www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT | Juli 2021

Bild: iStock.com/beeldlab

Tests sind nur ein Baustein von vielen, um eine Rückkehr an den Arbeitsplatz vor Ort zu ermöglichen. Und die Testpflicht wird wohl bestehen bleiben – die Corona-ArbSchV wird vermutlich in geänderter Form in die Verlängerung gehen.

Rückkehr an den Arbeitsplatz

Impfstatus, Impfungen, Tests, Büro-Orga – das ist zulässig

Unter welchen Bedingungen können beschäftigte Personen in einen einigermaßen normalen Büroalltag zurückkehren? Was müssen Arbeitgeber und Arbeitnehmer dazu aus Datenschutzsicht wissen? Und wie können Datenschutzbeauftragte dabei beratend unterstützen?

Derzeit überschlagen sich die Maßnahmen, die Arbeitgeber treffen müssen, um den Mitarbeitenden die Möglichkeit zu geben, wieder verstärkt in den Büroräumlichkeiten zu arbeiten.

Impfstatus und Impfangebot

Zunächst stellt sich die Frage, ob die Tatsache, ob und wann bzw. gegen was eine Person geimpft ist, ein Gesundheitsdatum im Sinne von Art. 9 Abs. 1 Datenschutz-Grundverordnung (DSGVO) ist. Ein Blick in die Verordnung hilft.

Art. 4 Nr. 15 DSGVO besagt: Gesundheitsdaten sind „personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen."

Erwägungsgrund 35 zur DSGVO macht deutlich, dass der Begriff der Gesundheitsdaten alle Tatsachen umfasst, die in irgendeiner Art und Weise einen Rückschluss auf den Gesundheitszustand des Betroffenen ermöglichen – die DSGVO legt den Gesundheitsbegriff also weit aus.

Abfragen des Impfstatus

Zwar lässt sich allein aus der Tatsache, dass jemand geimpft ist oder nicht, noch nicht die Schlussfolgerung ziehen, dass die betroffene Person nicht an COVID-19 erkrankt war bzw. ist – doch gehen Sie aufgrund der Eingriffsintensität, die eine Impfung darstellt, von der Verarbeitung eines Gesundheitsdatums aus, wenn ein Arbeitgeber den Impfstatus seiner Beschäftigten verarbeiten möchte. →

Editorial

Ricarda Veidt,
Chefredakteurin

Back to Business?

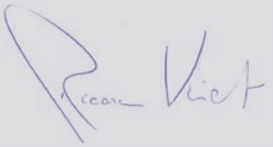
Liebe Leserin, lieber Leser! Die Inzidenz-Zahlen sinken rapide, die Zahl der Sonnenstunden und Biergartenbesucher steigt dagegen gefühlt exponentiell (zumindest zum Zeitpunkt, zu dem ich diesen Text in meinem „Outdoor-Homeoffice" auf der heimischen, Gott sei Dank beschatteten Terrasse verfasse). Da stellt sich langsam die Frage, ob und, wenn ja, unter welchen Voraussetzungen es möglich und sinnvoll ist, wieder mehr Beschäftigte ins Büro zu holen.

Was dabei aus Datenschutzsicht in Bezug auf Impfstatus, Tests u.Ä. wichtig ist, beleuchtet unsere geschätzte Autorin Frau Doris Kiefer.

Ergänzende praktische Hinweise aus einem mehr sicherheitstechnischen Blickwinkel liefert aktuell die US-amerikanische Federal Trade Commission (FTC) in ihrer fünfteiligen Reihe „Back to Business". Der erste Teil, überschrieben mit „Where's your Data?", ist abrufbar unter https://ogy.de/ftc-back-to-business.

Nun wünsche ich uns allen einen möglichst unbeschwerten Sommer. Bleiben Sie vorsichtig und gesund!

Herzliche Grüße
Ihre Ricarda Veidt



Raten Sie dem Verantwortlichen daher, sämtliche Verpflichtungen, die mit der Verarbeitung besonderer Kategorien personenbezogener Daten in Zusammenhang stehen, zu erfüllen.

Erforderlich?

Doch wie sieht es mit der Rechtsgrundlage aus, wenn ein Arbeitgeber von seinen Beschäftigten verlangt, bei Zutritt zu den Büroräumlichkeiten nachzuweisen, dass sie gegen COVID-19 geimpft sind? Das wäre nur zulässig, wenn der Impfstatus erforderlich wäre, damit der Arbeitgeber seinen arbeits- oder sozialrechtlichen Verpflichtungen nachkommen kann und kein schutzwürdiges Interesse des Arbeitnehmers bzw. der Arbeitnehmerin am Ausschluss der Verarbeitung überwiegt. Nicht zuletzt treffen nämlich den Arbeitgeber Fürsorgepflichten gegenüber seinen Arbeitnehmern – u.a. trifft ihn die Pflicht, vermeidbare Schäden abzuwenden.

Eine rechtliche Grundlage dafür, dass Arbeitgeber den Impfstatus ihrer Beschäftigten abfragen, gibt es (derzeit) nicht. Weder die SARS-CoV-2-Arbeitsschutzverordnung (Corona-ArbSchV) noch das Infektionsschutzgesetz (IfSG) sehen solche Verpflichtungen für den Arbeitgeber vor. Fraglich ist daher, ob es erforderlich ist, den Impfstatus abzufragen, um das Beschäftigungsverhältnis durchzuführen.

Weisen Sie den Verantwortlichen darauf hin, dass er zunächst mildere Mittel in Betracht ziehen muss, um Ansteckungen zu verhindern. Hier dürften insbesondere Corona-Tests (zur möglichen Verpflichtung siehe unten) im Vordergrund stehen.

Einwilligung?

Selbstverständlich könnte der Impfstatus eine Angabe sein, die die Beschäftigten freiwillig machen. Dann müssen allerdings sämtliche Voraussetzungen einer Einwilligung zur Verarbeitung dieser Daten vorliegen. Prüfen Sie in diesem Fall unbedingt die folgenden Punkte:

- Erfolgt die Einwilligung durch eine eindeutig bestätigende Handlung?
- Erteilen die Beschäftigten die Einwilligung freiwillig? Hierbei ist zu berücksichtigen, dass die Freiwilligkeit im Arbeitsverhältnis insbesondere dann vorliegen kann, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird.
- Erteilen die Beschäftigten die Einwilligung in informierter Weise?
- Ist die Einwilligung unmissverständlich?
- Weist die Einwilligung auf alle Verarbeitungszwecke eindeutig hin?
- Dokumentiert der Verantwortliche die Einwilligung und hält sie zu Nachweiszwecken nach?
- Weist die Einwilligung die Arbeitnehmer auf ihr Widerrufsrecht hin?
- Bezieht sich die Einwilligung bei der Verarbeitung sensibler Daten ausdrücklich auch auf diese Daten?

An dieser Stelle sei darauf hingewiesen, dass der Verantwortliche für entsprechende technische und organisatorische Maß-

WICHTIG

Auf den Punkt gebracht: Der Arbeitgeber kann – zumindest nach derzeitigem Stand – den Impfstatus beim Betreten der Büroräumlichkeiten nur mit ausdrücklicher Einwilligung abfragen.

nahmen für eine etwaige Abfrage sorgen muss. Klären Sie daher:

- Wie werden die Daten erhoben? Mittels ausliegender Liste, elektronisch? Wer hat Zugriff auf die Abfragedaten?
- Wie lange werden diese Daten aufbewahrt?

Außerdem ist eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO nötig. Achten Sie daher darauf, dass der Verantwortliche Sie von Beginn an in den Prozess einbindet, um bei der Umsetzung von technischen und organisatorischen Maßnahmen zu beraten und alle Informationen, die für eine Datenschutz-Folgenabschätzung erforderlich sind, abzufragen.

Anbieten von Impfungen

Ähnlich verhält es sich, wenn der Arbeitgeber seinen Arbeitnehmern Corona-Impfungen anbieten möchte. Eine Impfpflicht besteht in Deutschland nicht. Daher ist es in einem Unternehmen nur auf freiwilliger Basis möglich, eine solche Impfung durchzuführen. Für die Einwilligung müssen die oben genannten Voraussetzungen zur Freiwilligkeit vorliegen.

Die Coronavirus-Impfverordnung (CoronaImpfV) vom 31.03.2021 sieht vor, dass neben Impfzentren und Arztpraxen auch Betriebsärzte eine Corona-Impfung durchführen können. Inwieweit hierbei allerdings arbeitsrechtliche Verpflichtungen für den Arbeitgeber entstehen (z.B. haftungsrechtliche Fragen für den Arbeitgeber, Arbeitsunfähigkeit von Arbeitnehmern aufgrund einer durch den Betriebsarzt durchgeführten Impfung etc.), bleibt ausdrücklich außen vor.

Anbieten und Durchführen von Corona-Tests

Regelmäßige Tests durchzuführen, ist ein wichtiger Bestandteil der Pandemiebekämpfung. Denn die Zahl und Verteilung von infizierten Personen zu erfassen, bildet die Grundlage, um Infektionsketten zu unterbrechen. Im Gegensatz zu einer Impfung stellt ein Corona-Test einen geringeren Eingriff für die Betroffenen dar.

Für die datenschutzrechtliche Beurteilung müssen Sie in einem ersten Schritt danach unterscheiden, welche Pflicht den Arbeitgeber in Bezug auf Corona-Tests überhaupt trifft: das reine „Anbieten" oder auch das „Durchführen".

Was sagt die Corona-ArbSchV?

Die SARS-CoV-2-Arbeitsschutzverordnung (Corona-ArbSchV) dient dazu, das Risiko einer Infektion mit dem Coronavirus am Arbeitsplatz zu minimieren sowie die Sicherheit und Gesundheit der Beschäftigten zu schützen. Zum Zeitpunkt der Erstellung dieses Beitrags wurde die Corona-ArbSchV mit Wirkung zum 23.04.2021 zum dritten Mal geändert.

Bezüglich des Themas „Corona-Test" müssen Arbeitgeber § 5 der Corona-ArbSchV beachten. Danach sind sie verpflichtet, mindestens zweimal pro Kalenderwoche einen Test in Bezug auf einen direkten Erregernachweis des Coronavirus SARS-CoV-2 anzubieten, um das betriebliche Infektionsrisiko zu minimieren. Das gilt, sofern die Beschäftigten nicht ausschließlich in ihrer Wohnung arbeiten, und ist nicht auf bestimmte Berufsgruppen beschränkt. Die Verordnung spricht ausdrücklich von „Anbieten", nicht von „Durchführen".

Arbeitgeber sind darüber hinaus verpflichtet, Nachweise bereitzuhalten, dass sie solche Tests beschafft haben. Sollten Arbeitgeber Dritte mit der Durchführung der Testungen beauftragen, so sind diese Vereinbarungen als Nachweis aufzubewahren. Die Aufbewahrungsfrist gilt für beide Fälle bis zum 30. Juni 2021.

Wichtig an dieser Stelle ist: Die Nachweispflicht bezieht sich nicht auf die tatsächliche Durchführung von Testungen, sondern auf das Beschaffen und damit verbundene „Anbieten" von Testungen.

Tests durch Dritte

Sind Dritte damit beauftragt, Tests durchzuführen, prüfen Sie,

- inwieweit sie personenbezogene Daten der Beschäftigten verarbeiten,
- auf welcher Rechtsgrundlage dies beruht und
- ob bzw. wie sie die Daten dem Arbeitgeber mitteilen.

Denn hier gilt: Das Ergebnis eines Tests mit Namen eines Beschäftigten ist nicht zu übermitteln! Das ändert sich auch nicht dadurch, dass den Arbeitnehmer selbstverständlich die Pflicht trifft, sich nach einem positiven Test umgehend aus den Räumlichkeiten des Arbeitgebers zu entfernen und die weiteren Schritte wie Meldung beim Gesundheitsamt mit entsprechender Kontaktdatenverfolgung einzuleiten.

Testangebot dokumentieren

Streng genommen müssten Arbeitgeber nicht einmal dokumentieren, welchen Arbeitnehmern sie zu welchem Zeitpunkt einen Test ausgehändigt haben. Denn der Nachweis bezieht sich lediglich auf die „Beschaffung" der Tests. Wie kann dann aber der Arbeitgeber sicherstellen, dass er Arbeitnehmern zwei Tests pro Woche angeboten bzw. ausgehändigt hat?

Um einen Nachweis zu erbringen, sollte dokumentiert sein, an welche Mitarbeitenden welche Anzahl von Tests ausgehändigt worden sind – selbstverständlich mit Zugriffsbeschränkungen auf die Dokumentation. Einsicht sollten nur Personen aus dem Office Management, die die Dokumentation vornehmen, und die Geschäftsleitung haben.

So weit zumindest die Vorschriften auf Bundesebene. Die Länder haben z.T. Regelungen, die sich davon unterscheiden. Denken Sie an dieser Stelle insbesondere daran, das Verzeichnis von Verarbeitungstätigkeiten zu aktualisieren und die entsprechenden Rechtsgrundlagen zu dokumentieren – je nachdem kann dies die jeweilige Länderregelung oder aber § 5 Corona-ArbSchV in Verbindung mit Art. 6 Abs. 1 Buchst. c DSGVO sein.

Prozesse definieren

Definieren Sie die Prozesse, wie die Aushändigung und ggf. Durchführung →

Testpflicht in der Pflege u.Ä.

Regelungen der Länder zu Corona-Tests

Die Länder haben teilweise sehr unterschiedliche Regelungen in Bezug auf das Anbieten oder gar auf die Verpflichtung, Testungen durchzuführen. Die abweichenden Regelungen betreffen z.B. bestimmte Einrichtungen wie Pflegedienste. Datenschutzbeauftragte sollten daher die Regelungen, die im jeweiligen Bundesland einschlägig sein, beobachten und den Verantwortlichen dementsprechend beraten.
Herausfordernd wird es, wenn mehrere Gesellschaften in unterschiedlichen Bundesländern tätig und daher unterschiedliche Regelungen zu beachten sind. Eine enge Abstimmung dahingehend mit der Personalabteilung bzw. dem Office Management ist dann unumgänglich.

der Testungen im Detail vonstattengehen mit sämtlichen technischen und organisatorischen Maßnahmen. Das heißt insbesondere:

- Empfehlen Sie, den Personenkreis so klein wie möglich zu halten, der auf die Aushändigung und ggf. Durchführung der Mitarbeiter-Testungen Zugriff hat – z.B. das Office Management oder die Personalabteilung.
- Raten Sie davon ab, Listen auszulegen, in die sich die Mitarbeiter selbst eintragen. Denn so können die Kolleginnen und Kollegen Daten anderer Mitarbeitender einsehen.

Datenschutz-Folgenabschätzung

Sofern auch Ihr Bundesland Testungen vorschreibt, denken Sie daran, dass der Verantwortliche bei der Verarbeitung von Gesundheitsdaten eine Datenschutz-Folgenabschätzung nach Art. 35 Abs. 3 Buchst. b DSGVO durchführen muss.

Behalten Sie dabei die aktuellen Änderungen im Auge. Kurz vor Abgabe dieses Artikels hat beispielsweise der Freistaat Bayern ab dem 06.05.2021 – und damit früher als der Bund – vollständig Geimpfte und Genesene in vollem Umfang negativ getesteten Personen gleichgestellt. Sollten andere Bundesländer ähnliche Regelungen treffen, sind Testungen hoffentlich bald überflüssig.

Büro-Organisation

Die Corona-ArbSchV sieht eine Vielzahl von Bestimmungen vor, um für die Mitarbeiter das Risiko einer Corona-Infektion bei der Arbeit zu minimieren. Die wichtigsten Eckpfeiler dabei sind:

- Mindestabstand von 1,5 m
- Tragen medizinischer Gesichtsmasken
- Hygienekonzept
- regelmäßiges Lüften
- wenn möglich: Einteilen von festen Arbeitsgruppen
- Pro Person müssen 10 m² zur Verfügung stehen, wenn sich Kollegen die Räumlichkeiten teilen.

Gerade der letzte Punkt ist in den meisten Unternehmen an der Tagesordnung. Denn es dürfte selten der Fall sein, dass der Arbeitgeber allen Mitarbeitenden ein Einzelbüro anbieten kann. Auch Großraumbüros oder „Share-a-desk"-Konzepte sind nichts Neues mehr.

„Book a desk"

Einige Unternehmen bieten mittlerweile sogenannte „Book-a-desk"-Services an. Dabei können Mitarbeiter ihren Schreibtisch im Vorfeld buchen und bestimmen, welchen Platz mit welcher technischen Ausrüstung sie für welche Dauer benötigen. Damit hat der Arbeitgeber einen Überblick, wie viele Mitarbeitende anwesend sind, kann Schreibtische „sperren", um den Mindestabstand zu wahren, und kann „Desinfizierungspausen" einbauen, sodass nach erfolgter Benutzung der Tisch erst wieder nach einer bestimmten Zeit an den Nächsten vergeben wird. So kann er den Hygienevorschriften nachweislich nachkommen.

Mit QR-Code einchecken

Dieser Service ist oft mit einer App-Nutzung verbunden: Beschäftigte müssen bei Arbeitsantritt einen QR-Code scannen, der sich auf dem gebuchten Schreibtisch befindet, und somit „einchecken". Stellen Sie als DSB dem Arbeitgeber dabei insbesondere die folgenden Fragen:

- Ist die geplante Lösung eine SaaS- oder On-Premises-Lösung? Sprich: Kaufen wir die Nutzung in der Cloud ein oder hosten wir sie selbst?
- Wo werden die Daten gespeichert? In der EU/im EWR oder in Drittstaaten?
- Wie ist ein ggf. stattfindender Datentransfer in Drittstaaten aus Datenschutzsicht abgesichert (Standardvertragsklauseln, zusätzliche Maßnahmen)?
- Wie sind die Zugriffsberechtigungen geregelt?
- Sieht man Daten der Kollegen? Wenn ja: Welche? Gibt es eine Erforderlichkeit hierfür?
- Welche Schlussfolgerungen zieht der Arbeitgeber, wenn ein Mitarbeiter trotz Buchung nicht erscheint? Binden Sie hierbei unbedingt die Rechtsabteilung ein und – falls vorhanden – den Betriebsrat.
- Werden sensible Daten verarbeitet, z.B. weil der Verantwortliche behindertengerechte Plätze anbietet? Das hätte zur Folge, dass er für die Verarbeitung dieser Daten Art. 9 DSGVO beachten muss.

Auch hier gilt: Aktualisieren Sie beim Einsatz solcher Tools das Verzeichnis von Verarbeitungstätigkeiten bzw. weisen Sie den Verantwortlichen auf die Notwendigkeit hin, das Verzeichnis anzupassen!

Doris Kiefer ist Rechtsanwältin und leitet als Head of Data Protection das Datenschutzteam eines im SDAX gelisteten E-Commerce-Unternehmens.

Bild: iStock.com/Imagesines

Kein schönes, aber ein durchaus notwendiges Thema: Was tun mit Daten verstorbener Beschäftigter?

Möglichst viel mit Betriebsvereinbarungen regeln!

Todesfälle im Betrieb aus Sicht des Datenschutzes

Was gebietet der Anstand, und was ist datenschutzrechtlich zulässig? Ist die nötige Sensibilität bei anderen Themen oft wenig ausgeprägt, bekommt im Angesicht des Todes der Datenschutz eine neue Bedeutung; zu groß ist die Angst, in ein Fettnäpfchen zu treten.

Versterben Mitarbeiter plötzlich, reißt dies eine große Lücke in das Leben von Familie und Freunden. Aber nicht nur das Privatleben ist betroffen: War der Verstorbene ein geschätzter langjähriger Mitarbeiter in einem Unternehmen, entsteht auch am Arbeitsplatz und im Kollegenkreis eine plötzliche Leere. Während das Erbrecht den Nachlass – und mittlerweile sogar den sogenannten „digitalen Nachlass" – von Verstorbenen regelt, ist in Unternehmen nach dem Tod einer Mitarbeiterin oder eines Mitarbeiters guter Rat oft teuer.

Persönliche Gegenstände und Unterlagen im Büro bleiben ebenso zurück wie das persönliche E-Mail-Postfach und das persönliche Daten-Laufwerk auf dem Unternehmensserver. Soll es einen Nachruf in einer lokalen Zeitung oder sogar im Internet geben? Soll den Angehörigen das Beileid in Form einer Trauerkarte oder eines Gestecks für das Grabmal ausgesprochen werden?

Nicht selten greifen Chefs zu diesem Zeitpunkt zum Telefon, um mit ihrem Datenschutzbeauftragten (DSB) wichtige Fragen zu klären. Um sie nicht erst im Ernstfall beantworten zu müssen, gehen Sie doch im Rahmen einer Schulung einmal die zentralen Punkte durch.

Was sagt die DSGVO?

Nach Art. 1 Abs. 2 schützt die Datenschutz-Grundverordnung (DSGVO) die Grundrechte und Grundfreiheiten natürlicher Personen. Unter „natürlicher Person" versteht man den Menschen selbst als Träger von Rechten und Pflichten. Seine Rechtsfähigkeit beginnt mit der Geburt und endet mit dem Tod. Per Definition fallen Verstorbene daher nicht in den Geltungsbereich der DSGVO.

Zur Verdeutlichung hat der Unionsgesetzgeber in Erwägungsgrund 27 ergänzt, dass „diese Verordnung nicht für die personenbezogenen Daten Verstorbener gilt".

Zwar enthält Erwägungsgrund 27 neben der angesprochenen Regelung eine sogenannte „Öffnungsklausel" bzw. eine „Konkretisierungsklausel". Danach können die Mitgliedstaaten eigene Vorschriften für die Verarbeitung personenbezogener Daten Verstorbener erlassen. Der deutsche Gesetzgeber hat davon bisher allerdings keinen Gebrauch gemacht.

Informationelle Selbstbestimmung und das postmortale Persönlichkeitsrecht

Wirft man einen Blick in die Todesanzeigen-Spalten der lokalen Tageszeitung, finden sich dort unterschiedliche Angaben zur Person des Verstorbenen. Der Name sowie das Geburts- und Sterbedatum gehören dabei zum Standardrepertoire. Hört der Datenschutz nach dem Tod also wirklich auf?

Das Grundrecht der informationellen Selbstbestimmung, das dem Datenschutz zugrunde liegt, schützt nach herrschender Meinung die Erwartung des noch Lebenden, dass die über ihn gespeicherten Daten auch nach seinem Tod nicht jedermann frei zugänglich sind.

Daneben existiert ein sogenanntes „postmortales Persönlichkeitsrecht". Es handelt sich dabei um einen Achtungsanspruch, der jedem lebenden Menschen innewohnt und unveräußerlich ist. Er besteht auch nach dem Tod fort. Bei seiner Verletzung können die Angehörigen von Verstorbenen zumindest einen zivilrechtlichen Abwehranspruch geltend machen.

Mit Todesfällen im Unternehmen umgehen

Neben Behörden, Vereinen und Kirchen gehören in erster Linie Unternehmen in ihrer Funktion als Arbeitgeber zum →

Kreis derer, die sich mit der Verarbeitung personenbezogener Daten Verstorbener konfrontiert sehen.

Im Folgenden seien die drängendsten Fragestellungen und die häufigsten Fallkonstellationen beleuchtet.

Was geschieht mit dem dienstlichen persönlichen E-Mail-Postfach?

Das dienstliche persönliche E-Mail-Postfach ist in erster Linie für den dienstlichen Gebrauch bestimmt. Es umfasst neben der rein dienstlichen Kommunikation wie dem Austausch von Arbeitsergebnissen auch die teils dienstliche, teils persönliche Kommunikation wie etwa den Schriftwechsel mit dem Betriebsarzt, dem Betriebsrat oder der Personalabteilung. Ob darüber hinaus eine private Nutzung erlaubt ist, regelt für gewöhnlich eine entsprechende Betriebsvereinbarung.

- Ist die Privatnutzung untersagt, haben Angehörige des Verstorbenen keine Möglichkeit, auf Inhalte des Postfachs zuzugreifen.
- Doch auch dann, wenn der Arbeitgeber die Privatnutzung duldet bzw. gestattet, ist davon auszugehen, dass die Kommunikationsinhalte persönliche oder gar intime Belange des Verstorbenen betreffen können. Einer uneingeschränkten Zugriffsmöglichkeit der Angehörigen steht in diesem Fall das postmortale Persönlichkeitsrecht des Verstorbenen entgegen.

Ausnahmen können sich ergeben, wenn die Informationen zur Geltendmachung weiterer Ansprüche der Angehörigen des Verstorbenen zwingend erforderlich sind. In so einem Fall ist insbesondere der Grundsatz der Datenminimierung zwingend zu beachten.

Was geschieht mit dem dienstlichen persönlichen Laufwerk des Verstorbenen?

In Unternehmen gibt es in der Regel mindestens ein zentrales gemeinsames Laufwerk, auf dem die Beschäftigten Arbeitsergebnisse und sonstige firmen- bzw. betriebsbezogene Daten speichern und verwalten. Daneben bekommt jeder Mitarbeiter oftmals ein dienstliches persönliches Laufwerk. Es ist zwar nicht für die private, jedoch für die arbeitsbezogene persönliche Nutzung bestimmt.

Typische Datenkategorien, die nicht der privaten, aber der arbeitsbezogenen persönlichen Nutzung unterfallen, sind dabei beispielsweise Lohnabrechnungen, Krankmeldungen oder Urlaubsanträge. Denkbar ist auch, dass der Verstorbene Mitarbeitergespräche, Beurteilungen oder gar Abmahnungen in seinem dienstlichen persönlichen Laufwerk abgelegt hat.

PRAXIS-TIPP

Im Idealfall regelt eine entsprechende Betriebsvereinbarung, dass die private Nutzung des persönlichen Laufwerks ausgeschlossen ist. In diesem Fall stellt sich die Frage, was mit den Daten geschieht, die der Verstorbene dort gespeichert hat, nicht. Ein Zugriff durch Angehörige ist ausgeschlossen.

Gibt es im Unternehmen jedoch keine solche Betriebsvereinbarung oder ist die private Nutzung geduldet bzw. gestattet, so könnten die Angehörigen des Verstorbenen auf die Idee kommen, Zugriff auf die privaten Datenbestände zu verlangen. Auch hier steht – wie im vorhergehenden Abschnitt erwähnt – einem uneingeschränkten Zugriff der Angehörigen das postmortale Persönlichkeitsrecht des Verstorbenen entgegen.

Etwas anderes darf auch hier ausnahmsweise nur gelten, wenn die Informationen zwingend erforderlich sind, damit Angehörige weitere Ansprüche geltend machen können.

Was muss der Arbeitgeber bei Beileidsbekundungen beachten?

Beileidsbekundungen wie die Veröffentlichung einer Todesanzeige, die Kranzniederlegung am Grab oder das Halten einer Trauerrede anlässlich der Beerdigung eines verstorbenen Mitarbeiters sind in den meisten Unternehmen fest in der Unternehmenskultur verankert.

Gemein ist solchen Beileidsbekundungen der Umstand, dass der Arbeitgeber personenbezogene Daten des bzw. der Verstorbenen veröffentlicht und damit verarbeitet. Dies betrifft neben dem Namen in der Regel das Sterbedatum und die ehemalige Abteilung bzw. Organisationseinheit, der die oder der Verstorbene angehörte.

Um eine entsprechende Rechtsgrundlage zu schaffen und datenschutz- sowie persönlichkeitsrechtliche Belange der Betroffenen noch zu Lebzeiten bestmöglich zu berücksichtigen, empfiehlt es sich, eine Betriebsvereinbarung abzuschließen. Existiert keine Vereinbarung, können Arbeitgeber später nur auf das berechtigte Interesse des Unternehmens im Sinne von Art. 6 Abs. 1 Buchst. f DSGVO zurückgreifen.

Art. 13 DSGVO bestimmt darüber hinaus, dass Unternehmen transparent über die Verarbeitung informieren müssen. Das muss zumindest hinsichtlich der Angehörigen des Betroffenen und ggf. weiterer Personen gelten, die die Todesanzeige nennt. Dabei ist in erster Linie darüber zu informieren, wo die Anzeige veröffentlicht werden soll (Tageszeitung, Internet, Social Media etc.). An die Form der Information sind für gewöhnlich keine allzu hohen Anforderungen zu stellen. (So auch das bayerische Landesamt für Datenschutzaufsicht: www.lda.bayern.de/media/bayl-da_report_08.pdf, S. 44.)

PRAXIS-TIPP

Ein freundliches Gespräch mit den Angehörigen der oder des Verstorbenen zeugt nicht nur von Rücksichtnahme und Sensibilität, sondern sichert gleichzeitig den respektvollen Umgang mit den personenbezogenen Daten der bzw. des Verstorbenen.

Jana Thieme, Dipl.-Jur. Univ., ist Geschäftsführerin und Datenschutzexpertin der TH Datenschutz+ GmbH (info@th-datenschutz.plus).

Bild: iStock.com/metamorworks

Der zweite Teil setzt die Anforderungen an die Fernwartung fort. Außerdem geht es um Geräte des Internet of Things, sei es die Kaffeemaschine, eine Klima- oder eine Messkomponente.

Datenübermittlung

Schutzverletzung bei Wartungszugriffen von außen vermeiden (Teil 1)

Maschinen in der Produktion müssen gewartet werden. Dazu sind entweder Wartungsintervalle vorgegeben oder es erfolgt eine Ad-hoc-Wartung, wenn es zu einer Störung kommt. Wie verhindern Verantwortliche, dass es dabei zu Datenpannen kommt, weil Techniker auf Daten zugreifen, die nicht für sie bestimmt sind?

Früher kam der Wartungstechniker vorbei, wenn der Zeitpunkt für die Wartung gekommen war. Kam es zu einer Störung, wurde der Techniker informiert. Im ungünstigsten Fall setzte er sich ins Auto und fuhr vor Ort. Im günstigsten Fall konnte er am Telefon eine Anleitung geben, wie die Störung zu beseitigen ist.

Früher kam der Techniker persönlich, heute digital

Durch die Digitalisierung ist es immer häufiger so, dass die Geräte oder Maschinen integrierte Messgeräte und/oder Sensoren haben, die die erforderlichen Daten an den Wartungsdienst übermitteln. Es kann auch sein, dass der Wartungsdienst temporären oder permanenten Zugriff hat, um eine Störung rasch zu beseitigen.

Oder, und das ist immer häufiger der Fall: Die Daten lassen sich für Prognosen nutzen, wann mutmaßlich ein Wartungs- oder Störfall außerhalb des üblichen Wartungsintervalls eintritt. Das frühe Erkennen möglicher Störungen wird immer beliebter. Denn es verringert die Wahrscheinlichkeit eines teuren Produktionsausfalls.

Was geht das den Datenschutz an?

Das alles erweckt den Anschein, als könnte das dem Datenschutz egal sein. Das ist jedoch nicht so. Denn die Messgeräte und Sensoren übermitteln grundsätzlich nicht nur Daten, die die Abläufe in der Maschine betreffen, sondern in der Regel auch personenbezogene Daten der Fachkräfte, die gerade an der Maschine arbeiten oder zuvor dort gearbeitet haben.

Möglicherweise enthält die Elektronik der Maschine auch weitere Daten wie Produktionsmenge, Pausenzeiten oder Fehlereintritt sowie Fehlerhäufigkeit bei einer beschäftigten Person, auf die ein Wartungsdienst ebenfalls zugreifen kann. Damit werden auch personenbezogene Daten verarbeitet.

Datenschutz einbinden

Aus diesem Grund muss der Datenschutz in die Verarbeitung dieser Daten eingebunden sein und die Abläufe kennen. Nach Art. 39 Abs. 2 Datenschutz-Grundverordnung (DSGVO) sind Datenschutzbeauftragte verpflichtet, zu →

Überblick verschaffen

Gehen Sie in die Produktion und fragen Sie bei beliebigen Maschinen oder Anlagen, wie diese gewartet werden. Sie werden vermutlich unterschiedliche Wartungsvarianten vorfinden. Welche möglich sind, zeigt die Tabelle auf der nächsten Seite.

Wartungsszenario	Risiko
Szenario eins: Datenzugriff nach Meldung des Unternehmens, anschließender Support	Eine beschäftigte Person meldet eine Störung an den Supportdienstleister. Der Support erfolgt entweder, sofern möglich, digital, oder es kommt ein Servicetechniker. **Risiko: eher gering**
Szenario zwei: Datenzugriff nach Meldung des Unternehmens, automatischer Support	Die Meldung einer beschäftigten Person löst einen automatischen Support aus. Das setzt allerdings voraus, dass es sich um einen klassifizierbaren Wartungsfall handelt. Klären Sie, ob hier eine fachkundige Person aus dem auftraggebenden Unternehmen eingebunden ist. Das ist auf alle Fälle sinnvoll, damit sie den Wartungszugriff bei Bedarf unterbinden kann. **Risiko: eher normal**
Szenario drei: permanenter Datenzugriff, Vorschlag Support	Der Wartungsdienst hat einen permanenten Datenzugriff oder es erfolgt ein permanenter Datenzugriff, der bei Bedarf eine Unstimmigkeit an den Wartungsdienst meldet. Das löst einen Vorschlag für einen Support aus, der in der Folge entweder aus der Ferne erfolgt oder durch den Wartungseinsatz eines Technikers. Beim Support aus der Ferne sollte eine fachkundige Person aus dem Unternehmen dabei sein, die in der Lage ist, im Zweifelsfall den Vorgang abzubrechen. **Risiko: größer**
Szenario vier: permanenter Datenzugriff, automatischer Support	Der für das auftraggebende Unternehmen bequemste, aber aus Datenschutzsicht riskanteste Weg ist Szenario vier. Hier erfolgt ein permanenter Datenzugriff, und soweit lösbar, kommt es auch zu einem automatischen Support. In diesem Fall ist mutmaßlich keine fachkundige Person des auftraggebenden Unternehmens beteiligt. Daher muss auf anderem Weg sichergestellt sein, dass keine unbefugten Zugriffe auf personenbezogene Daten erfolgen. Möglich ist auch, dass nach einer Gefährdungsmeldung ein Wartungstechniker losfährt, im Unternehmen aber noch gar nicht bekannt ist, dass es zu einem Störfall kommen wird und eine Wartung erforderlich ist. **Risiko: hoch**

Die vier grundsätzlichen Szenarien bei der Wartung und ihr Risiko aus Datenschutzsicht

Sensibilisieren hilft

Erfahrungsgemäß freut sich kaum jemand, wenn Datenschutzbeauftragte aufschlagen. Die Reaktion gerade von Prozessverantwortlichen für Wartungsvorgänge ist durchwachsen nach dem Motto: „Jetzt haben wir schon so viel zu tun und sollen auch noch den Datenschutz zufriedenstellen?" Anders kann es aussehen, wenn die Prozessbeteiligten eigens geschult wurden. Prüfen Sie daher, ob alle Verantwortlichen für Wartungsarbeiten hinreichend sensibilisiert sind und ob die Projektcheckliste den Kontakt zum Datenschutz vorgibt, wenn Wartungsaufträge erteilt werden.

überwachen, inwieweit der Verantwortliche die Vorgaben der DSGVO umsetzt. Demzufolge müssten eigentlich die Prozessverantwortlichen von sich aus Datenschutzbeauftragte (DSB) in die Gestaltung der Prozesse einbinden. Die Praxis sieht jedoch eher so aus, dass DSB sich selbst darum kümmern müssen, welche personenbezogenen Daten im Rahmen der Wartungsvorgänge verarbeitet werden.

Sind Leistungsdaten und Profile entstanden?

Ist hinlänglich geklärt, warum Sie als DSB ein Interesse an den Vorgängen rund um die Wartung von Maschinen und Anlagen haben, gehen Sie in der Prüfung den nächsten Schritt. Klären Sie, auf welche Daten Wartungsdienste konkret zugreifen können. Das hängt davon ab, zu welchen Zwecken und wie viele Daten von beschäftigten Personen die Anlagen verarbeiten:

- Ist es z.B. üblich, Leistungsdaten wie die Anzahl der produzierten Teile zu ermitteln, um sie als Grundlage für die Bezahlung einzusetzen, haben diese Daten wahrscheinlich nichts beim Wartungsdienst verloren.
- Sind sie erforderlich, um die Leistungsfähigkeit einer Maschine beurteilen zu können, muss klar sein, dass die personenbezogenen Daten der dort arbeitenden Personen nur angemessen pseudonymisiert übermittelt werden dürfen. Vermutlich ist in diesem Fall der Betriebsrat einbezogen, weil hier Daten zur Kontrolle von Verhalten und Leistung beteiligt sind. Ob die Prozesseigner daran gedacht haben, den Datenschutz zu informieren, steht auf einem anderen Blatt.

Nur aktuelle personenbezogene Daten oder mit Historie?

Prüfen Sie zudem, ob nur die Daten der derzeit an der Maschine oder Anlage arbeitenden Personen übermittelt werden oder ob es eine Historie gibt, über die sich zurückverfolgen lässt, wer wann an der Maschine gearbeitet hat. Ohne eine Löschroutine könnten so auch längst zurückliegende Daten übermittelt werden, und zwar im ungünstigsten Fall seit Aufstellen der Maschine. Oder eben so lange, bis der Speicher alte Daten überschreibt, weil die Speicherkapazität erschöpft ist.

Das sollte im Verzeichnis der Verarbeitungstätigkeiten erfasst sein. Das setzt aber voraus, dass die Produktion diese Datenverarbeitung überhaupt als Verarbeitungstätigkeit gemeldet hat. Erfahrungsgemäß ist das eher selten der Fall.

Risiko ermitteln und bewerten

Normalerweise unterliegen die Daten der Personen, die an der Maschine arbeiten, aus Sicht des Datenschutzes auf den ersten Blick nur einem relativ niedrigen Risiko. Nehmen Sie das Schutzstufenmodell der Datenschutzkonferenz als Basis, so sind Vorname und Nachname der Person, die dort arbeitet, sowie die Zeit, wann sie die Arbeiten begonnen und wann sie sie beendet hat, einschließlich der Pausen, Daten der Schutzstufe B. Es sind also Daten, bei denen für die Rechte und Freiheiten der betroffenen Personen nur ein geringes Risiko besteht.

Allerdings lassen sich in Kombination mit anderen Daten, etwa mit der Menge der produzierten Produkte oder Waren, auch Profile über Verhalten und Leistung ermitteln. Damit bewegt sich die Datenübermittlung im Bereich der Beurteilungsdaten. Nach dem Schutzstufenmodell befinden wir uns in der Kategorie D, also bei Daten mit einem erheblichen Risiko für die Rechte und Freiheiten betroffener Personen.

Fernwartung planen

Wissen Sie, welche Anlagen, Maschinen und informationstechnischen Systeme Techniker durch Fernwartung in welcher Form auch immer warten, prüfen Sie, ob es einen geplanten Ablauf gib. Er muss regeln, wie die Fernwartung konkret abläuft und wie mögliche Gefährdungen minimiert werden. Im Idealfall existiert für jede Maschine und Anlage ein Ablaufplan mit spezifischen Regeln.

Wartung im normalen IT-Netz oder ein einem eigenen Wartungsnetz?

Eine der zentralen Fragen bei der Fernwartung ist, ob sie innerhalb des normalen informationstechnischen Netzes des Unternehmens erfolgt, (auch als In-Band bezeichnet), oder ob ein eigenes Administrationsnetz für die Wartungszwecke eingerichtet ist (auch als Out-of-Band bezeichnet).

Einerseits ist ein eigenes Netz für Wartungszwecke aufwendig. Es gilt, immer mehr reale Gefährdungen bei immer mehr Wartungsmodulen, die über das Internet gesteuert werden, und immer mehr anderen Geräten des Internet of Things (IoT) einzudämmen. Hier ist es kaum noch möglich, den Überblick zu behalten, welche davon den aktuellen Gefährdungen trotzen und welche nicht. Andererseits minimiert ein eigenes Netzwerk für Fernwartung die Risiken erheblich. Diese Entscheidung ist u.a. davon abhängig, wie groß der Schaden durch den Ausfall nach einem erfolgreichen Angriff auf einzelne Maschinen und Anlagen ist. Außerdem lässt sich durch eine getrennte Netzverwaltung das Verwaltungsnetz besser schützen.

Prüfen Sie, ob ein eigenes Netzwerk für Wartungen eingerichtet ist oder ob es erforderlich wäre. Um das zu beurteilen, ermitteln Sie, wie kritisch Ausfälle ohne Fernwartung oder durch falsche Fernwartung für die Abläufe sind und inwieweit ein durch Wartung erleichterter Hacker-Angriff massive Störungen auslösen kann.

Weitere wichtige Fragen zur Fernwartung

- Welche Schnittstellen und Protokolle werden für die Fernwartung verwendet?
- Welche personenbezogenen Daten sind im Rahmen der Fernwartung betroffen? Handelt es sich um pseudonymisierte Daten, etwa wenn das Bedienpersonal der zu wartenden Maschine nur eine Nummer als Kennung eingibt, sind Klarnamen vorhanden oder gar ganze Profile wie Leistungszahlen, produzierte Stückzahlen oder Qualitätsprofile? Je nachdem sind die Anforderungen an die Vertraulichkeit des Wartungspersonals höher oder geringer einzustufen. Achtung! Das kann für jede Maschine/Anlage anders sein!
- Gibt es gesetzliche (z.B. ärztliche Schweigepflicht bei medizinischen Geräten) oder interne Pflichten oder Compliance-Regelungen, die berücksichtigt werden müssen? Gibt es z.B. Bereiche, bei denen ein Zugriff durch Dienstleister per Vertrag mit dem Auftraggebern untersagt ist?
- Hat der Verantwortliche den Dienstleister selbst überprüft, oder handelt es sich um einen Dienstleister, den der Maschinenlieferant quasi durch die Hintertür implementiert hat? Konkret: Wer trägt die Verantwortung, wenn etwas schiefgeht?
- Auf welchem Weg erfolgt die Fernwartung? Dürfen Online-Dienste zur Fernwartung herangezogen werden, bei denen eine Kontrolle durch den Verantwortlichen eigene Prüfkriterien erfordert?
- Wer begleitet die Fernwartung intern? Je stärker automatisiert die Wartungs- →

PRAXIS-TIPP

- **Ermitteln Sie, ob Sie in die Wartungsprojekte eingebunden sind – oder ob das bisher nur z.T. oder gar nicht der Fall ist.**
- **Prüfen Sie, welche Daten der beschäftigten Personen, die an der Maschine oder Anlage arbeiten, konkret verarbeitet werden und wie sie sich mit Leistungsdaten verknüpfen lassen.**
- **Prüfen Sie, ob die personenbezogenen Daten im Klartext erfasst sind oder pseudonymisiert und ob die Wartung als Verarbeitungstätigkeit erfasst ist.**
- **Versuchen Sie, herauszubekommen, wie, wo und wie lange genau die Speicherung dieser Daten erfolgt.**

PRAXIS-TIPP

Prüfen Sie, welche Möglichkeiten für den Verbindungsaufbau bestehen. Leider kann es sein, dass Ihre IT sich da raushält, denn sie sieht sich ggf. nicht für die IT in der Produktion zuständig. Hier gilt es zu klären, wer dann zuständig ist. Das sei am Beispiel Energielieferung gezeigt: Hier muss gesetzlich eine Trennung von Netzbetrieb und Energielieferung erfolgen. Das hat normalerweise zwei IT-Bereiche unter getrennter Leitung zur Folge. Die eine IT weiß normalerweise nichts von der andern IT – aber beide müssten bei der Fernwartung zusammenwirken.

zugriffe erfolgen, desto schwieriger wird es, dass Beschäftigte die Fernwartungsvorgänge strukturiert begleiten. Außerdem dürfte die Zahl derjenigen, die sich gut mit Wartungsarbeiten auskennen, begrenzt sein.

- In welche Segmente muss das Netz separiert sein, über das die Fernwartungszugriffe erfolgen? Es ist wenig sinnvoll, alle Wartungszugriffe über ein einziges Netzsegment laufen zu lassen. Würde hier ein Angriff durchschlagen, ließe sich der gesamte Wartungsbereich außer Kraft setzen. Je mehr Netzsegmente aber vorhanden sind, desto komplexer ist es, sie zu verwalten und zu überprüfen.

Wie sicher ist der Verbindungsaufbau?

Beim Verbindungsaufbau kommt es darauf an, ob jemand unternehmensintern den Zugriff für die Fernwartung öffnen muss oder ob der Zugriff automatisiert erfolgt. Im ersten Fall hat das Unternehmen in der Regel Einfluss auf die Qualität der Verbindung. Normalerweise kommt als gesicherte Verbindung nur VPN o.Ä. infrage. Was aber, wenn Maschinenkomponenten als IoT-Komponenten geführt werden und der wartende Dienstleister sie ohne Zutun des Verantwortlichen zu jeder Zeit ansprechen kann? Empfehlen Sie, klare Regelungen zu treffen und ggf. dauerhaft sichere Leitungskapazitäten bereitzuhalten, mindestens sofern sicherheitskritische Maschinen und Anlagen zu warten sind. Und wenn sensible personenbezogene Daten übermittelt werden bzw. Wartungstechniker auf solche Daten zugreifen können.

Am besten ist es, wenn sich die Support-Mitarbeiter zu Beginn der Wartung, möglichst mit Mehrfaktorauthentifizierung, anmelden müssen. Kommt es zu Unterbrechungen der Verbindung, sollte sichergestellt sein, dass die Session beendet wird und der Support-Mitarbeiter den Zugriff auf das System erneut aufbauen muss.

Ausblick

Beim ersten Mal gestaltet sich das „Einmischen" des Datenschutzes in die Wartungsarbeiten erfahrungsgemäß eher holprig. Haben die Beteiligten aber verstanden, dass sie ja auch Beratung bekommen, werden sich weitere Prüfzyklen deutlich flüssiger gestalten. Angesichts der Herausforderungen der Künstlichen Intelligenz und der Quantencomputer stehen wir bei den Wartungsaufgaben erst am Anfang. Da schadet es nicht, jetzt schon auf einem guten Stand zu sein.

Eberhard Häcker ist seit vielen Jahren als externer Datenschutzbeauftragter tätig und weiß daher, wo sich überall personenbezogene Daten verstecken.

Übersicht verschaffen

Zur Wartung zu klärende Fragen

Um zur Wartung eine aussagekräftige Beurteilung aus Datenschutzsicht vornehmen zu können, lassen Sie sich mindestens folgende Fragen beantworten:

- Existiert eine vollständige und aktuelle Übersicht, für welche Maschinen, Produktionsanlagen oder einzelne Geräte Wartung erfolgt?
- Ist bekannt, für welche Maschinen, Produktionsanlagen oder Geräte Wartungsverträge vorhanden sind?
- Ist der Ablauf der Wartung aktuell, vollständig definiert und protokolliert? (Was löst die Wartung aus, wer ist beteiligt, gibt es externe Zutritte zu den Anlagen oder erfolgt die Wartung in elektronischer Form, ist eine Person aus dem Unternehmen bei der Wartung dabei und kann im Zweifelsfall eingreifen usw.?)
- Insbesondere sind die Fälle von Interesse, bei denen ein Wartungszugriff über das Internet erfolgt und das Messgerät von der Maschine, Produktionsanlage oder dem einzelnen Gerät in ein Netzwerk (LAN, WLAN, VLAN) beim Unternehmen eingebunden ist.
- Besteht die Gefahr, dass durch falsche Konfiguration über das Netzwerk Zugriffe auf andere Bereiche des Unternehmens erfolgen können?
- Hätte das möglicherweise zur Folge, dass Dritte weitere personenbezogene Daten abgreifen können?
- Lassen sich Firmware-Fehler, die nicht behoben werden, bei eingebauten Messgeräten oder Sensoren ausschließen?
- Oder wird das Gerät in diesem Fall wenigstens abgeschaltet? Denn sonst könnten Angreifer sowohl die personenbezogenen als auch anderweitig schützenswerte Daten abziehen.
- Gibt es eine Übersicht oder kann diese anfertigt werden, in welchen Fällen welcher Wartungszugriff mit welcher Technik erfolgt, um die entsprechende Verarbeitungstätigkeit aufnehmen zu können und sowohl Hinweise für den Datenschutz als auch für die Informationssicherheit zu sammeln?

Wahrung der Vertraulichkeit

Anfragen an den DSB

Anfragen, die ausdrücklich an den Datenschutzbeauftragten (DSB) eines Unternehmens gerichtet sind, muss ihm das Unternehmen direkt zuleiten. Die Zuleitung muss dabei ausschließlich an den DSB erfolgen. Jede Kenntnisnahme des Inhalts durch weitere Personen ist unzulässig. Auf diese Vorgaben hat die Datenschutzaufsicht Berlin hingewiesen.

Verschwiegenheitspflicht!

Die Kontaktdaten des DSB müssen veröffentlicht werden (Art. 37 Abs. 7 DSGVO). Dies geschieht häufig im Rahmen einer Datenschutzerklärung. Wer diese Kontaktdaten für eine Anfrage verwendet, muss sich darauf verlassen können, dass ausschließlich der DSB die Anfrage zur Kenntnis nehmen kann. Das ergibt sich aus der Verschwiegenheitspflicht des DSB (Art. 38 Abs. 5 DSGVO). Damit ist es nicht vereinbar, wenn ein Unternehmen E-Mails, die ausdrücklich an den DSB gerichtet sind, auch noch an die IT-Leitung oder den Kundenservice weitergibt.

Eigene Kontaktformulare und eigene Mailadresse

Unklarheiten darüber, an wen eine Nachricht geht, muss das Unternehmen durch organisatorische Maßnahmen ausschließen. Deshalb darf es für den Kontakt zum DSB auch nicht dasselbe Formular anbieten wie für den Kontakt zu anderen Bereichen des Unternehmens. Vielmehr sind besondere Kontaktformulare und Mailadressen für den DSB vorzusehen.

Briefpost oder E-Mails, die ausdrücklich an den DSB gerichtet sind, darf niemand anderes im Unternehmen öffnen oder lesen, auch nicht die Poststelle. Erfordert es die Zahl der eingehenden Anfragen, ist der DSB durch geeignete Mitarbeiter zu unterstützen (Art. 38 Abs. 2 DSGVO). Sie dürfen nur nach den Vorgaben des DSB tätig werden. Die Vertraulichkeit muss auch in diesem Fall gewahrt bleiben. Die „Entscheidungshoheit" über eingehende Anfragen muss stets ausschließlich beim DSB liegen.

Quelle: Datenschutzaufsicht Berlin, Jahresbericht 2020, Nr. 10.8 (Seiten 163/164), abrufbar unter https://ogy.de/zafta-tb-berlin-2020.

Bild: iStock.com/Elena Lukyanova

Initiative von Fraunhofer

Allianz Cloud Computing

Zuverlässige Basisinformationen, die auch für DSB nützlich sind, bietet das Informationsportal „Fraunhofer-Allianz Cloud Computing – IT-Dienste aus der Wolke". Ein „Kleines Einmaleins der Cloud-Nutzung" erläutert, wann sich die Nutzung einer Cloud lohnt und welcher Aufwand damit verbunden ist. Ein Video informiert über den sicheren Datenaustausch. Mögliche Anwendungsfelder sind erläutert und teilweise sehr detailliert dargestellt.

Cloud-Projekte besser verstehen

Fragen des Datenschutzes sind angeschnitten, stehen aber nicht im Mittelpunkt. Für DSB dürfte das Portal v.a. nützlich sein, um den Ablauf entsprechender Projekte zu verstehen. Auf dieser Basis ist es dann möglich, die relevanten Datenschutzfragen zu formulieren. Das Portal ist zu finden unter www.cloud.fraunhofer.de/.

BSI zu Clouds

Risiken und Sicherheitstipps

Einen gut verständlichen Einstieg zum Thema „Cloud: Risiken und Sicherheitstipps" bietet das Bundesamt für Sicherheit in der Informationstechnik (BSI) auf seiner Website. Jeder Themenkreis beginnt mit einem kurzen Überblick, Links verweisen zu vertiefenden Darstellungen:

- Grundsätzliches zur Cloud-Nutzung
- Daten löschen und Nutzung beenden
- Datenverschlüsselung in der Cloud
- Konfiguration von Cloud-Diensten
- Schutz vor Fremdzugriffen, Sicherheitskennung, Auswahl des Anbieters
- Standort des Cloud-Anbieters

Auswahl des Anbieters

Das Thema „Auswahl des Cloud-Anbieters" widmet sich u.a. der Frage, welche Aussagekraft Zertifikate und Testate haben. Dort heißt es etwa: „Oft findet man ein Zertifikat nach der internationalen Norm ISO/IEC 27001. Dabei wird nachgewiesen, dass der Cloud-Anbieter strukturierte Prozesse hat, um die Informationssicherheit zu gewährleisten. Leider ist damit aber keine Aussage über die eingesetzten Sicherheitsmaßnahmen verbunden."

Vertragsgestaltung

Welche Bedeutung der Vertragsgestaltung zukommt, macht folgender Hinweis bei „Standort des Cloud-Anbieters" deutlich: „Jeder Anbieter kann – innerhalb des gesetzlichen Rahmens, der für ihn Gültigkeit hat – seine eigenen Nutzungsbedingungen und Datenschutzbestimmungen aufstellen. Diese können so formuliert sein, dass Sie dem Anbieter womöglich Zugriffs- und Nutzungsrechte für die gespeicherten Dateien einräumen, obwohl Sie das nicht möchten." Die Seite ist abrufbar unter https://ogy.de/bsi-cloud-tipps.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken. Er beschäftigt sich seit Jahren mit dem Datenschutz in Unternehmen und Behörden.

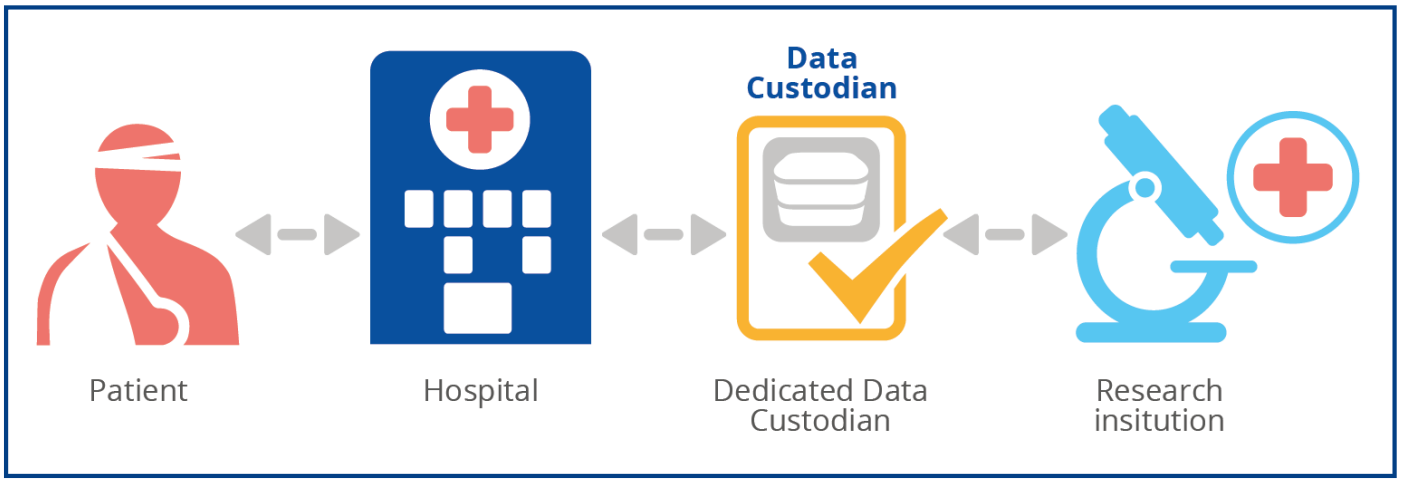


Bild: ENISA

Verfahren zur Pseudonymisierung

Wenn Datenverwalter die Pseudonyme liefern

Mit der Pseudonymisierung tun sich viele Unternehmen immer noch schwer. Eine Trusted Third Party als Datenverwalter könnte hier Abhilfe schaffen, setzt aber eine genaue Prüfung durch den Verantwortlichen voraus. Die EU-Agentur für Cybersicherheit ENISA gibt Hinweise dazu.

Bei mehr als jedem zweiten Unternehmen (56 %) sind neue, innovative Projekte aufgrund der Datenschutz-Grundverordnung (DSGVO) gescheitert – entweder wegen direkter Vorgaben oder wegen Unklarheiten in der Auslegung der DSGVO, so eine Umfrage des Digitalverbands Bitkom. Vier von zehn Betrieben (41 %) geben an, dass sie deswegen keine Datenpools aufbauen konnten, um etwa Daten mit Geschäftspartnern teilen zu können. Jedes fünfte betroffene Unternehmen (20 %) verzichtete auf den Einsatz neuer Datenanalysen, so weit die Umfrage (abrufbar unter https://ogy.de/umfrage-bitkom-innovationen).

DSGVO ist kein Hindernis

Doch verhindert die DSGVO wirklich Datenanalysen? Nein, aber viele Unternehmen haben Schwierigkeiten, Maßnahmen wie die Pseudonymisierung richtig umzusetzen. Und das, obwohl nicht erst die Datenschutz-Grundverordnung die Bedeutung und die Vorteile einer Pseudonymisierung betont.

Mögliche Unterstützung durch Trusted Third Parties

Unternehmen, die die Pseudonymisierung nicht selbst durchführen können oder wollen, haben die Möglichkeit, einen vertrauenswürdigen Dritten als Dienstleister einzusetzen. Ein Data Custodian oder Datenverwalter bildet die Brücke zwischen Unternehmen und den betroffenen Personen, damit Unternehmen sensible Daten verarbeiten können, die sich zwar der betreffenden Person zuordnen lassen, aber nicht ohne den Datenverwalter einzuschalten. Der Datenverwalter ersetzt die Identität der betroffenen Personen durch ein Pseudonym, sodass nur er eine individuelle Zuordnung der Daten vornehmen kann.

BEISPIEL

Auf dem Markt gibt es bereits Anbieter wie Custodix (https://www.custodix.com/index.php), Viacryp (https://www.viacryp.de/) und ZorgTTP (https://www.zorgttp.nl/), die als Trusted Third Party (TTP) personenbezogene Daten pseudonymisieren.

Was muss ein Datenverwalter können?

Die EU-Agentur für Cybersicherheit (ENISA) hat einen neuen Bericht zur Pseudonymisierung (https://ogy.de/pseudonymisierung-enisa) veröffentlicht. In dem – auf Englisch verfassten – Bericht beschreibt die ENISA ausführlich die Nutzung von sogenannten Data Custodians. Für Verantwortliche besonders wichtig sind die Kriterien, die ein zuverlässiger Datenverwalter erfüllen muss.

Der Datenverwalter muss zunächst die informative Gewaltenteilung aufrechterhalten. Das bedeutet,

- einen zuverlässigen Dienst bei der Anwendung der Pseudonymisierungsfunktion bereitzustellen,
- die erforderlichen Daten für die Zuordnung zwischen identifizierenden Daten und Pseudonymen auf sichere Weise aufzubewahren sowie – unter vordefinierten Bedingungen –
- die Wiederherstellung durchzuführen.

Ein Datenverwalter kann pseudonymisierte Daten von verschiedenen Daten verarbeitenden Stellen wie z.B. Krankenhäusern sammeln und übergreifende Datenbanken mit pseudonymen Daten bereitstellen, auf die die teilnehmenden

Unterstützung für Unternehmen

Leitfäden und Arbeitshilfen zur Pseudonymisierung

Viele Unternehmen wünschen sich mehr Anleitung, um das richtige Verfahren zur Pseudonymisierung auszuwählen und zuverlässig umzusetzen. Der langjährigen Bedeutung der Pseudonymisierung für den Datenschutz entsprechend finden sich dazu zahlreiche Arbeitshilfen und Leitfäden im Internet, u.a.:

- Arbeitshilfe zur Pseudonymisierung/Anonymisierung, Deutsche Gesellschaft für Medizinische Informatik, Biometrie und Epidemiologie e.V. (GMDS), Arbeitsgruppe „Datenschutz und IT-Sicherheit im Gesundheitswesen“: https://ogy.de/pseudonymisierung-gmds
- Anonymisierung und Pseudonymisierung von Daten für Projekte des maschinellen Lernens. Eine Handreichung für Unternehmen, Bitkom e.V.: https://ogy.de/pseudonymisierung-bitkom
- Entwurf für einen Code of Conduct zum Einsatz DS-GVO konformer Pseudonymisierung. Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2019: https://ogy.de/pseudonymisierung-code-of-conduct
- Anforderungen an den datenschutzkonformen Einsatz von Pseudonymisierungslösungen. Ein Arbeitspapier der Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft im Rahmen des Digital-Gipfels 2018: https://ogy.de/pseudonymisierung-bmwi

Organisationen wie die Krankenhäuser, aber auch z.B. medizinische Forschungseinrichtungen zugreifen können. Der zuverlässige Service des Datenverwalters muss die Verfügbarkeit und Integrität der gespeicherten Daten sowie die Überprüfung der Autorisierung umfassen, bevor er einen Zugriff zulässt.

Um die Datenzugriffe der teilnehmenden Organisationen besser kontrollieren zu können, bietet der Datenverwalter möglicherweise keinen direkten Zugriff, sondern verarbeitet die pseudonymisierten Daten gemäß der Spezifikation des auftraggebenden Unternehmens. Somit wäre der Datenbestand von anderen Parteien nicht direkt zugänglich, aber diese könnten ihre Verarbeitungsoperationen (z.B. Code) dem Datenverwalter zur Verfügung stellen, der die Ergebnisse zurücksendet.

Verlangt z.B. eine Forschungseinrichtung vom Datenverwalter Zugriff auf die von einem Krankenhaus bereitgestellten Daten einer betroffenen Person, überprüft der Datenverwalter die Rechtmäßigkeit der Anforderung anhand der Bedingungen und Einschränkungen, die die betroffene Person gemacht hat. Ähnlich wie ein Notar fungiert ein Datenverwalter daher auch als Vertreter der betroffenen Person und als Treuhänder bei Konflikten hinsichtlich des Zugriffs auf die Daten. Bei diesem Ansatz ist eine wesentliche Anforderung, dass die Betroffenen dem Datenverwalter vertrauen.

Sicherheit und Vertrauenswürdigkeit des Datenverwalters

Die Fokusgruppe Datenschutz der Plattform Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft macht deutlich: Für einen Datenverwalter besteht keine Notwendigkeit, die Inhaltsdaten zu kennen. Es empfiehlt sich daher, die Inhaltsdaten auf einem getrennten Übertragungsweg von den Daten verarbeitenden Stellen wie einem Krankenhaus direkt in die zur Speicherung vorgesehene Datenbank zu übermitteln.

Der getrennte Übertragungsweg kann dabei physikalischer Natur sein. Die Inhaltsdaten können aber auch über den Datenverwalter laufen und vorab mit einem Chiffrierverfahren verschlüsselt sein, bei dem ausschließlich die verantwortliche Stelle in der Lage ist, die Daten zu entschlüsseln.

Der Digitalverband Bitkom erklärt zum Einsatz eines solchen Datenverwalters, dass dieser Ansatz ein hohes Vertrauen in die Motive und Sicherheitskompetenzen des Datentreuhänderdienstes voraussetzt: Kommen die Daten dort z.B. durch das Fehlverhalten von Mitarbeitern oder durch Angriffe abhanden, kann dadurch immenser Schaden entstehen.

Das PAUTH-Verfahren

Doch Bitkom nennt auch mögliche Schutzmaßnahmen wie das sogenannte PAUTH-Verfahren (Pseudonyme Authentifizierung). Dieses Verfahren verwendet eine Kombination aus Kryptografie, Token-Management und Funktionstrennung, um zwei Ziele zu erreichen: Zwei Dienste können im Zusammenspiel eindeutige Pseudonyme zu realen, authentifizierten Nutzern erzeugen. Sie sind aber anschließend dennoch nicht in der Lage, die reale Identität zu einem Pseudonym aufzudecken, auch dann nicht, wenn sie sich absprechen oder Daten durch Angriffe oder Leaks abhandenkommen. Allein die Nutzer können die Verbindung bei Bedarf wiederherstellen. Damit behält der Betroffene als Data Owner die Hoheit über seine Daten, und das Risiko einer Re-Identifizierung ist minimiert.

Oliver Schonschek, Dipl.-Phys., ist Technology Analyst und wurde 2021 als „Top 25 Global Thought Leader and Influencer on Privacy“ ausgezeichnet.

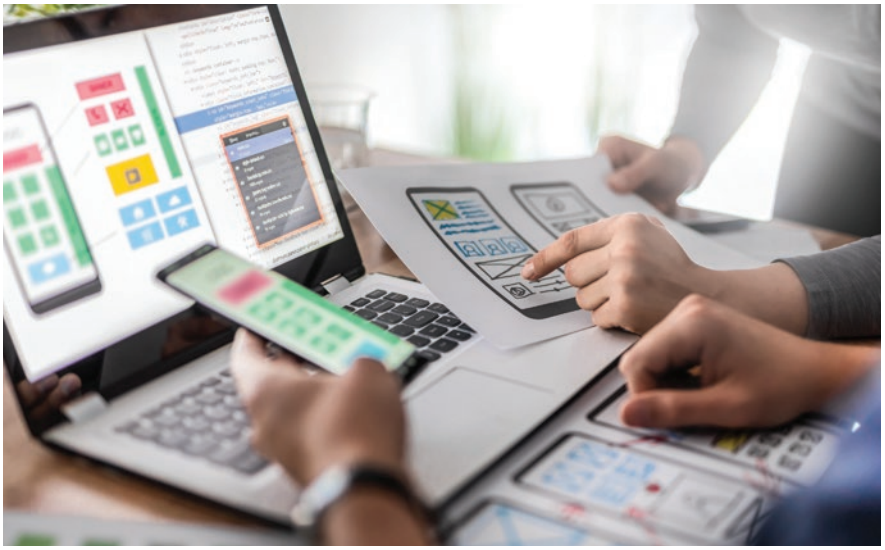


Bild: iStock.com/scyther5

Eine zentrale Rolle spielt, welche Daten die App für welche Zwecke verarbeitet

Datenschutzrecht

Apps: Welche Anforderungen müssen DSB prüfen?

Unternehmen und Behörden setzen immer häufiger auf Apps für Smartphones und Tablets, um dienstliche Abläufe zu optimieren. Welche datenschutzrechtlichen Aspekte müssen Verantwortliche und Datenschutzbeauftragte bei der Einführung einer solchen App beachten?

Typische Apps, die sich schon im Einsatz befinden, sind derzeit beispielsweise Collaboration Apps, Zeiterfassungs-Apps oder Apps für Spesenabrechnungen. Auch „Book-a-Desk"-Apps u.Ä. (siehe Seite 4) sind im Kommen.

1. Erlaubnisgrundlage und Datenminimierung

Zunächst bedarf es für den Einsatz der App einer Erlaubnisgrundlage. Die häufigsten Rechtsgrundlagen sind:

- Einwilligung
- § 26 Abs. 1 Bundesdatenschutzgesetz (BDSG) und die entsprechenden landesgesetzlichen Normen für Beamte und Beschäftigte im öffentlichen Dienst
- Art. 6 Abs. 1 Satz 1 Buchst. f Datenschutz-Grundverordnung (DSGVO)
- Betriebs- bzw. Dienstvereinbarungen

Welche Erlaubnisgrundlage greifen kann, müssen Datenschutzbeauftragte (DSB) im Einzelfall ermitteln. Zum einen müssen die Zwecke der App von einer Erlaubnisgrundlage gedeckt sein. Zum anderen folgt aus dem Grundsatz der Datenminimierung (Art. 5 Abs. 1 Buchst. c DSGVO), dass die App nur die Daten verarbeiten sollte, die für den Zweck erforderlich sind. Erkundigen Sie sich daher insbesondere nach folgenden Datenverarbeitungen:

- Welche Bestandsdaten fragt die App ab (z.B. Name, Adresse)?
- Welche Nutzungsdaten verarbeitet sie (z.B. GPS-Daten)?
- Welche Daten verarbeitet sie ggf. im Rahmen einer Registrierung als Pflicht- bzw. freiwillige Angaben?
- Welche geräte- oder betriebsbezogenen Daten verarbeitet die App (z.B. IMEI, IMSI, Werbeidentifikatoren)?
- Verarbeitet sie besondere Arten von personenbezogenen Daten (z.B. Gesundheitsdaten)?
- Loggt sie personenbezogene Daten? Wenn ja, welche?

Ermitteln Sie bei möglichst allen Daten, warum sie jeweils verarbeitet werden.

2. Berechtigungen

Berechtigungen sind auf zwei Ebenen relevant. Fragen Sie zum einen nach den Berechtigungen, die die App benötigt (z.B. Zugriff auf das Adressbuch). Prüfen Sie zum anderen, wie die Berechtigungen innerhalb der Organisation vergeben werden sollen. Folgende Punkte sind also zu klären:

- Welche Berechtigungen erhält die App auf dem Gerät?
- Fordert sie nur Berechtigungen ein, die für die Funktionalität der App gemäß dem geplanten Einsatzzweck zwingend nötig sind?
- Ist gewährleistet, dass die App keine personenbezogenen Daten von unbeteiligten Dritten verarbeitet?
- Fragt sie die Erlaubnis des Nutzers ab, wo notwendig (z.B. bei GPS-Daten)?

Die App muss in der Lage sein, das für ihre Nutzung vorgesehene Berechtigungskonzept umzusetzen. Das bedeutet, dass nur diejenigen Personen Lese- und Zugriffsrechte auf verarbeitete Daten erhalten, die diese Rechte zu ihrer Aufgabenerfüllung benötigen (Need-to-know-Prinzip). Sollen Nutzer jeweils nach ihrer Rolle unterschiedliche Berechtigungen bekommen, so muss die App unterschiedliche Rollen und dementsprechend abgestufte Rechte umsetzen können.

3. Datenübermittlung

Kein DSB möchte eine App absegnen, die sich als Datenschleuder entpuppt. Eine App sammelt nicht nur Daten, sondern kann sie auch Dritten wie Vertriebspartnern offenlegen. Um Herr der Daten zu bleiben, prüfen Sie Folgendes:

- An wen und zu welchem Zweck übermittelt die App personenbezogene Daten vom Gerät?
- Welche personenbezogenen Daten übermittelt sie jeweils an den Dritten?
- Auf welche Rechtsgrundlage wird die Übermittlung gestützt?
- Erfolgt die Übermittlung innerhalb oder außerhalb des Europäischen Wirtschaftsraums (EWR)?
- Wenn außerhalb: Sind hinreichende Datenschutzgarantien im Sinne von Art. 44 ff. DSGVO für einen Transfer in ein Drittland vorhanden?

Der Verantwortliche sollte den Einsatz der App erst freigeben, wenn Sie als DSB die Offenlegung der Daten aufgeklärt haben.

4. Integrität und Vertraulichkeit

Geeignete technische und organisatorische Maßnahmen (TOM) müssen die Daten, die die App erhebt, schützen (Art. 5 Abs. 1 Buchst. f DSGVO). Prüfen Sie die ergriffenen TOM auf ihre Angemessenheit für die beabsichtigten Datenverarbeitungen.

Eine gute Orientierung speziell für Apps bieten der OWASP Mobile Application Verification Standard (MASVS; abrufbar unter https://github.com/OWASP/owasp-masvs) und der OWASP Mobile Security Testing Guide (abrufbar unter https://github.com/OWASP/owasp-mstg). Daneben sind insbesondere folgende Aspekte relevant:

- Nutzt die App nur verschlüsselte Verbindungen, z.B. TLS 1.2 oder neuer?
- Werden die Daten mit kryptografischen Verfahren verschlüsselt?
- Sind ausdifferenzierte Backup-Mechanismen vorgesehen?
- Liegen Zertifizierungen vor, die einen Anhaltspunkt für ausreichende Sicherheitsmaßnahmen bieten wie ISO 27001?
- Ist die Stabilität des Systems gewährleistet (z.B. durch Penetrationstests)?

5. Tracking

Es gibt Technologien, die es App-Anbietern ermöglichen, Nutzerverhalten minutiös nachzuverfolgen. Ein berechtigtes Interesse daran, die App-Nutzer auf Schritt und Tritt zu verfolgen, gibt es selten. Außerdem können Unternehmen und Behörden darüber unwissentlich Dienst- bzw. Geschäftsgeheimnisse offenbaren. Klären Sie daher folgende Punkte:

- Setzt die App Tracking-Technologien ein und wer nutzt sie?
- Welche Daten erhebt das Tracking?
- Informieren die Datenschutzbestimmungen ausreichend über das Tracking?
- Auf welche Rechtsgrundlage wird die Datenverarbeitung gestützt?
- Müssen die Nutzer einwilligen?
- Können die Nutzer ihre Einwilligung jederzeit einfach widerrufen?
- Erfolgt eine Anonymisierung der personenbezogenen Tracking-Daten?

6. Speicher- und Löschfristen

Die über die App verarbeiteten personenbezogenen Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Im Anschluss sind die Daten zu löschen, sofern keine gesetzlichen Aufbewahrungsfristen – etwa aus dem Steuer- oder Handelsrecht – entgegenstehen. Überprüfen Sie folgende Aspekte:

- Welche Daten werden a) auf dem Gerät lokal, b) auf Servern oder c) auf zusätzlichen Speichermedien wie SD-Karten gespeichert?
- Werden die Daten in einer Cloud gespeichert, die an das Gerät oder die App angebundenen ist?
- Lassen sich die Daten nach eigenen Regeln löschen – auch von zusätzlichen Speichermedien?

7. Rechtsbeziehung zum App-Anbieter

Prüfen Sie immer auch, in welcher datenschutzrechtlichen Beziehung Ihre Organisation zum App-Anbieter steht. Folgende Konstellationen sind denkbar:

- Der App-Anbieter ist ein Auftragsverarbeiter im Sinne von Art. 28 DSGVO.
- Der App-Anbieter und das Unternehmen/die Behörde sind gemeinsame Verantwortliche im Sinne von Art. 26 DSGVO.
- Der App-Anbieter und das Unternehmen/die Behörde sind jeweils getrennt Verantwortliche.

PRAXIS-TIPP

Die App sollte in der Lage sein, die Löschregeln, die Sie als DSB empfehlen, automatisch umzusetzen. Ferner ist die Kenntnis der jeweiligen Speicherorte von essenzieller Bedeutung, damit sich die personenbezogenen Daten rückstandslos löschen lassen. Eine manuelle Löschung ist fehleranfällig und (je nach Datenmenge) sehr zeitintensiv, sodass davon abzuraten ist.

Die Art der datenschutzrechtlichen Beziehung hat unmittelbare Auswirkungen darauf, welche datenschutzrechtliche Vereinbarung der Verantwortliche mit dem App-Anbieter treffen muss. Außerdem kann es auch Auswirkungen darauf haben, ob sich der Einsatz der App mit einer gesetzlichen Erlaubnisgrundlage legitimieren lässt. Letzteres dürfte bei einer Auftragsverarbeitung leichter gelingen.

8. Vergessen Sie die Basics nicht

Und zu guter Letzt: Es gibt datenschutzrechtliche Basics, die sich nicht speziell auf Apps beziehen, aber natürlich gleichwohl zu beachten sind:

- Werden die App-Nutzer gemäß Art. 12 ff. DSGVO informiert?
- Bedarf es einer Datenschutz-Folgenabschätzung?
- Inwieweit muss das Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) ergänzt werden?
- Sind durch ein App-Update neue Features hinzugekommen, die eine Neubewertung der App erfordern?


Dr. André Schmidt (schmidt@lutzabel.com) und Angelika Maria Szalek (szalek@lutzabel.com) sind Rechtsanwälte der Wirtschaftskanzlei LUTZ | ABEL. Sie unterstützen Unternehmen in allen IT- und datenschutzrechtlichen Fragestellungen.

Bild: iStock.com/ST.art

Auch MS Teams bietet einige Möglichkeiten, mit datenschutzfreundlichen Voreinstellungen zu arbeiten

Microsoft Teams

Prüfpflichten des DSB bei Microsoft 365 (Teil 5)

Microsoft Teams ist eine Anwendung, die viele Organisationen derzeit intensiv einsetzen. In einem mehrstufigen Prüfplan erfahren Sie, was Sie sich als Datenschutzbeauftragte für Ihre Prüfungen anschauen sollten.

In den letzten Beiträgen zu Microsoft 365 (MS 365) lernten Sie das zentrale Admin Center mit diversen Funktionalitäten für datenschutzrelevante Einstellungen kennen. Zum Abschluss der Reihe sehen wir uns nun Microsoft Teams genauer an.

Administration nach Erforderlichkeit regeln

MS 365 bietet Ihnen die Möglichkeit, zur Administration von MS Teams unterschiedliche Rollen zu nutzen. Je nachdem, wie groß Ihre IT-Abteilung ist und wie die Aufgaben funktional aufgeteilt sind, können Sie Berechtigungen nach Erforderlichkeit vergeben (lassen).

Als Rollen stehen zur Verfügung:

- Teams-Administrator (verwaltet Gruppen und hat Vollzugriff auf das Teams Admin Center)
- Teams-Geräteadministrator (administriert Geräte wie Teams-Räume, Teams-Displays und Smartphones)
- Teams-Kommunikationsadministrator (weist Telefonnummern zu, verwaltet Besprechungsrichtlinien, analysiert Anrufe)
- Teams-Kommunikationssupportspezialist und Teams-Kommunikationssupporttechniker (analysieren Benutzeranruf- und Anrufaufzeichnungsdetails und lösen Kommunikationsprobleme)

Ein erster Prüfpunkt ist somit, ob Ihre IT die Möglichkeiten des Rollenkonzepts so nutzt, dass die jeweiligen Kolleginnen und Kollegen nur Zugriff auf die Funktionen haben, die sie benötigen, um ihre Aufgaben zu erfüllen.

Im Teams Admin Center datenschutzfreundliche Voreinstellungen treffen

Nun widmen wir uns dem Teams Admin Center für datenschutzfreundliche Voreinstellungen. Nutzen Sie hier die vielfältigen Einstellungsmöglichkeiten. Als Erstes betrachten wir den Bereich Teams.

1. Teams datenschutzfreundlich verwalten

Unter „Teams verwalten“ erhalten Sie einen Überblick über sämtliche Teams, die in MS Teams angelegt sind. Sie sehen, wie viele Mitglieder ein Team hat, ob Gäste (= Organisationsfremde) in diesem Team mitarbeiten und welcher Datenschutzlevel gewählt ist.

Zur Erklärung: Der Datenschutzlevel unterscheidet zwischen öffentlich und privat. Öffentlich bedeutet, dass jeder in der Organisation sich diesem Team anschließen kann. Privat hingegen bedeutet, dass es einen Besitzer gibt, der aktiv andere Benutzer einlädt, d.h. darüber entscheidet, ob sich jemand einem bestimmten Team anschließen darf. Daraus lassen sich gleich mehrere Prüfpflichten ableiten:

- Wer ist dafür verantwortlich, Teams anzulegen und zu administrieren?
- Wer archiviert alte Teams oder löscht sie?
- Wer löscht ausgeschiedene oder nicht mehr benötigte Benutzer aus Teams?
- Welche organisatorischen Vorgaben gibt es für die Wahl des Datenschutzlevels? Ein Personal-Team sollte privat sein, während eine organisationsweite Sportgruppe öffentlich sein darf.
- Prüfen Sie außerdem, welche weiteren Einstellungen für die Teams in Ihrer Organisation sinnvoll sind.

Profitipp: Sie können alte Teams über eine Einstellung im Azure Active Directory admin center („Gruppen“ ⇨ „Ablaufdatum“) nach einer definierten Zeit automatisch löschen!

2. Mit Benutzern korrekt umgehen

Der nächste Prüfbereich ist der der „Benutzer". Dort sehen Sie sämtliche angelegten Benutzer, auch Gäste. Aus Sicht des Datenschutzes sind die hinter einem Benutzer liegenden Daten zu schützen. Mit administrativen Rechten sehen Sie unter „Besprechungen und Anrufe", welche Besprechungen oder Anrufe eine Benutzerin durchgeführt hat, wann diese gestartet sind, wie lange sie gedauert haben, welche Personen daran teilgenommen haben und je nachdem noch tiefergehende Informationen wie IP-Adresse, verwendetes Gerät, Name des Geräts, CPU oder Betriebssystem.

Bei Kommunikationsproblemen mögen diese Daten hilfreich sein, um Fehler zu analysieren. Abseits davon sind diese Daten nicht für Leistungs- oder Verhaltenskontrollen zu nutzen! Als Prüfpflicht ergibt sich daher:

- Gibt es organisatorische Vorgaben, die den Umgang mit Benutzern regeln? Wer legt Benutzer an und administriert sie?
- Wer löscht ausgeschiedene oder nicht mehr benötigte Benutzer?
- Was ist im Umgang mit den Daten der Besprechungen und Anrufe erlaubt?

PRAXIS-TIPP

Profitipp: Nutzen Sie die gewonnenen Informationen der Besprechungs- und Anrufdaten auch für die Informationspflichten nach Art. 13 DSGVO!

3. Richtlinien für Besprechungen, Nachrichten und Apps definieren

Im dritten Schritt nutzen Sie Richtlinien, um datenschutzfreundliche Voreinstellungen für Besprechungen, Nachrichten und Apps zu treffen. Die relevanten Bereiche für Sie sind „Besprechungen", „Nachrichtenrichtlinien" und „Teams-Apps".

Bei den Besprechungen treffen Sie zentrale Vorgaben, z.B. dafür, ob Sie Transkription, d.h. die Umwandlung des gesprochenen Worts in angezeigte Schrift, zulassen möchten. Sie können Aufzeichnungen von Besprechungen zulassen oder verbieten. Und Sie können Vorgaben treffen, ob Benutzer den Wartebereich umgehen können oder nicht. Darüber hinaus sei noch erwähnt, dass Sie in den Besprechungseinstellungen auch deaktivieren können, dass anonyme Benutzer an Besprechungen teilnehmen können.

ACHTUNG!

Profitipp: Überlegen Sie sich gut, ob Sie deaktivieren möchten, dass anonyme Benutzer nicht mehr an Besprechungen teilnehmen können. Das kann dazu führen, dass organisationsfremde Personen, die weder ein MS-365- noch ein sonstiges Microsoft-Konto haben, nicht mehr an Ihren Besprechungen teilnehmen können!

Nun kommen wir zu den „Nachrichtenrichtlinien". Wie der Name schon sagt, geht es darum, zu regeln, wie Ihre Organisation mit Nachrichten umgeht. Dürfen Benutzer z.B. Nachrichten nachträglich bearbeiten und löschen? Dürfen sie im Chat Giphys und Memes verwenden? Das mag sich unscheinbar anhören. Da Sie bei Giphys und Memes jedoch Daten von Drittanbietern laden, stellt sich auch hier die Frage, welche Daten Sie dabei übermitteln und ob dabei ein angemessenes Datenschutzniveau gewährleistet ist.

Schließlich betrachten wir noch den Bereich der „Teams-Apps". Dort treffen Sie organisationsweite App-Einstellungen. Standardmäßig sind Apps von Drittanbietern oder von Microsoft selbst erlaubt. Als DSB müssen Sie jedoch wissen, dass diese Apps nicht den Nutzungsbedingungen oder den Datenschutzbestimmungen unterliegen, die Ihre Organisation mit Microsoft geschlossen hat. Im Umkehrschluss heißt das, dass Sie standardmäßig alle Drittanbieter-Apps untersagen und erst nach einer sorgfältigen Prüfung freigeben sollten.

Übrigens ist den drei betrachteten Bereichen – Besprechungen, Nachrichten und Apps – gemein, dass Sie Richtlinien mit den gewünschten Einstellungen definieren und Benutzern zuweisen können.

Welche Prüfpflichten ergeben sich daraus für den Datenschutz?

- Sind Richtlinien für datenschutzfreundliche Voreinstellungen für Besprechungen, Nachrichten und Teams-Apps getroffen?
- Sind Drittinhalte wie Giphys, Memes und Apps standardmäßig deaktiviert und erst nach Prüfung freigegeben?

Berücksichtigen Sie abschließend „Organisationsweite Einstellungen". Mit diesen Einstellungen entscheidet die Organisation beispielsweise,

- wie sie mit Externen und Gästen umgeht oder
- ob Benutzerinnen oder Benutzer bestimmte externe Clouddienste in Teams einbinden dürfen und
- inwieweit Adressbuchrichtlinien verhindern, dass organisationsfremde Nutzer über Teams hinweg namentlich nach anderen Nutzern suchen dürfen.

Fazit: MS Teams bietet eine Bandbreite an datenschutzfreundlichen Voreinstellungen. Sie als DSB sollten diese kennen und für Ihre Prüfungen nutzen. Viel Erfolg!

Julian Häcker, Geschäftsführer der ENSECUR GmbH, löst als Datenschutzberater seit 2010 die Praxisherausforderungen im Datenschutzalltag von Organisationen.

WEBINAR-TIPP

Nicht nur für Verantwortliche wichtig, die Microsoft-Produkte einsetzen: die neuen Standardvertragsklauseln, die die EU am 4. Juni veröffentlicht hat. Wie ist dieses Instrument für den Datenaustausch mit Drittländern aufgebaut? Welche rechtlichen Gesichtspunkte sind zu beachten? In welchem technisch-organisatorischen Kontext sind sie einsetzbar? In einem Schwerpunkt-Webinar klären Dr. Eugen Ehmann und Eberhard Häcker die wirklich relevanten Fragen zur Datenübermittlung in Drittländer. Gleich anmelden unter https://weka.de/ds/scc!

Bild: iStock.com/monsitj

Der BGH sieht gespeicherte E-Mails als Telekommunikation an, nicht nur als gespeicherte Daten

Eine gewagte Konstruktion

BGH-Urteil: Kein Schutz für ruhende E-Mails

Der BGH ist immer für Überraschungen gut. Manchmal mit einer Entscheidung, die den Strafverfolgungsbehörden nicht gefällt. Dann erlaubt das Gericht ihnen wieder mehr, als manchem lieb sein kann. Zu Letzterem gehört ein auch aus Datenschutzsicht interessantes Urteil.

Der Bundesgerichtshof (BGH) erlaubt in einer Entscheidung vom 14.10.2020 im Rahmen einer Überwachung der Telekommunikation (TKÜ) kurz gesagt den Zugriff auf E-Mails, die beim Provider zwischen- oder endgespeichert sind (Az. 5 StR 229/19, abrufbar unter https://ogy.de/bgh-ruhende-mails). Diese Mails nennt man „ruhende" E-Mails, weil der Zugriff nicht erfolgt, während diese Nachrichten gerade gesendet werden.

Keine zeitliche Eingrenzung

Diesen Zugriff erlaubt der BGH nun grundsätzlich ohne jegliche zeitliche Eingrenzung. Er hält § 100a Strafprozessordnung (StPO) für die Norm, die solche Eingriffe in die Freiheit der Telekommunikation rechtfertigt. Die rein praktischen Konsequenzen finden geneigte Leserinnen und Leser im Fazit. Wer sich für die juristischen Fragestellungen bzw. Inkonsequenzen der Entscheidung interessiert, möge gleich hier weiterlesen.

Grundrechtsschutz für Telekommunikation

Angesichts der BGH-Entscheidung stellt sich die Frage, ob das noch eine TKÜ ist, wie sie § 100a StPO ermöglicht. Sie wirft auch Fragen des Grundrechtsschutzes auf. Eingriffe in die Grundrechte betroffener Personen sind nur durch oder aufgrund eines Gesetzes zulässig. Und es sollte auch klar sein, in welches Grundrecht aufgrund eines bestimmten Gesetzes eingegriffen werden darf. Bei der TKÜ ist das eindeutig das Fernmeldegeheimnis aus Art. 10 Grundgesetz (GG).

Klar ist, dass unter die TKÜ das Abhören und Mitschneiden von Telefonaten gehört und bei E-Mails das Mitlesen bzw. Abfangen während der Versendung. Im Kern sind also „flüchtige" Daten betroffen. Das gesprochene Wort ist nicht mehr vorhanden, nachdem es gesagt wurde. Ein Mitschneiden ist daher zwingend notwendig, will man es konservieren. Eins zu eins lassen sich E-Mails allerdings nicht mit einem Gespräch vergleichen, eher mit einem Brief. Deshalb liegt es nahe, für den Zugriff auf E-Mails andere Normen heranzuziehen. Zu denken ist hier an die Postbeschlagnahme nach § 99 StPO oder an einen Beschlagnahmebeschluss nach § 94 StPO, wie er auch sonst bei Daten zum Zuge kommt.

Besonderheiten des E-Mail-Verkehrs

Der maßgebliche Unterschied zur herkömmlichen Telefonüberwachung liegt darin, dass das Versenden einer E-Mail verschiedene Phasen durchlebt, vom Erstellen über das Versenden an den Provider bis zum Abruf durch den Empfänger. Zwischen Versenden und Abruf ist die E-Mail beim Provider zwischengespeichert und nach dem Abruf in der Regel endgespeichert. Um den Zugriff während dieser beiden Speicherungen, während sich die E-Mail gerade nicht „bewegt", geht es hier.

Telekommunikation oder nicht?

Die entscheidende Frage, von der abhängt, welche Eingriffsnorm zum Zuge kommt, ist, ob auch die gespeicherten E-Mails Telekommunikation darstellen, die dem Schutz von Art. 10 GG unterfallen, oder ob sie nur gespeicherte Daten sind, die der Beschlagnahme unterliegen. Diese Frage hat der BGH nun erstmals dahin beantwortet, dass es sich bei diesen E-Mails um Telekommunikation handelt.

WICHTIG

Die Begründung, die der BGH gibt, lässt sich zunächst durchaus hören: Die E-Mail ist schutzbedürftig, egal, ob sie gerade gesendet oder abgerufen wird oder ruht. Ihr Inhalt ändert sich durch die Speiche-

rung nicht. In erster Linie gehe es, so der BGH, um den Inhalt der Kommunikation und nicht darum, in welchem Stadium der Kommunikation sich die E-Mail zum Zeitpunkt des Zugriffs gerade befindet. Das ist unter dem Blickwinkel des Grundrechtsschutzes nachvollziehbar. Schließlich ist § 100a StPO eine Rechtsgrundlage, die zwar inzwischen bei (zu) vielen, aber bei Weitem nicht bei allen Straftaten nutzbar ist, anders als die Beschlagnahme.

Dann aber verlässt der BGH seine klare Argumentationslinie. Er hält nämlich neben dem Zugriff über eine Telekommunikationsüberwachung eine (normale) Beschlagnahme beim Provider nach wie vor für möglich. Beide prozessualen Maßnahmen würden sich ergänzen, nicht ausschließen. Auch dieser Satz ist für sich genommen richtig. Natürlich kann z.B. bei der Bekämpfung von Drogenkriminalität neben eine TKÜ auch eine Durchsuchung mit anschließender Beschlagnahme treten. Beides kann dazu beitragen, unterschiedliche Beweismittel zu gewinnen.

Nur trifft das den Kern nicht. Es geht hier um die Austauschbarkeit von Rechtsgrundlagen. Und insoweit sollte man sich einig sein, dass der Zugriff auf ein und dasselbe Beweismittel eben gerade nicht beliebig erfolgen darf, weil sich sonst die Voraussetzungen der strengeren Norm umgehen lassen könnten.

Geht man wie der BGH ausdrücklich davon aus, dass es sich auch bei ruhenden E-Mails um Telekommunikation handelt, dann ist konsequenterweise ein Zugriff nur dann zulässig, wenn eine richterliche Anordnung nach § 100a StPO vorliegt.

Rückwirkung der Überwachungsmaßnahme

Die nächste Ungereimtheit der Entscheidung besteht in zeitlicher Hinsicht. Der BGH erlaubt nämlich nicht nur den Zugriff auf E-Mails, die seit dem Zeitpunkt der Anordnung der Maßnahme versandt oder empfangen wurden. Vielmehr soll sich der Zugriff auch auf solche E-Mails erstrecken, die der Provider zu einem beliebigen Zeitpunkt vorher gespeichert hat.

Die Begründung, dass diese ja auch nach § 94 StPO beschlagnahmt werden dürften, ist – wie oben dargelegt – inkonsequent. Denn das wäre ja ein Eingriff in die Telekommunikationsfreiheit, den nur § 100a StPO erlaubt, nicht aber § 94 StPO.

Im zugrunde liegenden Fall war § 100a StPO die Rechtsgrundlage, sodass an sich auch ein Eingriff in die Vergangenheit möglich wäre. Denn anders als bei der sogenannten Quellen-TKÜ besteht hier kein Verbot für rückwirkende Zugriffe. Das setzt aber eines voraus, auf das der BGH nicht eingeht: Ein Richter muss die Rückwirkung ausdrücklich anordnen. Enthält ein Beschluss keinen entsprechenden Passus, so dürfen die Ermittler nur solche ruhenden E-Mails beschlagnahmen, die nach der richterlichen Anordnung gespeichert wurden. Andernfalls droht der Zugriff auf viel zu viele, auch private E-Mails.

Fazit: erhebliche Ausweitung zu befürchten

Die Entscheidung ist nicht in allen Konsequenzen durchdacht. Es bleibt daher zu hoffen, dass das Bundesverfassungsgericht Gelegenheit erhält, sich mit diesen Fragen auseinanderzusetzen. Sonst bestünde die Gefahr einer erheblichen Ausweitung des Zugriffs auf E-Mails, die oft jahrelang beim Provider gespeichert bleiben.

PRAXIS-TIPP

Für die Hausanwälte eines betroffenen Unternehmens und des betroffenen Providers ist empfehlenswert, die richterliche Anordnung genau unter die Lupe zu nehmen. Gerade hinsichtlich der Rückwirkung ist das wichtig. Und generell ist diese Entscheidung ein guter Anlass, den E-Mail-Bestand beim Provider daraufhin zu überprüfen, ob sich nicht das eine oder andere löschen lässt.

Dr. Claus Pätzel ist ein ausgewiesener Experte des Datenschutzes im Justizbereich. Zuletzt war er Vorsitzender Richter am Oberlandesgericht München.

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 232,00 €
(zzgl. MwSt. und Versandkosten)
Einzelheft 22 €
(zzgl. MwSt. und Versandkosten)

Druck:
Geiselmann Printkommunikation GmbH
Leonhardstraße 23, 88471 Laupheim

Layout & Satz:
METAMEDIEN
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4090

ISSN-Nr.:
1614-6867

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

Berechtigungskonzept

Wie man charmant überzeugt, nicht benötigte Berechtigungen abzugeben

Ein Klassiker in Unternehmen und Behörden: Beschäftigte Personen häufen gern Zugriffsberechtigungen an, selbst wenn sie sie mittlerweile gar nicht mehr benötigen. Und niemand hat ein Auge darauf – außer den unbequemen Datenschutzbeauftragten ...

Zu den Aufgaben von Datenschutzbeauftragten gehört es, Zugriffe auf Datenbanken zu überprüfen. Wer feststellt, dass einzelne beschäftigte Personen mehr Berechtigungen haben, als sie für die Aufgabenerfüllung benötigen, sollte zuerst einmal prüfen, warum das so ist. Denkbar ist ja, dass diese Personen Stellvertretung für andere sind und dann im Fall der Fälle die Zugriffe objektiv benötigen.

Statussymbol Berechtigungen

Häufig ist es aber schlicht so, dass im Laufe der Zeit eine Berechtigung nach der anderen hinzukommt, aber sich niemand traut, der immer weiter aufsteigenden Person eine nicht mehr benötigte Berechtigung zu nehmen. Es scheint fast so, als ob alle Beteiligten die Berechtigungen als eine Art Statussymbol ansehen. Daher wäre es am einfachsten, wenn die betreffenden Personen von sich aus darum bitten, die Berechtigungen auf das erforderliche Maß zu reduzieren. Doch wie bekommen Sie das hin?

Lockmittel Datenpanne

Charmant funktioniert das erfahrungsgemäß wie folgt: Entdecken Sie, dass jemand deutlich mehr Berechtigungen hat als erforderlich, sprechen Sie diese Person an. „Ihre Arbeit ist ja sehr wichtig, so viele Berechtigungen, wie Sie haben!“ Meistens sind die Rechteinhaber dann sehr stolz. „Aber dann sind Sie ja auch mit der Verantwortung vertraut, die damit verbunden ist. Kommt es im Zusammenhang mit den Daten zu einer Datenpanne und wird ermittelt, wer da die Verantwortung trägt, müssen natürlich alle Berechtigungen durchforstet werden. Und dann ist erst mal jeder verdächtig, der Zugriff hat. Aber das kennen Sie ja und haben immer ein gutes Alibi.“ Oft ist die Reaktion darauf: „Ach wissen Sie, Sie haben eigentlich Recht. Wenn ich mir das so überlege, habe ich den Zugriff ja wirklich schon lange nicht mehr genutzt. Den können Sie wirklich sperren.“ Bingo! Charmant haben wir die nicht mehr benötigte Berechtigung zurückerhalten!

Eberhard Häcker ist seit vielen Jahren selbstständig mit Schwerpunkt Datenschutzberatung. Als externer DSB hat er schon viel erlebt.

IN DER NÄCHSTEN AUSGABE

Besserer Schutz für DNS

Das DNS ist das „Telefonbuch“ für das Internet. Ein neuer Standard will den Datenschutz bei der DNS-Nutzung erhöhen.

Das TTDSG

Am 01.12.2021 tritt das Telekommunikation-Telemedien-Datenschutz-Gesetz in Kraft – das müssen Sie dazu wissen.

Die neuen Standardvertragsklauseln

Was bringen die völlig neu gestalteten Musterformulare?