicherheitslücken und Datenschutzpannen zu produzieren.

Sicheres Kennwort vergeben

Wer eine Videokonferenz erstellt, muss v.a. Wert auf ein sicheres Kennwort legen. Generell lassen sich Konferenzen auch ohne Kennwort anlegen. Allerdings besteht in diesem Fall die Gefahr eines „Zoom-Bombing“: Dabei betreten unberechtigte Personen ein Meeting, das nicht durch ein Kennwort geschützt ist. Stehen in diesem Fall auch noch heikle Daten zur Diskussion, lassen sich die Auswirkungen bezüglich des Datenschutzes erahnen. Aus diesem Grund ist es wichtig, Meetings gleich im ersten Schritt davor zu schützen, dass sich unberechtigte Personen aufschalten.

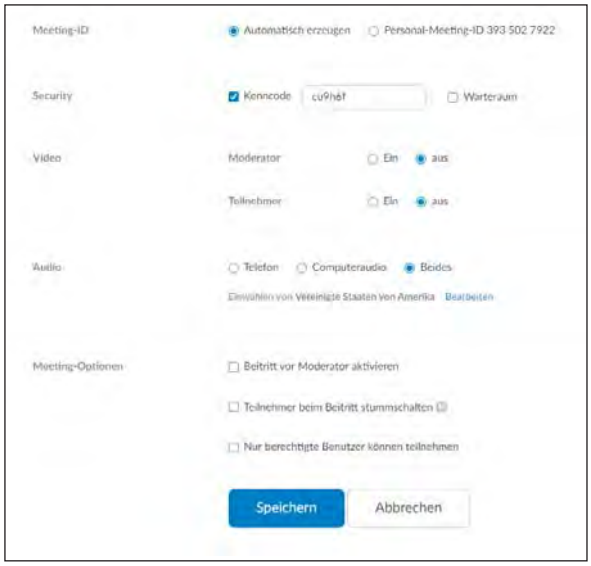
Warteraum aktivieren

Eine weitere wichtige Option beim Erstellen eines Meetings ist „Warteraum aktivieren“ unter „Meeting-Optionen“. Die Option stellt sicher, dass alle neuen Teilnehmer zunächst im sicheren Warteraum positioniert werden, bis der Moderator sie aktiv in das Meeting einlässt.

Wer als Moderator einen Warteraum angelegt hat, kann Teilnehmer zudem jederzeit in den Warteraum verschieben, wenn z.B. nicht alle Teilnehmer bestimmte Informationen mitbekommen sollen.

Sicherheit von Meetings steuern

Grundsätzlich sollte niemand die URL von Meetings veröffentlichen, auch dann nicht, wenn ein Kennwort und ein Warteraum vorhanden sind. Nach dem Erstellen eines Meetings steht für Moderatoren bzw. Administratoren der Bereich →



Wichtige Sicherheitsoptionen lassen sich bereits beim Erstellen eines Meetings festlegen

„Security" in den „Einstellungen" zur Verfügung. Hier lassen sich verschiedene Optionen nutzen, um die Sicherheit in Zoom zu verbessern.

Im Meeting-Client steht nach dem Start des Meetings der Bereich „Sicherheit" zur Verfügung. Hier kann der Moderator über „Meeting sperren" festlegen, dass kein neuer Teilnehmer am Meeting teilnehmen kann, auch dann nicht, wenn er die URL und das Kennwort kennt. Hier kann der Moderator außerdem unterbinden, dass Teilnehmer ihren Bildschirm freigeben oder Nachrichten in den Chat schreiben.

Im Zoom-Client lässt sich über das kleine rechte Icon oben links auf der Seite überprüfen, ob das Meeting optimal verschlüsselt wird (AES-256-GCM) und ob ein deutsches Rechenzentrum das Meeting bereitstellt.

Mehr Sicherheit in Pro, Business und Enterprise

Unternehmen, die Zoom häufiger einsetzen, sollten sich für ein Abonnement mit den Editionen Pro, Business und Enterprise entscheiden. Hier stehen deutlich mehr Sicherheitsoptionen zur Verfügung.

Zunächst kann ein Administrator des Abonnements für alle Meetings in diesem Konto zentral Sicherheitseinstellungen vorgeben. Bei „Benutzerverwaltung" und „Gruppenverwaltung" kann er Benutzerkonten und Rechte für diese Benutzer anlegen. Auch hier steht der Bereich „Sicherheit" zur Verfügung, der für alle Meetings gilt, die in diesem Abonnement durchgeführt werden. Hier lassen sich z.B. Kennwortregeln definieren.

Sichere Passwörter

Im Darknet sind eine halbe Million Kennwörter von Zoom-Benutzern aufgetaucht. Hier haben Benutzer die gleichen Kennwörter verwendet wie bei anderen Diensten im Internet, die offensichtlich gehackt wurden. Greifen Hacker mit den Kontodaten auf Meetings und deren Daten zu, besteht die massive Gefahr, dass personenbezogene Daten, aber auch Geschäftsgeheimnisse verloren gehen. Aus diesem Grund sollten die Nutzer bei Zoom nur sichere Kennwörter verwenden, die sie ansonsten bei keinen anderen Diensten nutzen.

Zugang nur für berechtigte Nutzer

Das Anlegen von Benutzerkonten macht es möglich, bei der Erstellung von Meetings die Option „Nur berechtigte Benutzer können teilnehmen" zu setzen. Das stellt sicher, dass keine unbefugten Personen auf ein Meeting und die dazugehörigen Daten zugreifen können.

Zwei-Faktor-Authentifizierung verwenden

Setzen Unternehmen dauerhaft auf Zoom, sollte die IT neben den Benutzerkonten in den erweiterten Sicherheitseinstellungen von Business, Pro oder Enterprise zentral definieren, dass sich Anwender mit der Zwei-Faktor-Authentifizierung anmelden müssen.

Anschließend können sich Anwender an Zoom anmelden und müssen entweder eine Authenticator-App installieren oder die Zwei-Faktor-Authentifizierung per SMS aktivieren. Das stellt sicher, dass keine unberechtigten Anwender Zugriff auf ein Konto erhalten.

Aufzeichnung von Meetings steuern

Bei der Erstellung eines Meetings und in den Admin-Optionen von Zoom lässt sich bei „Aufzeichnung" festlegen, ob Teilnehmer das komplette Meeting lokal aufzeichnen können oder ob ein Meeting automatisch aufgezeichnet und die Daten in der Cloud gespeichert werden.

Hier sollte das Unternehmen sicherstellen, dass die Einstellungen den Datenschutz-Richtlinien entsprechen. Es ist klar, dass das lokale Aufzeichnen von Meetings höchst problematisch ist. Ist diese Option auf Ebene der Administratoren in Pro, Business und Enterprise zentral deaktiviert, können Anwender diese Option in den Einstellungen von Meetings bei „Aufzeichnung" auch nicht mehr aktivieren.

Fazit: Konfigurationsmöglichkeiten ausschöpfen

Zoom bietet einiges an Verbesserungspotenzial in puncto Datenschutz. Setzt Ihr Unternehmen auf Zoom, sorgen Sie z.B. durch Schulungen dafür, dass Moderatoren und Administratoren die Datenschutzeinstellungen so gut wie möglich konfigurieren. Das gilt auch für die Ende-zu-Ende-Verschlüsselung. Empfehlen Sie die Editionen Pro, Business und Enterprise. Denn nur hier lassen sich alle Optionen so setzen, dass Datenschutz und Datensicherheit soweit in diesem Zusammenhang möglich gewährleistet sind.

PRAXIS-TIPP

Und nicht zuletzt gilt wie immer: Datenminimierung! Also möglichst wenige personenbezogene Daten über ein Videokonferenz-Tool preisgeben und z.B. überlegen, was man wirklich an Informationen hochladen muss.

Thomas Joos hat über 30 Jahre Berufserfahrung als IT-Consultant und Trainer.

Bild: iStock.com/AndreyPopov

Um ein passendes BGM-Konzept zu entwickeln, sind u.a. Überlegungen wichtig wie „Welche Ziele verfolgen wir?", „Welche Strukturen sind vorhanden?" und „Woher erhalte ich belastbare Daten für die Analyse?"

Beschäftigtendatenschutz

Datenschutz im betrieblichen Gesundheitsmanagement

Ein betriebliches Gesundheitsmanagement datenschutzkonform umzusetzen, ist zwar keine unlösbare Aufgabe, aber eine Herausforderung.

Die Gesundheit der Mitarbeiter ist ein wichtiger wirtschaftlicher Faktor. Unternehmen suchen vor diesem Hintergrund stets nach Möglichkeiten, einerseits die Kosten für Entgeltfortzahlungen zu verringern und andererseits durch diverse Maßnahmen für Beschäftigte attraktiv zu bleiben bzw. zu werden.

Was ist ein BGM?

Eine Möglichkeit, um die Gesundheit der Mitarbeiter zu verbessern bzw. Krankheitskosten zu reduzieren, ist, ein betriebliches Gesundheitsmanagement – kurz BGM – zu entwickeln. Dieses BGM ist per Definition die systematische und strukturierte Entwicklung, Planung und Lenkung betrieblicher Strukturen und Prozesse mit dem Ziel, die Gesundheit der Beschäftigten zu erhalten und zu fördern.

Es fasst alle betrieblichen Elemente zusammen, die einerseits dazu dienen, die Arbeits- und Organisationsgestaltung gesundheitsförderlich zu verändern (Verhältnisprävention) und andererseits dazu, die Beschäftigten zu einem gesundheitsförderlichen Verhalten zu befähigen (Verhaltensprävention).

Zwei zentrale Fragen

Ein BGM setzt sich in der Regel besonders mit diesen zwei Fragen auseinander:

1. Was hemmt, demotiviert, frustriert, macht krank?
2. Was fördert, motiviert, schafft Arbeitszufriedenheit, hält gesund?

Um Antworten auf diese Fragen zu formulieren, gilt es, solche Faktoren wie Mitarbeiterkompetenz, Mitarbeitergesundheit und den Arbeitsplatz im Allgemeinen mit all seinen Facetten – vom physischen Arbeitsplatz über die Arbeitsaufgabe bis hin zu den sozialen Beziehungen – genau zu analysieren.

Um eine solch diffizile Analyse vornehmen und geeignete Maßnahmen ableiten zu können, nutzen Unternehmen häufig das Prinzip „je mehr Informationen und Daten wir von Beschäftigten sammeln und auswerten, umso effizienter ist unser BGM". Nicht jedes Vorgehen ist hierbei mit dem Betriebsrat abgestimmt und (datenschutz)rechtlich einwandfrei. →

Die drei Säulen eines BGM

1. Säule: freiwillige Leistungen, die auf unternehmerischen Interessen aufbauen
2. Säule: gesetzliche Verpflichtungen zum Arbeits- und Gesundheitsschutz (Arbeitsschutzgesetz – ArbSchG)
3. Säule: betriebliches Eingliederungsmanagement (BEM, § 167 Abs. 2 Sozialgesetzbuch IX)

Diese drei Säulen sind sehr unterschiedlich ausgeprägt. In einem mittelständischen Metallbau-Unternehmen wird das BGM in der Regel anders aussehen als bei einer Stadtverwaltung. Ein Handwerksbetrieb wird das Thema BGM für sich anders interpretieren als ein Chemiekonzern mit tausenden Mitarbeitern und mehreren Produktionsstandorten.

ACHTUNG!

Bei der Verarbeitung von Gesundheitsdaten im Rahmen eines BGM greift die Wahrung von berechtigten Interessen des Verantwortlichen (Art. 6 Abs. 1 Buchst. f DSGVO) als rechtliche Begründung in der Regel nicht. Denn diese Vorschrift ist nicht auf die Verarbeitung von Gesundheitsdaten anwendbar.

Weitere Kriterien für die Freiwilligkeit einer Einwilligung

- **Die Beschäftigten müssen eine echte Wahlmöglichkeit haben.**
- **Es darf ihnen kein Nachteil entstehen, wenn sie keine Einwilligung erteilen oder sie widerrufen.**
- **Bei mehreren Verarbeitungsprozessen sollen Beschäftigte die Möglichkeit haben, für jeden einzelnen Prozess zu entscheiden, ob sie einwilligen.**
- **Die Einwilligung muss auf informierter Grundlage erfolgen.**
- **Die Beschäftigten müssen die Einwilligung jederzeit widerrufen können.**
- **Die Einwilligung muss eindeutig sein.**
- **Die Einwilligung muss in der Regel schriftlich erfolgen.**

Rechtmäßigkeit der Verarbeitung: Welche Rechtsgrundlage greift?

In fast jeder Phase des BGM verarbeiten Verantwortliche Daten, bei denen es sich in der Regel um personenbezogene Daten im Sinne von Art. 4 Nr. 1 Datenschutz-Grundverordnung (DSGVO) oder um Gesundheitsdaten im Sinne von Art. 4 Nr. 14 DSGVO handelt. Diese Daten zu erheben und zu bearbeiten, ist unabdingbar, um ein funktionierendes BGM zu entwickeln. Wichtig ist hierbei, die Grundsätze zur Verarbeitung von Gesundheitsdaten entsprechend den Vorschriften von Art. 9 DSGVO zu berücksichtigen. Denn prinzipiell ist deren Verarbeitung untersagt, es sei denn, es liegen bestimmte Voraussetzungen vor, die zu einer Verarbeitung berechtigen.

Ausnahmetatbestände nutzen

Um besondere Kategorien personenbezogener Daten – dazu gehören Gesundheitsdaten – rechtmäßig zu verarbeiten, lohnt sich ein Blick auf Art. 9 Abs. 2 DSGVO. Die dort angeführten Ausnahmen zum Verarbeitungsverbot (Art. 9 Abs. 1 DSGVO) sind grundlegend, wenn es um die Umsetzung des BGM geht. Hierbei sind im Wesentlichen folgende Ausnahmetatbestände zu betrachten:

- Es liegt eine Einwilligung des Beschäftigten vor (Art. 9 Abs. 2 Buchst. a DSGVO).
- Die Verarbeitung ist erforderlich, „damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann, …“ (Art. 9 Abs. 2 Buchst. b DSGVO).
- Die Verarbeitung ist erforderlich, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen (Art. 9 Abs. 2 Buchst. c DSGVO).
- Die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin bzw. für die Beurteilung der Arbeitsfähigkeit des Beschäftigten erforderlich. Diese Datenverarbeitung ist allerdings nur durch Fachpersonal oder unter dessen Verantwortung möglich (siehe Art. 9 Abs. 3 DSGVO).

Konkret lässt sich sagen, dass für bestimmte Elemente des BGM die Verarbeitung ohne Einwilligung untersagt ist, für andere – z.B. zur Beurteilung der Arbeitsfähigkeit der Beschäftigten oder zum Zweck der Gesundheitsvorsorge – ist sie wiederum grundsätzlich zulässig.

Zentral: Die Einwilligung – und die Anonymisierung

In der Regel können Sie allerdings davon ausgehen, dass Verantwortliche bei einem BGM viele Daten zur Beurteilung von Maßnahmen der Gesundheitsförderung nur über eine Einwilligung der Beschäftigten verarbeiten dürfen. Grundsätzlich gilt, dass eine Einwilligung nur als Rechtfertigung für eine Datenverarbeitung taugt, wenn die Beschäftigten diese Einwilligung freiwillig, informiert, auf einen konkreten Fall bezogen und unmissverständlich erklären.

§ 26 Abs. 2 Bundesdatenschutzgesetz (BDSG) regelt in Verbindung mit § 26 Abs. 3 Satz 2 BDSG, was bei der Beurteilung der Freiwilligkeit im Beschäftigungsverhältnis zu berücksichtigen ist. Ob Arbeitnehmer rechtswirksam in die Verarbeitung ihrer personenbezogenen Daten einwilligen können, ist seit Jahren umstritten. Im Rahmen eines BGM ließe sich anführen, dass der Beschäftigte einen rechtlichen oder wirtschaftlichen Vorteil erlangen kann, wenn er seine Einwilligung erteilt. Jedoch sind weitere Kriterien bei der Umsetzung wichtig.

PRAXIS-TIPP

Verantwortliche sollten jede Verarbeitungstätigkeit in einem BGM einzeln und für sich betrachten, die zu verarbeitenden Daten konkret definieren und die möglichen Ausnahmetatbestände von Art. 9 DSGVO individuell prüfen. Außerdem ist es vor diesem Hintergrund empfehlenswert, wo immer möglich, die Datenverarbeitung im Rahmen des BGM anonym zu gestalten.

Verarbeitungstätigkeiten im Rahmen eines BGM: Analyseverfahren

Verantwortliche verarbeiten im Rahmen eines BGM an vielen Stellen personenbezogene Daten. Das gilt besonders im Bereich der Analyse. Die Analysetätigkeiten lassen sich in der Regel in vier verschiedene Ebenen unterteilen:

1. Quantitativ-objektive Verfahren: z.B. Fehlzeiten-, Personalstruktur- und Altersstrukturanalyse, Gesundheitsbericht der gesetzlichen Krankenversicherungen
2. Qualitativ-objektive Verfahren: z.B. Arbeitsplatzanalysen, arbeitsmedizinische Untersuchungen, Fitness-Tracker
3. Quantitativ-subjektive Verfahren: z.B. Mitarbeiterbefragung
4. Qualitativ-subjektive Verfahren: z.B. Gesundheitszirkel mit Mitarbeiterinnen und Mitarbeitern sowie Führungskräften, Experteninterviews, Gender-Perspektivenwechsel

Zusätzlich fließen meist die Ergebnisse der Gefährdungsbeurteilung und die Rückmeldungen des Betriebsarztes in die Analyse ein.

Bei der Betrachtung der Datenschutzkonformität der verschiedenen Analyseverfahren in BGM-Verfahren gilt es zu klären, welche Daten üblicherweise verarbeitet werden (sollen). Exemplarisch seien zwei Analyseverfahren betrachtet:

- Mitarbeiterbefragungen sowie
- arbeitsmedizinische Untersuchungen und Gefährdungsbeurteilungen

Beispiel 1: Mitarbeiterbefragungen

In erster Linie dient eine Mitarbeiterbefragung dazu, Meinungen, Einschätzungen und Informationen von den Beschäftigten zu bestimmten Fragen – Motivation, Zufriedenheit, Problemen, Sorgen, Kritik etc. – zu erhalten. Somit kann eine Mitarbeiterbefragung ein gutes Instrument sein, um Analysen vorzunehmen und Maßnahmen im Rahmen eines BGM zu entwickeln. Hierzu müssen Mitarbeiterbefragungen gut vorbereit und die Fragen ausdrücklich auf das zu erreichende Ziel formuliert werden.

Die Verarbeitung der Daten aus der Mitarbeiterbefragung erfolgt in der Regel nicht zur Durchführung eines Beschäftigungsverhältnisses, sodass sich die rechtlichen Grundlagen von § 26 BDSG nicht heranziehen lassen.

Auch die Vorschriften von Art. 6 Abs. 1 Buchst. f DSGVO bieten keine ausreichende rechtliche Grundlage, um die Beschäftigtendaten im Rahmen einer Mitarbeiterbefragung zu verarbeiten. Das Interesse des einzelnen Mitarbeiters wiegt in der Regel schwerer als die Interessen des Arbeitgebers, auch wenn es im besonderen Interesse des Arbeitgebers liegt, bestimmte Informationen von und zu den Mitarbeitern zu erfassen und zu verarbeiten.

Da eine Verpflichtung, an der Mitarbeiterbefragung teilzunehmen, auszuschließen ist, verbleibt die Einwilligung des Arbeitnehmers auf Grundlage von Art. 6 Abs. Buchst. a DSGVO bzw. von Art. 9 Abs. 2 Buchst. a DSGVO bei Gesundheitsdaten. Dieses Instrument ist wiederum schwierig umzusetzen. Denn die Hürden für eine tatsächlich rechtswirksame Einwilligung im Arbeitsverhältnis sind sehr hoch.

Vor diesem Hintergrund empfiehlt es sich, die Mitarbeiterbefragung grundsätzlich anonym durchzuführen. Sind keine Rückschlüsse auf den einzelnen Arbeitnehmer möglich, können Verantwortliche die erhobenen Daten ohne Probleme nutzen. Denn hier findet die DSGVO keine Anwendung.

Beispiel 2: arbeitsmedizinische Untersuchungen und Gefährdungsbeurteilung

Bevor Mitarbeiter eine gefährdende Tätigkeit aufnehmen, sind Unternehmen nach der Verordnung zur arbeitsmedizinischen Vorsorge (ArbmedVV) verpflichtet, für diese Mitarbeiter eine arbeitsmedizinische Vorsorge anzubieten (Pflicht- und Angebotsvorsorge) bzw. vorzuhalten (Wunschvorsorge). Diese Untersuchungen werden in der Regel nach einiger Zeit wiederholt bzw. wiederholt angeboten.

Der Betriebsarzt soll über diese Untersuchungen feststellen, ob sich eine Beschäftigung ohne Bedenken verantworten lässt und sie die Gesundheit des Arbeitnehmers nicht gefährdet. Der Beschäftigte darf die Tätigkeit dann ausüben, wenn er an der Pflichtuntersuchung teilgenommen hat und der Betriebsarzt eine weitere Beschäftigung als unbedenklich bewertet.

Die Gefährdungsbeurteilung ist das Fundament, um festzustellen, für welche Tätigkeiten eine Pflichtuntersuchung erforderlich ist. Zum Beispiel ist das stets bei Arbeiten der Fall, bei denen der Arbeitnehmer mit einem Gefahrstoff, den die ArbMedVV angibt, in Kontakt gerät. Des Weiteren zeigt die Gefährdungsbeurtei- →

Wichtige Aspekte bei der Befragung

- **Freiwilligkeit der Teilnahme der Mitarbeiter gewährleisten (auch bei Anonymität).**
- **Mitarbeiterbefragung transparent gestalten: Wie wird sie durchgeführt? Wann findet sie statt? Was wird damit beabsichtigt? Wer ist in die Befragung eingebunden? Was passiert mit den Informationen?**
- **Belegschaft vor der Befragung über den Zweck und die Durchführung, die Anonymität etc. informieren.**
- **Während der Befragung über Ablauf und Umsetzung etc. informieren.**
- **Im Anschluss über die Auswertungen, die geplanten Maßnahmen etc. informieren.**
- **Anonymität der Befragung einhalten.**
- **DSB einbeziehen.**
- **Betriebsrat frühzeitig einbinden, um die Akzeptanz zu erhöhen.**

Zentrale Position

Die Rolle des Betriebsarztes im BGM

Der Betriebsarzt besitzt aufgrund seiner besonderen Rolle im Betrieb ein fundamentales Wissen über die gesundheitliche Situation der Mitarbeiter und die Gefährdungen an den jeweiligen Arbeitsplätzen. Bei seiner üblichen Tätigkeit im Betrieb verarbeitet er unvermeidlich umfassende Gesundheitsdaten der Beschäftigten. Daher kann er

- aufgrund der Informationen, die er durch seine Tätigkeit gewinnt, dem Unternehmen anonymisierte Hinweise geben, wie es Arbeitsplätze unter medizinischen Aspekten optimieren kann.
- Empfehlungen aussprechen, welche gesundheitsfördernden Maßnahmen dem Betrieb bzw. den Mitarbeitern helfen.
- aufgrund seiner zentralen Position an der Schnittstelle zwischen den Angestellten und dem Betrieb die notwendigen Gesundheitsprozesse am besten mit entwickeln, umsetzen und in der Folge begleiten.

Aus datenschutzrechtlicher Sicht ist der Betriebsarzt ein Teil des Unternehmens. Er nutzt die Gesundheitsdaten von Mitarbeitern, übermittelt sie jedoch nicht inhaltlich weiter. Er hat gegenüber dem Unternehmen seine ärztliche Schweigepflicht zu beachten, wenn er sich nicht nach § 203 Strafgesetzbuch (StGB) strafbar machen möchte.

Vor diesem Hintergrund kann auch der Betriebsarzt dem Unternehmen keine konkreten, sondern nur anonymisierte Daten zu den Mitarbeitern des Unternehmens zur Verfügung stellen. Trotzdem besteht für ihn die Möglichkeit, den Arbeitgeber bei einem BGM mit wesentlichen Informationen datenschutzkonform zu unterstützen.

lung gesundheitliche Gefahren und Risiken auf, die mit einem Arbeitsplatz gekoppelt sind. Im Rahmen dieses Prozesses erfolgen eine Aufklärung über die Präventionsmaßnahmen sowie eine ausführliche Beratung des Arbeitgebers.

Wie die ArbMedVV bestimmt, hat der Arbeitgeber über Pflichtuntersuchungen eine Vorsorgekartei zu führen. Sie enthält Angaben zum Anlass, zum Tag und zum Ergebnis der Untersuchungen. Dabei darf der Betriebsarzt ähnlich wie bei Eignungsuntersuchungen dem Arbeitgeber als Ergebnis nur allgemein mitteilen, ob Bedenken gegen die Beschäftigung bestehen oder nicht.

Die Verarbeitung dieser Daten erfolgt auf betriebsärztlicher Seite auf Grundlage von Art. 9 Abs. 2 DSGVO in Verbindung mit Art. 88 DSGVO und § 22 Abs. 1 Nr. 1b BDSG. Denn die Verarbeitung ist erforderlich „zum Zweck der Gesundheitsvorsorge“ und „für die Beurteilung der Arbeitsfähigkeit des Beschäftigten“.

Auf Arbeitgeberseite ist die Verarbeitung der Vorsorgekartei durch § 26 Abs. 3 Satz 1 BDSG legitimiert. Denn abweichend von Art. 9 Abs. 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

PRAXIS-TIPP

Die aufgeführten Beispiele zeigen, dass es möglich ist, personenbezogene Daten im Rahmen eines betrieblichen Gesundheitsmanagements zu verarbeiten, jedoch in der Regel anonymisiert. Es ist empfehlenswert, den Betriebsarzt in ein BGM einzubinden. Denn er ist häufig berechtigt, Gesundheitsdaten zu verarbeiten, und kann dem Unternehmen wertvolle Erkenntnisse in anonymisierter Form zur Verfügung stellen. Gesundheitsdaten im Rahmen von BGM auf Basis einer Einwilligung zu verarbeiten, sollten Verantwortliche aufgrund der hohen Anforderungen an eine wirksame Einwilligung nur in Einzelfällen in Betracht ziehen.

Arnd Fackeldey ist Geschäftsführer der Digital Compliance Consulting GmbH. Als DSB und Auditor unterstützt er Unternehmen dabei, Datenschutzprozesse einzuführen, sowie Datenschutzbeauftragte und Betriebsräte bei Kontrollaufgaben.

Datenschutzaufsicht in Deutschland

So viele Aufsichtsbehörden für den Datenschutz wie Deutschland hat kein anderer Mitgliedstaat der EU. Das ist schon seit Jahrzehnten so und liegt in erster Linie an der föderalen Struktur Deutschlands. Die Datenschutz-Grundverordnung (DSGVO) nimmt das so hin. Sie legt fest, dass es Sache der Mitgliedstaaten ist, die Aufsichtsbehörden für den Datenschutz einzurichten, und dass sie „eine oder mehrere" solche Behörden einrichten können (Art. 51 Abs. 1 DSGVO).

Gutachten der Datenethikkommission

In Deutschland hat gleichwohl eine Diskussion über die Struktur der Datenschutzaufsicht in Deutschland begonnen. Erster Auslöser dafür war das Gutachten der Datenethikkommission vom September 2019. In einem Kapitel „Bedarf nach einer Vereinheitlichung der Datenschutzaufsicht für den Markt" stellt es die Überlegung an, „die Datenschutzaufsicht … durch eine neue Behördenstruktur zu vereinheitlichen."

Zu denkbaren neuen Organisationsstrukturen heißt es: „Im Zuge seiner Zuständigkeit zur Regelung des Rechts der Wirtschaft könnte der Bund die Kompetenz der Datenschutzaufsicht über die Wirtschaft (nicht-öffentlicher Bereich) auf den Bundesbeauftragten für den Datenschutz und die Informationsfreiheit übertragen und diesen entsprechend ausstatten. Dieser könnte durch verschiedene Außenstellen eine Präsenz der Datenschutzaufsicht in der Fläche garantieren (ähnlich dem Bundesamt für Migration und Flüchtlinge oder der Bundesbank). Denkbar ist auch die Bildung einer gemeinsamen Einrichtung der Länder qua Staatsvertrag nach den Modellen etwa im Rundfunkbereich oder der gemeinsamen Zentralstellen der Länder für Sicherheitstechnik und Gesundheitsschutz." (Gutachten der Datenethikkommission vom September 2019, Seite 103, abrufbar unter https://ogy.de/gutachten-201909).

Stellungnahme des Bitkom

Nicht so weit geht der Bitkom in einer Stellungnahme vom September 2020. Er rügt zwar, dass gerade in Deutschland die Aufsichtsbehörden die DSGVO zum Teil recht unterschiedlich interpretieren würden: „Anstatt eines einheitlichen Rechtsrahmens sehen sich die Anwender heute aufgrund der unterschiedlichen Interpretation der 27 nationalen Datenschutzbehörden in den Mitgliedstaaten nach wie vor einem regulatorischen Flickenteppich in Europa ausgesetzt. Die Situation in Deutschland ist darüber hinaus zusätzlich verschärft, da mit 17 Landesdatenschutzaufsichtsbehörden und dem Bundesdatenschutzbeauftragten insgesamt 18 verschiedene Behörden für Interpretation und Durchsetzung der Datenschutzvorschriften zuständig sind." (Bitkom, Stellungnahme „Struktur der Datenschutzaufsichtsbehörden in Deutschland", September 2020 [Umfang 3 Seiten], Seite 1, abrufbar unter https://ogy.de/stellungnahme-bitkom).

Vielleicht in der Erkenntnis, dass sich bundesweite Änderungen von Behördenstrukturen nur sehr schwer durchsetzen lassen, erhebt er jedoch keine konkreten Forderungen in diese Richtung. Vielmehr verlangt er beispielsweise: „Die Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder (DSK) sollte … mehr bindende Guidelines herausgeben, sodass keine Abweichung in den Bundesländern mehr möglich ist. Die bisherigen Verfahren fördern einen Austausch, legen allerdings keine verpflichtenden Abstimmungsverfahren fest und resultieren daher nicht in einer einheitlichen Umsetzung der DS-GVO." (Bitkom, Stellungnahme, Seite 2).

Sollte Einheitlichkeit nicht gelingen, fürchtet der Bitkom gravierende Nachteile: „Die unterschiedliche Interpretation der DS-GVO durch die Behörden behindert Wachstum, da für jeden Geltungsbereich rechtlicher Rat eingeholt werden muss und evtl. Produkte verändert werden müssen. Rechtsunsicherheit führt zudem dazu, dass innovative Projekte gar nicht erst angegangen werden." (Bitkom, Stellungnahme, Seite 2).

Presse-Erklärung des BvD

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. vertritt die Meinung, entscheidend sei weniger eine föderale oder zentrale Struktur der Datenschutzaufsicht, sondern die einheitliche Anwendung der bestehenden Datenschutzgesetze (Pressemitteilung vom 23. September 2020, https://ogy.de/pm-aufsicht-bvd).

Und die Folgen für die Praxis?

Praktische Auswirkungen werden die Diskussionen auf absehbare Zeit nicht haben. Jedenfalls vor der Bundestagswahl im Herbst 2021 erscheint es ausgeschlossen, dass die Regelungen des Bundesdatenschutzgesetzes zur Datenschutzaufsicht geändert werden. Die politische Lage nach der Bundestagswahl kann noch niemand prognostizieren.

Bild: iStock.com/suksunt sansawast

RESISCAN

Ersetzendes Scannen von Dokumenten

Scannen Unternehmen oder Behörden Dokumente und vernichten sie die Originale dann, stellen sich zahlreiche Rechtsfragen. Der Datenschutz spielt dabei eine wesentliche Rolle. Maßgebliches Grundlagendokument ist die Technische Richtlinie (TR) 03138 des Bundesamts für Sicherheit in der Informationstechnik (BSI), bekannt unter der Kurzbezeichnung BSI TR-03138 Ersetzendes Scannen (RESISCAN).

Die umfangreichen Vorgaben umzusetzen, ist eine erhebliche Herausforderung. Deshalb hat das BSI das Papier „Ersetzendes Scannen leichtgemacht – eine Handlungshilfe für Institutionen und Unternehmen" veröffentlicht. Es befindet sich auf dem Stand vom 5.6.2020 und hat einen Umfang von 37 Seiten. Es ist zusammen mit der TR RESISCAN abrufbar unter https://ogy.de/bsi-resiscan.

Neue Diskussionspapiere

Schrems II und die Folgen

Die Diskussion um die Bewältigung der Folgen von Schrems II (Urteil des EuGH vom 16.7.2020 – C 311/18, siehe dazu in diesem Heft Ehmann, Seite 1–4) hält an:

- In einer gemeinsamen Stellungnahme fordern die Spitzenverbände der deutschen Wirtschaft schnell eine wirksame Nachfolge-Regelung zum Privacy Shield und das Aussetzen von Sanktionsmaßnahmen, bis Rechtsklarheit geschaffen ist. Das dreiseitige „Verbändepapier zum Schrems II-Urteil des EuGH/ Statement on the Schrems II ruling oft he ECJ" vom 22.9.2020 ist auf Deutsch und Englisch abrufbar unter https://ogy.de/verbaendepapier-schremsII.
- Ein Whitepaper (Umfang 23 Seiten, nur auf Englisch verfügbar) mit dem Titel „Information on U.S. Privacy Safeguards Relevant to SCCs and Other EU Legal Bases for EU-U.S.Data Transfers after Schrems II" will Quellen zur Verfügung stellen, die aus offizieller US-Sicht für die Diskussion wichtig sind. Es ist abrufbar unter https://ogy.de/us-whitepaper.

Datenschutzaufsicht Rheinland-Pfalz

Erklärvideo „Recht am eigenen Bild"

Ein Erklärvideo von knapp drei Minuten zum Themenkreis „Recht am eigenen Bild" bietet die Datenschutzaufsicht Rheinland-Pfalz. Es ist abrufbar unter https://ogy.de/rlp-recht-am-eigenen-bild. Dort findet sich auch eine umfangreiche schriftliche Darstellung. Sie behandelt beispielsweise das Fotografieren in Vereinen, Schulen und Kindertagesstätten, aber auch das Fotografieren im Rahmen eines Beschäftigungsverhältnisses.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken (Bayern). Er befasst sich seit vielen Jahren intensiv mit Fragen des Datenschutzes.

Geldbuße möglich oder nicht?

„Mitarbeiter-Exzess" bei Abfragen am Arbeitsplatz

Ein Polizist nutzt dienstliche Datenbanken, um für private Zwecke zu recherchieren. Beispiel: Er fragt mithilfe des Kennzeichens die Halterdaten eines Pkw ab und nimmt zu der Pkw-Halterin aus rein privaten Motiven Kontakt auf. Ist gegen ihn eine Geldbuße auf der Basis von Art. 83 DSGVO möglich?

Eigener Verantwortlicher?

Die Datenschutzaufsichtsbehörde Baden-Württemberg beantwortet diese Frage mit einem klaren Ja. Ihre Begründung: „Dieses Vorgehen stellte einen sog. Exzess dar, welcher der Dienststelle des Polizeibeamten nicht zuzurechnen war ... Es handelte sich vielmehr um einen Verstoß, den der Beamte als Privatperson unter Nutzung dienstlicher Zugriffsbefugnisse beging. Sein Handeln war deshalb nach der DSGVO zu bewerten und wurde mit einem moderaten Bußgeld in Höhe von 1.400 Euro geahndet." (Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg, Tätigkeitsbericht Datenschutz 2019, Seite 41, abrufbar unter https://ogy.de/tb-bw-2020).

Oder Teil des Verantwortlichen?

Ganz anders behandeln das Bayerische Landesamt für Datenschutzaufsicht und der Bayerische Landesbeauftragte für den Datenschutz solche Sachverhalte. Sie vertreten übereinstimmend folgende Auffassung: „[Ein] Mitarbeiter einer öffentlichen Stelle, der Datenabrufe zu rein privaten Zwecken vornimmt, [wird dadurch] nicht zum selbstständigen Verantwortlichen im Sinne des Art. 4 Nr. 7 DS-GVO, sondern bleibt Teil der verantwortlichen Behörde." Eine Geldbuße auf der Basis der DSGVO halten sie daher gegen ihn nicht für möglich. Denkbar sei lediglich eine Ahndung als Ordnungswidrigkeit im Sinn von Art. 23 Bayerisches Datenschutzgesetz (Bayerisches Landesamt für Datenschutzaufsicht, Tätigkeitsbericht 2019, Seite 71, abrufbar unter www.lda.bayern.de/media/bayl-da_report_09.pdf .

Das Thema spielt in der Diskussion um die uneinheitliche Anwendung der DS-GVO in Deutschland eine Rolle. Siehe dazu auch Ehmann, Datenschutz PRAXIS 12/2019, Seite 1.

Bild: iStock.com/AnnettVauteck

Detailliert erfasste Fehlzeiten, verknüpft mit den Einflussfaktoren auf Fehlzeiten, ermöglichen aussagekräftige Auswertungen und effektive Gegenmaßnahmen

Beschäftigtendatenschutz

Fehlzeiten datenschutzkonform erfassen – die Beispiele

Ausfall- und Fehlzeiten von Beschäftigten zu erfassen und zu analysieren, ist ein komplexer Vorgang. Wie lässt sich das am besten im Verzeichnis von Verarbeitungstätigkeiten abbilden?

Unternehmen haben in der Regel ein sehr konkretes Interesse daran, Fehlzeiten so gering wie möglich zu halten. Um die dazu notwendigen Daten zu erfassen, kommen meist IT-gestützte Personalinformationssysteme zum Einsatz, die für die Lohn- und Gehaltsabrechnung wichtig sind und zusätzlich Ausfall- sowie Fehlzeiten erfassen und auswerten.

Vorsicht, gläserner Mitarbeiter

Diese IT-Systeme bieten umfassende Dokumentations-, Auswertungs- und Analysemöglichkeiten, um einzelne Mitarbeiter zu durchleuchten. Sie lassen erste Angaben über Regelmäßigkeiten, Häufungen und Auffälligkeiten sowie die Berechnung spezifischer Kennzahlen zu.

So lässt sich beispielsweise analysieren,

- welche Zusammenhänge zwischen verschiedenen Merkmalen und dem Auftreten von Fehlzeiten existieren,
- wie sich Fehlzeiten über Monate und z.T. Jahre verteilen,
- wann Fehlzeiten beginnen und enden etc.

Anhand einer personengruppenbezogenen Datensammlung ist es möglich, eine Schwachstellenanalyse bezüglich der Fehlzeiten im Betrieb durchzuführen, Ursachenfelder für auffällige oder höhere Fehlzeiten auszumachen und so zu ersten Anhaltspunkten für mögliche und geeignete Maßnahmen zu gelangen, um Fehlzeiten zu reduzieren.

Rechtmäßigkeit hinterfragen

Bevor Unternehmen solche Möglichkeiten nutzen, gilt es jedoch, jede Verarbeitung von personenbezogenen Daten sowie deren Rechtmäßigkeit im Sinne der Datenschutz-Grundverordnung (DSGVO) bzw. des Bundesdatenschutzgesetzes (BDSG) zu hinterfragen. Technisch möglich ist an dieser Stelle viel, rechtlich einwandfrei geht tatsächlich nur einiges.

Die Aufgaben des DSB

Zu beachten ist, dass Verantwortliche neben der eventuell vorhandenen Arbeitnehmervertretung den Datenschutzbeauftragten (DSB) einbeziehen müssen, bevor sie ein System einführen, das Fehl- bzw. Ausfallzeiten dokumentiert und analysiert. Ihre Aufgabe als DSB ist es, bei der Erstellung bzw. Ergänzung des Verzeichnisses von Verarbeitungstätigkeiten zu unterstützen und auf Datenschutz-Fallstricke bei Verarbeitungen hinzuweisen. Daneben beraten Sie dabei, eine möglicherweise erforderliche Datenschutz-Folgenabschätzung durchzuführen.

Darstellung im Verzeichnis von Verarbeitungstätigkeiten

Wie der erste Teil gezeigt hat, ist es für Verantwortliche empfehlenswert, jede Verarbeitungstätigkeit einzeln zu betrachten (siehe Datenschutz PRAXIS 10/2020, S. 14–15). Da jede Verarbeitungstätigkeit einen anderen rechtlichen Bezug haben kann, können sich unterschiedliche Folgen ableiten, z.B. bei den Aufbewahrungszeiten (Löschpflichten). Die Beispiele auf der folgenden Seite zeigen, wie eine Darstellung und Dokumentation der Verarbeitungstätigkeiten aussehen kann.

Ideal: Betriebsvereinbarung + Verfahrensbeschreibung

Der beste Weg, eine betriebliche Regelung zum Umgang mit Fehlzeitendaten zu finden, sind eine ausgewogene Betriebsvereinbarung (oder arbeitsvertragliche Regelungen) und eine ausführliche Verfahrensbeschreibung. Verantwortliche sollten sich in Zusammenarbeit mit dem DSB hierzu folgende Eckdaten bewusst machen und schriftlich fixieren:

1. Welche Möglichkeiten bietet die verwendete Technologie? →

Beschreibung	Unternehmensbezogene Angaben
Verantwortlicher	Max Muster GmbH, Geschäftsführerin Lise Lotte, Beispielstraße 123, 12345 Musterhausen
Fachbereich	Fachbereich Pflege
Verarbeitungstätigkeit	Das Führen von Monatslisten mit An- und Abwesenheitszeiten der einzelnen MitarbeiterInnen
Zweckbestimmung	Identifikation und Dokumentation von Zeiten zur Berechnung von unständigen Lohnbestandteilen, z.B. Bereitschaftsdienstzuschläge, Krankentagezuschlag
Rechtliche Grundlage	Art. 6 Abs. 1 Buchst. c DSGVO i.V.m. § 26 BDSG
Kategorien betroffener Personen	Beschäftigte
Kategorien personenbezogener Daten	Name, Personalnummer, Abteilung, Anwesenheitszeiten, Abwesenheitszeiten mit Gründen (Krankheit, Urlaub etc.), Soll-Arbeitszeit, Ist-Arbeitszeit
Kategorien von Empfängern	Intern: HR, Geschäftsführung, Abteilungsleitung, Fachbereichsleitung, Betriebsrat Extern: Steuerberater, Wirtschaftsprüfer, Finanzbehörden, Rentenversicherung, Berufsgenossenschaft
Übermittlung in ein Drittland	Nein
Löschfristen	2 Jahre
Technische und organisatorische Maßnahmen (TOM)	Die Listen werden von der Fachbereichsleitung geführt und unter Verschluss gehalten (Aktenordner in Stahlschrank). Die Fachbereichsleitung reicht die Listen in einem geschlossenen Umschlag bis spätestens zum 3. Werktag im Folgemonat im Bereich HR persönlich ein. Der HR-Bereich übernimmt die Daten in das Gehaltsabrechnungsprogramm (TOM in eigenem Verfahren beschrieben) und sichert die bearbeiteten Daten in einem Ordner im verschlossenen Aktenschrank.
Sonstige Anmerkungen	Die dokumentierten Abwesenheitsdaten werden im Bereich HR als Statistik zusammengefasst und ausgewertet.

Verzeichnis von Verarbeitungstätigkeiten: Fehlzeitenerfassung in der Pflege (oben) und für das Betriebliche Gesundheitsmanagement

Beschreibung	Unternehmensbezogene Angaben
Verantwortlicher	Max Muster GmbH, Geschäftsführerin Lise Lotte, Beispielstraße 123, 12345 Musterhausen
Fachbereich	HR
Verarbeitungstätigkeit	Betriebliches Gesundheitsmanagement
Zweckbestimmung	Bereitstellung von Maßnahmen im Rahmen eines betrieblichen Gesundheitsmanagements
Rechtliche Grundlage	Art. 6 Abs. 1 Buchst. f DSGVO i.V.m. § 26 BDSG
Kategorien betroffener Personen	Beschäftigte
Kategorien personenbezogener Daten	Name, Krankenkasse, SV-Nummer, Fehlzeiten mit Gründen (Krankheit, Urlaub etc.), Daten zu Verletzungen, Daten zu Erkrankungen, Behinderungsdaten
Kategorien von Empfängern	Intern: HR, Geschäftsführung, Abteilungsleitung, Betriebsrat Extern: Betriebsarzt, Dienstleister für Gesundheitsangebote
Übermittlung in ein Drittland	Nein
Löschfristen	Unmittelbar nach Wegfall des Zwecks
Technische und organisatorische Maßnahmen (TOM)	Die vorgenannten Daten werden im Bereich HR verarbeitet. Die Auswertung der Fehlzeitengründe erfolgt mittels Software XYZ, die auf dem Server in einem eigenen gesicherten Bereich kennwortgeschützt zugängig ist. Die Sicherung der Daten innerhalb dieser Software erfolgt im Rahmen des IT-Sicherheitskonzepts (eigene Verfahrensbeschreibung). Der HR-Bereich ist für die Aufbereitung der Daten und Weiterleitung an die Geschäftsleitung verantwortlich. Einzeldaten können zur weiteren Verarbeitung an den externen Betriebsarzt weitergeleitet werden. Die Gesamtstatistik wird zur Diskussion der Maßnahmen zur betrieblichen Gesundheit an die Abteilungsleiter und den Betriebsrat übermittelt.
Sonstige Anmerkungen	Maßnahmen, an denen Mitarbeiter freiwillig teilnehmen können, werden im Rahmen von Art. 6 Abs. 1 Buchst. a DSGVO auf Basis einer Einwilligung durchgeführt.

2. Welche der Möglichkeiten sind erforderlich, um welchen Zweck zu erreichen?
3. Welche Daten sind hierfür nötig?
4. Wer erhält Zugriff auf diese Daten und wer darf sie verarbeiten?
5. Wie soll mit Zweckänderungen umgegangen werden?
6. Welche Aufbewahrungsfristen sind vorgesehen? Wie lassen sich welche Löschprozesse nach Ablauf der Fristen implementieren?

Arnd Fackeldey ist Geschäftsführer der Digital Compliance Consulting GmbH. Als DSB und Auditor unterstützt er Unternehmen, Datenschutzprozesse einzuführen.

Bild: iStock.com/asiandelight

Mit einer Kombination aus Betriebsvereinbarung und individueller Vereinbarung lässt sich BYOD gut in den Griff bekommen

Muster-Betriebsvereinbarung

Bring your own Device revisited

Viele Beschäftigte arbeiten immer noch im Homeoffice, ein Teil davon mit privaten Geräten – und das oft völlig ungeregelt. Das hier vorgestellte Muster einer Betriebsvereinbarung ist eine gute Ausgangsbasis, mit der Unternehmen für klare und sichere Verhältnisse sorgen.

Die Corona-Pandemie hat sowohl die Digitalisierung der Prozesse als auch die Arbeit im Homeoffice quasi über Nacht vorangebracht. Selbst Unternehmen und Behörden, die die Arbeit im Homeoffice bis dato strikt abgelehnt hatten, sahen plötzlich Vorteile in der Arbeit von zu Hause. Sie hatten allerdings das Problem, dass kurzfristig nicht hinreichend mobile IT-Geräte (Notebooks, Mini-PCs und Tablets) am Markt verfügbar waren. Damit stand verstärkt die Frage der Nutzung von privaten IT-Geräten im Raum.

Selbst Datenschutzaufsichtsbehörden erteilten aufgrund der Notsituation unter Auflagen befristete Freigaben für den Einsatz privater IT-Geräte bis in den Gesundheits- und Sozialbereich. Doch mittlerweile ist es geboten, diese Nutzung privater Geräte in geregelte Bahnen zu lenken.

Kontrollverlust vermeiden

Arbeiten Beschäftigte mit privaten IT-Systemen, ist eine große Sorge der Arbeitgeber, die Kontrolle zu verlieren. Denn der Arbeitgeber darf die privaten IT-Geräte nicht ohne Weiteres untersuchen. Hier sind Regelungen nötig, die diesen Kontrollverlust weitgehend vermeiden, ohne die Beschäftigten unnötig im Privatbereich zu tangieren.

Eine Regelung zur Nutzung privater IT-Systeme besteht aus zwei Teilen:

- einer Betriebsvereinbarung, die den allgemeinen Rahmen bestimmt, und
- einer individuellen Vereinbarung mit der oder dem Beschäftigten.

Betriebsvereinbarung

Das auf Seite 17 vorgestellte und an Unternehmen angepasste Beispiel für eine Betriebsvereinbarung orientiert sich an zwei Dokumenten:

- zum einen am Runderlass des niedersächsischen Kultusministeriums zur Nutzung der privaten IT-Geräte von Lehrern bei der Verarbeitung der Schüler- und Elterndaten.
- zum anderen an einem Muster für einen entsprechend Antrag mit individueller Verpflichtung, das das Niedersächsische Landesinstitut für schulische Qualitätsentwicklung veröffentlicht hat (beides abrufbar unter https://ogy.de/nibis-private-it-systeme-1).

Allgemeiner Rahmen

Das angepasste Muster enthält die wesentlichen Bestandteile der Betriebsvereinbarung. Auf den Abdruck üblicher Einleitungsklauseln (Platzhalter ist § 1) und Schlussklauseln (§ 8 ff) mit Geltungsbereich, Kontrollrechten des Betriebsrats, Beschwerdeverfahren und Kündigung der Betriebsvereinbarung verzichten wir. Denn hierzu gibt es in vielen Unternehmen individuelle, über Jahre ausgefeilte Standardformulierungen.

Das Muster finden Datenschutz-PRAXIS-Leser zum Herunterladen unter www.datenschutz-praxis.de.

Die Betriebsvereinbarung regelt den allgemeinen Rahmen wie z.B. die Grundsätze (§ 2), die Details des Genehmigungsverfahrens und die Dauer der Genehmigung (§ 3). § 4 legt fest, welche Daten Beschäftigte maximal auf privaten IT-Systemen verarbeiten dürfen. Dieser Paragraf muss firmenindividuell erstellt werden. Das Muster gibt ein Beispiel. Alle Daten, →

die hier nicht aufgeführt sind, dürfen Mitarbeiter nicht auf privaten IT-Systemen verarbeiten.

Technisch-organisatorische Maßnahmen

§ 5 führt die mindestens einzuhaltenden technisch-organisatorischen Maßnahmen auf. Diese Maßnahmen kann die IT-Abteilung und/oder die oder der Informationssicherheitsbeauftragte ergänzen und konkretisieren. Das ermöglicht es, die Vereinbarung über einen längeren Zeitraum nicht zu ändern und trotzdem die Maßnahmen an technische Entwicklungen anzupassen (Stichwort: Stand der Technik).

Aktuelles Betriebssystem, aktueller Virenscanner

Wesentlich ist z.B., das Betriebssystem und jedwede genutzte Software aktuell zu halten und alle Sicherheitsupdates einzuspielen. Bei einem virengefährdeten Betriebssystem – definitiv Windows, aber auch MacOS – muss ein aktueller Virenscanner installiert sein und auf dem Laufenden gehalten werden (Signaturupdates).

Verschlüsselung

Alle dienstlichen Daten müssen verschlüsselt sein. Es empfiehlt sich eine grundlegende Verschlüsslung der Festplatten im Rechner (Bitlocker oder VeraCrypt bei Windows und FileVault 2 bei MacOS) mit einer Pre Boot Authentication (PBA). Bei einer PBA muss der Mitarbeiter das Verschlüsselungspasswort vor dem Start des Betriebssystems eingeben.

Das schützt allerdings nicht gegen berechtige weitere Nutzer eines Familien-PC. Denn alle berechtigten Nutzer eines solchen PC müssen das PBA-Passwort kennen. Deshalb muss auf einem Familien-PC ein eigenes Nutzerkonto für die dienstliche Nutzung vorhanden sein. Die personenbezogenen Daten sollten außerdem nochmals separat verschlüsselt sein. Besonders einfach geht das mit einer Containerverschlüsselung wie VeraCrypt.

E-Mail-Zugriff nur über Web

Der Zugriff auf dienstliche E-Mails erfolgt nur über eine Webmail-Oberfläche. Das stellt sicher, dass alle E-Mails auf Servern des Unternehmens bleiben und nicht – wie bei der Synchronisation mit einem E-Mail-Client – automatisch auf dem privaten IT-System gespeichert werden. Zusätzlich sollte der Mitarbeiter den Browser-Cache regelmäßig (automatisch) löschen.

Der Zugriff auf Unternehmensressourcen muss über VPN-Verbindungen erfolgen. Soweit ein Beschäftigter direkt aus dem Homeoffice auf vom Unternehmen genutzte Cloud-Services zugreift, muss mindestens eine Transport-Verschlüsslung (TLS 1.2 oder besser) stattfinden.

PRAXIS-TIPP

Ideal ist nach wie vor ein Zugriff aus dem Homeoffice auf eine zentrale Infrastruktur per Remote Desktop oder eine vergleichbare Lösung. In dem Fall erfolgt die Verarbeitung und Speicherung der Daten im Unternehmen. Der Mitarbeiter sieht nur die Anzeige.

Das Niedersächsische Landesinstitut für schulische Qualitätsentwicklung stellt auf dem Niedersächsischen Bildungsserver (NiBiS) im Datenschutzportal allgemein verständliche technisch-organisatorische Vorgaben als Konkretisierung für Lehrer und Schulen zur Verfügung. Das ist eine gute Ausgangsbasis für eigene Anpassungen. Die Vorgaben finden sich unter https://ogy.de/nibis-private-it-systeme-2.

Passen die Softwarelizenzen?

Ein weiterer Aspekt der Nutzung von privaten IT-Systemen ist die Notwendigkeit, die Software auf diesen Geräten für eine kommerzielle Nutzung zu lizenzieren. Microsoft nennt das in seinen Lizenzverträgen „kommerzielle, gemeinnützige oder Einnahmen erwirtschaftende Aktivitäten". Nutzt ein Mitarbeiter sein privates IT-System für die berufliche Arbeit, müssen die Softwarelizenzen das auch erlauben.

Prof. Dr. Rainer W. Gerling ist Autor und Referent sowie stellvertretender Vorsitzender des Vorstands der GDD e.V. Er lehrt IT-Sicherheit an der Hochschule München.

Zusatz zur Betriebsvereinbarung

Individuelle Vereinbarung

Der individuelle Zusatz ist nötig, weil die erforderlichen Vereinbarungen über das hinausgehen, was sich in einer kollektiven Regelung abbilden lässt. Das betrifft etwa die Erlaubnis, die Wohnung zu betreten oder auf den privaten Rechner zuzugreifen.
Der Betriebsrat kann in einer Betriebsvereinbarung nicht für die Beschäftigten in Dinge einwilligen, die sich auf den privaten Besitz beziehen. Hier muss die/der Beschäftige einwilligen.
Der Inhalt der individuellen Vereinbarung ergibt sich direkt aus der Betriebsvereinbarung. Insofern wiederholen sich Texte aus der Betriebsvereinbarung in der individuellen Verpflichtung. Das stellt zudem sicher, dass der Inhalt der individuellen Vereinbarung mitbestimmt bleibt. Es ist sinnvoll, die individuelle Vereinbarung mit einem Antrag auf Nutzung der privaten IT-Geräte zu verbinden. Dann gibt es nur ein Formular für diesen Zweck im Unternehmen.
Gibt es in einem Unternehmen keinen Betriebsrat, kann die Geschäftsleitung eine Dienstanweisung erlassen, die inhaltlich die Regelungen der Betriebsvereinbarung übernimmt, und sie im Rahmen des Direktionsrechts in Kraft setzen. Dann stützt sich die individuelle Vereinbarung auf die Dienstanweisung.

§ 2 Allgemeine Bestimmungen
(1) Diese Betriebsvereinbarung regelt den datenschutzkonformen Einsatz privater IT-Systeme zur Erledigung dienstlicher Aufgaben sowohl innerhalb wie auch außerhalb der Diensträume des >>UNTERNEHMENS<< (im folgenden Unternehmen).
Private Endgeräte (stationär oder mobil) dürfen genutzt werden, um personenbezogene Daten auf einem gesicherten Server des Unternehmens oder einer beauftragten Stelle i.S. des Artikels 28 der DSGVO zu verarbeiten. Die Speicherung personenbezogener Daten auf dem Festspeicher privater mobiler Endgeräte (Smartphones und Tablets) ist nicht zulässig. Das Speichern und Anzeigen personenbezogener Daten in Clouds oder über Applikationen von Fremdanbietern ist zulässig, wenn zuvor mit diesen vom Unternehmen ein Vertrag zur Auftragsverarbeitung i.S. von Artikel 28 Abs. 3 DSGVO geschlossen wurde. Für den Fall, dass im Rahmen einer Auftragsverarbeitung eine Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation erfolgt, sind die Artikel 44 bis 49 DSGVO einzuhalten.
(2) Wenn Beschäftigte auf privaten IT-Systemen Daten nach § 4 verarbeiten, ist das eine dienstliche Tätigkeit. „Verantwortlicher" i.S. der DSGVO ist daher auch in diesen Fällen das Unternehmen. Die Geschäftsleitung bleibt für die Einhaltung der datenschutzrechtlichen Vorschriften auch dann verantwortlich, wenn die Beschäftigten derartige Daten zu Hause verarbeiten.

§ 3 Genehmigungsverfahren
(1) Beschäftigte, die auf einem privaten IT-System personenbezogene Daten nach § 4 verarbeiten wollen, bedürfen dazu der schriftlichen Genehmigung der Geschäftsleitung.
In dem Antrag auf Genehmigung sind das IT-System, die Software und die Datenschutz- und Datensicherungsmaßnahmen nach § 5 Abs. 1 in Stichworten zu beschreiben. Die Genehmigung wird nur erteilt, wenn die oder der Beschäftigte die in § 6 vorgeschriebene Verpflichtungserklärung abgibt. Die Genehmigung ist auf dem Antrag zu vermerken und zur Personalakte zu nehmen.
Eine Kopie des genehmigten Antrags ist der oder dem Beschäftigten auszuhändigen, eine weitere Kopie der oder dem Datenschutzbeauftragten des Unternehmens.
(2) Die Genehmigung gilt für einen Zeitraum von maximal zwei Jahren; danach ist ggf. erneut eine Genehmigung zu beantragen. Bei wesentlichen Änderungen, wie z.B. Austausch des IT-Systems und/oder Wechsel des Betriebssystems, ist unverzüglich eine neue Genehmigung durch die oder den Beschäftigten zu beantragen.
(3) Der genehmigte Antrag und die Verpflichtungserklärung sind aufzubewahren. Der genehmigte Antrag ersetzt nicht das Verzeichnis von Verarbeitungstätigkeiten nach Artikel 30 Abs. 1 DSGVO. Die Sammlung der genehmigten Anträge ist für Überprüfungen durch die Datenschutzaufsichtsbehörde vorzuhalten.

§ 4 Datenrahmen
(1) Es dürfen nur personenbezogen Daten verarbeitet werden, die für die Aufgabenwahrnehmung durch die oder den Beschäftigten erforderlich sind.
(2) Folgender Datenrahmen darf nicht überschritten werden:
Auflistung der maximal erlaubten Daten bzw. Datenarten und der betroffenen Personengruppen
Beispiel:
Daten zu Verträgen mit Kunden (Kunden = Unternehmen)
Namen, Adressdaten, E-Mail-Adresse und Telefonnummer von Ansprechpartnern beim Kunden
Kommunikation mit den Ansprechpartnern, Vertragskonditionen
Von diesen Daten dürfen nur die Daten verarbeitet werden, die für die jeweilige Aufgabenerledigung tatsächlich erforderlich sind.

§ 5 Datenschutz- und Datensicherungsmaßnahmen
(1) Durch geeignete organisatorische und technische Maßnahmen ist sicherzustellen, dass nur die oder der Beschäftigte selbst Zugang zu den in § 4 genannten Daten erhält:
a. Werden die Daten auf internen Speichermedien (z.B. Festplatte) gespeichert, sind die Daten durch geeignete technische Maßnahmen gegen Zugriff zu sichern. Dafür ist mindestens eine Zugriffskontrolle durch das Betriebssystem auf Verzeichnis- oder Dateiebene einzurichten sowie eine Verschlüsselung der Verzeichnisse, in denen die Daten gespeichert sind, vorzunehmen. Online-Zugriffe auf die Daten sind durch den Stand der Technik entsprechende Vorkehrungen (z.B. Firewall) auszuschließen.
b. Werden für die Speicherung der Daten externe Speichermedien verwendet, sind diese zu verschlüsseln und so aufzubewahren, dass sie Unbefugten nicht zugänglich sind.
c. Es ist insbesondere darauf zu achten, dass aktuelle Updates und Patches auf der genutzten Hard- und Software (einschließlich Router, Endgeräte, Betriebssysteme, Applikationen und Programme) aufgespielt sind und ein hinreichender Schutz vor Schadprogrammen vorhanden ist.

(2) Es muss sichergestellt sein, dass die in § 4 genannten Daten jederzeit auch dann verfügbar sind, wenn das IT-System ausfällt oder der Datenträger oder -speicher beschädigt wird (Datensicherung).
(3) Die Daten nach § 4 dürfen auf den privaten Geräten nur so lange elektronisch gespeichert werden, wie die oder der Beschäftigte diese zur Aufgabenerfüllung auf dem privaten IT-System benötigt. Danach sind die elektronisch gespeicherten Daten zu löschen und es ist – soweit erforderlich – auf Daten, die auf Dienstgeräten gespeichert sind, zurückzugreifen.
(4) Die elektronische Übersendung oder Übertragung der Daten nach § 4 sowie der Transport der Daten mittels elektronischer Speichermedien sind nur zulässig, wenn die Daten verschlüsselt werden. Bei einer zulässigen Speicherung auf Speicherorten, die nur über das Internet erreichbar sind, ist ein verschlüsselter Transportweg einzuhalten.
(5) Weitergehende konkrete Vorgaben zur datenschutzkonformen Konfiguration der privaten IT-Systeme durch die IT-Abteilung bzw. die oder den Informationssicherheitsbeauftragte(n) müssen eingehalten werden.

§ 6 Verpflichtungserklärung
Mit dem Antrag auf Genehmigung der Verarbeitung personenbezogener Daten nach § 4 auf einem privaten IT-System ist der Geschäftsleitung folgende schriftliche Erklärung zu übergeben:
„Ich verpflichte mich, bei der Verarbeitung personenbezogener Daten des Unternehmens auf meinem privaten IT-System
- den Datenrahmen gemäß § 4 und die Datenschutz- und Datensicherungsmaßnahmen gemäß § 5 der Betriebsvereinbarung vom >>DATUM<< zur Verarbeitung personenbezogener Daten auf privaten Informationstechnischen Systemen (IT-Systemen) von Beschäftigten einzuhalten und
- dem Unternehmen einen Ausdruck oder ein verschlüsseltes elektronisches Speichermedium mit allen gespeicherten Daten zur Verfügung zu stellen, wenn das Unternehmen diese benötigt (z.B. wenn ein Antrag auf Auskunft nach Artikel 15 DSGVO gestellt worden ist).

Ich sichere zu, den Beschäftigten der zuständigen Datenschutzaufsichtsbehörde im Rahmen einer Prüfung auf Verlangen Zugang zu allen im Rahmen der o.g. Betriebsvereinbarung genutzten privaten IT-Systemen und Speichermedien zu gewähren, um ihr oder ihm die Wahrnehmung der gesetzlichen Kontrollaufgaben im dienstlichen Bereich zu ermöglichen."

§ 7 Rechtlicher Hinweis
Die Einhaltung der Bestimmungen dieser BV kann von der Unternehmensleitung, der oder dem für das Unternehmen bestellten Datenschutzbeauftragten im privaten Bereich der Beschäftigten nicht kontrolliert werden. Darum ist von den Beschäftigten die Verpflichtungserklärung gemäß § 6 abzugeben.
Es wird ausdrücklich darauf hingewiesen, dass Verstöße gegen diese Bestimmungen eine Verletzung der arbeitsrechtlichen Pflichten darstellen, die arbeitsrechtlich verfolgt werden muss, wenn sie der Unternehmensleitung bekannt wird.

Bild: iStock.com/AdrianHancu

Das BVerfG hat dem Gesetzgeber den klaren Auftrag erteilt, die Regelungen zur Bestandsdatenabfrage zu überarbeiten

Bestandsdatenauskunft – 6 Fragen zum Urteil

BVerfG: Hürden für Eingriffe in die Privatsphäre zu niedrig

Das Bundesverfassungsgericht ist immer wieder für klare Worte im Datenschutz gut. Nachdem die Hüterin des Grundgesetzes die Vorratsdatenspeicherung mehrmals gekippt hat, hat sie nun auch der Regelung zur Abfrage von Bestandsdaten durch Behörden eine Absage erteilt.

Das Urteil des Bundesverfassungsgerichts (BVerfG) zum Zugriff staatlicher Strafverfolgungs- und Sicherheitsbehörden auf Daten von Handy- und Internetnutzern mag auf den ersten Blick überraschen. Denn die Erhebung von Bestandsdaten greift bei Weitem nicht so tief in das Persönlichkeitsrecht ein wie etwa die Überwachung der Telekommunikation (Beschluss vom 27. Mai 2020 – 1 BvR 1873/13, abrufbar unter https://ogy.de/bverfg-bestandsdaten).

Mit welchen Daten hat sich das Gericht befasst?

Im Mittelpunkt der Entscheidung stehen die sogenannten Bestandsdaten. Das sind die personenbezogenen Daten, die ein Diensteanbieter bei der Erbringung von Telekommunikationsleistungen erheben und verwenden darf, um seine Verträge durchführen zu können. Es handelt sich dabei also in erster Linie um personenbezogene Daten über den Inhaber eines Telefonanschlusses. Das sind v.a. die nach § 111 Telekommunikationsgesetz (TKG) zu speichernden Daten, also

- Rufnummer,
- Name und Anschrift,
- Geburtsdaten,
- der Standort eines Festnetzanschlusses bzw. die Gerätenummer eines Mobilfunkendgeräts sowie
- das Datum des Vertragsbeginns.

Diese Daten können Strafverfolgungs- und Sicherheitsbehörden nach § 112 TKG von Telekommunikationsdienstleistern über die Bundesnetzagentur automatisiert abrufen. Darüber hinaus haben die Behörden nach § 113 TKG die Möglichkeit, in einem manuellen Verfahren weitere Daten heraus zu verlangen. Von Bedeutung sind hierbei in erster Linie dynamische IP-Adressen, die einem bestimmten Internetanschluss in einem bestimmten Zeitraum zugewiesen waren.

Hingegen sind Verkehrsdaten wie die Rufnummer, SIM-Kartennummer oder Standortdaten nicht Gegenstand dieser Entscheidung, erst recht nicht Inhaltsdaten, also Informationen, die den Inhalt der Telekommunikation betreffen.

Hält das BVerfG den Abruf von Bestandsdaten grundsätzlich für unzulässig?

Nein. Das Bundesverfassungsgericht hat den Abruf von Bestandsdaten nicht generell für unzulässig erklärt. Wie schon in seiner ersten Entscheidung aus dem Jahr 2012 stellt das Gericht die grundsätzliche Möglichkeit, Bestandsdaten abzurufen, nicht infrage. Es verlangt nur, dass Rechtsgrundlagen exakt festlegen müssen, ab wann Strafverfolgungs- und Sicherheitsbehörden in ein Grundrecht eingreifen dürfen.

Was fordert das Gericht konkret?

Der Gesetzgeber hat bislang einheitlich für alle Bereiche lediglich normiert, dass eine Auskunft erforderlich sein muss, um die jeweilige behördliche Aufgabe zu erfüllen. Das genügt verfassungsrechtlichen Anforderungen aber nicht, so das Gericht:

- Bei der Gefahrenabwehr muss eine abstrakte Gefahr vorliegen.
- Bei der Strafverfolgung muss mindestens ein Anfangsverdacht vorhanden sein.
- Zusätzlich muss der Abruf von Daten wie dynamischer IP-Adressen dem „Schutz oder der Bewahrung von Rechtsgütern von zumindest hervorgehobenem Gewicht“ dienen.
- Sind diese Voraussetzungen nicht ganz erreicht, kann zumindest dann ein Zugriff erfolgen, wenn das Gewicht der betroffenen Rechtsgüter erhöht ist.

Die Übermittlungsbefugnisse in § 113 TKG und in anderen Fachgesetzen erfüllen diese Anforderungen nicht. Denn Auskünfte über solche Daten, deren Aussagekraft und Verwendungsmöglichkeiten eng begrenzt sind, dürfen nicht ins Blaue hinein zugelassen sein

Die allgemeine Erlaubnis, die Datenabfrage zur Aufgabenerfüllung zuzulassen, ist nicht hinreichend bestimmt. Daneben müssen die Behörden die jeweiligen Grundlagen einer Entscheidung genau dokumentieren. Diese Entscheidung muss nicht nur nachvollziehbar, sondern auch überprüfbar sein.

Was muss nun geschehen?

Der Gesetzgeber muss die bisherigen Rechtsgrundlagen für die Erhebung von Bestandsdaten im TKG so ändern, dass sie den verfassungsmäßigen Anforderungen genügen. Das bedeutet, dass er die Normen klarer fassen muss. Es muss deutlich werden, unter welchen exakten Voraussetzungen und zu welchem Zweck diese Daten jeweils erhoben werden dürfen. Der Gesetzgeber hat nun bis längstens Ende 2021 Zeit, dies umzusetzen.

Was gilt in der Übergangszeit?

Bis zu einer Neuregelung, längstens bis 31. Dezember 2021, bleiben die Vorschriften, die das BVerfG für unvereinbar mit dem Grundgesetz erklärt hat, anwendbar.

WICHTIG

Bis zum Ende der Übergangszeit sind die Forderungen des Bundesverfassungsgerichts quasi in die jetzige Fassung hineinzulesen. Mit anderen Worten: Es muss tatsächlich eine konkrete Gefahr vorliegen, damit ein Zugriff zur Gefahrenabwehr erfolgen darf. Betroffene Anschlussinhaber sollten die Rechtmäßigkeit der Abfrage von Bestandsdaten daher genau prüfen! Ein Prüfschema findet sich online unter http://dspraxis.de/bverfgbestandsdaten.

Was ist mit Daten, die Behörden schon zuvor erhoben haben?

Soweit die Erhebung bereits vorher – wie wohl in den meisten Fällen – den Anforderungen des Bundesverfassungsgerichts genügt hätte, ist dies unproblematisch. Gerade im Strafprozess wird ohnehin in fast allen Fällen ein Anfangsverdacht vorliegen. Die Voraussetzungen an diesen Anfangsverdacht sind nicht allzu hoch. Denn es muss nur aufgrund von Tatsachen (Indizien) möglich erscheinen, dass eine Straftat vorliegt.

Ist das ausnahmsweise nicht der Fall, führt das allerdings auch nicht automatisch dazu, dass die erhobenen Daten nicht verwertbar sind. Vielmehr muss im Strafprozess jeder einzelnen Maßnahme widersprochen werden. Ist die Beschaffung von dynamischen IP-Adressen und Bestandsdaten rechtswidrig, hindert dies nicht an einer Verurteilung. Wird danach beim Nutzer der IP-Adresse erfolgreich durchsucht, lassen sich die aufgefundenen Beweismittel im Prinzip verwenden. Dagegen kann der Nutzer nur erfolgreich vorgehen, wenn er sowohl der Durchsuchungsanordnung als auch der Beschlagnahme widerspricht.

Fazit: Genau hinsehen lohnt sich

Die Bedeutung der Entscheidung für die Praxis ist enorm. Denn die Erhebung von Bestandsdaten – also in der Regel die Mitteilung, wer Inhaber eines bestimmten Anschlusses ist –, war bislang gang und gäbe. Nun muss einerseits der Gesetzgeber eine vernünftige Rechtsgrundlage schaffen. Andererseits müssen die Strafverfolgungs- und Sicherheitsbehörden in der Übergangszeit wenigstens gewisse Mindestvoraussetzungen beachten.

Es bleibt abzuwarten, ob der Gesetzgeber die verfassungsrechtlichen Anforderungen einmal mehr nur als Obergrenze versteht. Bis zu einer Neufassung kann es sich durchaus lohnen, genau hinzusehen, ob eine Maßnahme rechtmäßig ist oder nicht.

Dr. Claus Pätzel ist Vorsitzender Richter am Oberlandesgericht München. Zuvor leitete er die Strafabteilung des Landgerichts Augsburg.

IMPRESSUM

Verlag:
WEKA MEDIA GmbH & Co. KG
Römerstraße 4, 86438 Kissing
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
Website: www.weka.de

Herausgeber:
WEKA MEDIA GmbH & Co. KG
Gesellschafter der WEKA MEDIA GmbH & Co. KG sind als Kommanditistin:
WEKA Business Information GmbH & Co. KG und als Komplementärin:
WEKA MEDIA Beteiligungs-GmbH

Geschäftsführer:
Stephan Behrens, Michael Bruns, Kurt Skupin

Redaktion:
Ricarda Veidt, M.A. (V.i.S.d.P)
E-Mail: ricarda.veidt@weka.de

Anzeigen:
Anton Sigllechner
Telefon: 0 82 33.23-72 68
Fax: 082 33.23-5 72 68
E-Mail: anton.sigllechner@weka.de

Erscheinungsweise:
Zwölfmal pro Jahr

Aboverwaltung:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-740
E-Mail: service@weka.de

Abonnementpreis:
12 Ausgaben 219,00 €
(zzgl. MwSt. und Versandkosten)
Einzelheft 20 €
(zzgl. MwSt. und Versandkosten)

Druck:
Geiselmann Printkommunikation GmbH
Leonhardstraße 23, 88471 Laupheim

Layout & Satz:
metamedien
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4082

ISSN-Nr.:
1614-6867

Bestellung unter:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
www.datenschutz-praxis.de

Videoüberwachung

Wenn die Polizei schneller als „der Datenschutz“ ist

Dass Datenschutz kein Täterschutz sein darf, ist allen klar. Aber man kann es ja mal versuchen. Das dachte sich zumindest ein Anwalt, der im Namen seines Mandanten Videoaufnahmen löschen lassen wollte.

Videoüberwachung ist im öffentlich zugänglichen Bereich keine einfache Angelegenheit. § 4 Bundesdatenschutzgesetz (BDSG), der die Videoüberwachung öffentlich zugänglicher Räume regeln sollte, hat das Bundesverwaltungsgericht mangels Öffnungsklausel in der Datenschutz-Grundverordnung (DSGVO) gekippt. Und die DSGVO selbst kennt das Wort „Videoüberwachung“ nicht. Gleichwohl sind die Regelungen der DSGVO zu beachten. Und die haben es in sich.

Betroffenenrechte

Eine der wichtigsten Aufgaben ist es, die Informationspflicht zu erfüllen. Betroffene Personen müssen u.a. wissen, wer Verantwortlicher ist, wo sie sich über die verarbeiteten Daten informieren können usw. Außerdem haben die Betroffenen ein Recht auf Auskunft und Löschung. Und davon machen sie immer wieder Gebrauch. Bei solchen Anfragen wird normalerweise der Datenschutzbeauftragte eingebunden.

Aufnahmen zu Beweiszwecken

Videoaufnahmen, beispielsweise in Bussen und Straßenbahnen, bewahren die Betreiber zumeist für die folgenden 48 Stunden auf. Gab es keinen Vorfall, werden die Daten danach oder schon vorher wieder überschrieben. Manchmal kommt es aber doch zu Vorfällen, teilweise mit Verdacht auf Straftat. Beispielsweise wird jemand in der Straßenbahn beleidigt, geschlagen oder beraubt. Und manchmal sichern die Ermittlungsbehörden die Videoaufnahmen dann zu Beweiszwecken im sich anbahnenden Strafverfahren.

Antrag auf Löschung …

Eines Tages meldet sich der Anwalt einer betroffenen Person. Sein Mandant sei am soundsovielten zum Zeitpunkt z mit der Straßenbahnlinie xy von A nach B gefahren. Dabei sei er wohl unrechtmäßig von der Videoüberwachungsanlage gefilmt worden. Man möge doch bitte die Daten der Überwachung löschen.

… beim falschen Adressaten

Die Antwort des zuständigen Mitarbeiters der Verkehrsbetriebe war so lapidar wie verständlich und eindeutig: „Sie brauchen sich nicht zu bemühen. Die Polizei war schon da und hat die Aufnahmen mit richterlichem Beschluss gesichert. Wenden Sie sich doch einfach an die Ermittlungsbeamten. Vielleicht löschen die dann die Aufnahmen.“

Seit 2005 ist Eberhard Häcker selbstständig mit Schwerpunkt Datenschutzberatung. Er ist Mitbegründer von Team Datenschutz, Fachautor und Dozent sowie Geschäftsführer der HäckerSoft GmbH.

IN DER NÄCHSTEN AUSGABE

Datenschutz-Richtlinien

Welche Richtlinien sind ein Muss? Wie viele sind ein „gesundes Maß“? Und wie sollten die Richtlinien aufgebaut sein?

Nutzerfreundliches Einwilligungsmanagement

Ein Projekt des BMJV stellt Lösungsansätze vor. Wir geben einen Überblick.

„Anschwärzen“ ohne Risiko?

Wie können Behörden Informanten schützen? Die DSGVO gibt Anlass, diese Frage erneut zu durchdenken.