www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT | Mai 2020

Bild: iStock.com/Panuwat Sikham

**Derzeit weltweit im Fokus und in der Diskussion: Gesundheitsdaten**

Rechtsgrundlagen

# Gesundheitsdaten von Beschäftigten

**Die aktuelle Entwicklung rund um das Covid-19-Virus hält auch den Datenschutz auf Trab. Welche personenbezogenen Daten darf der Arbeitgeber in solchen Extremsituationen eigentlich verarbeiten?**

Gesunde und damit leistungsfähige Mitarbeiter zu haben, ist gerade in Krisenzeiten eine wichtige Säule. Gleich ob ein Beschäftigter nur für kurze Zeit erkrankt ist oder ob es sich um einen „Dauerkranken" handelt – der Arbeitgeber muss den erkrankten Mitarbeiter ersetzen und den betrieblichen Ablauf sicherstellen.

Sollten sich Mitarbeiter tatsächlich mit dem Corona-Virus infiziert haben, stellt dies den Arbeitgeber vor bisher nicht gekannte Herausforderungen: Wurden weitere Mitarbeiter infiziert? Welche Maßnahmen muss bzw. darf ich nun – auch aus Datenschutzsicht – ergreifen?

## Was genau sind „Gesundheitsdaten"?

Jeder Datenschützer könnte die Definition der „besonderen Kategorien personenbezogener Daten" vermutlich im Schlaf zitieren. Dass darunter auch die Gesundheitsdaten fallen, ist nichts Neues. Doch wo beginnt eigentlich genau der Begriff der „Gesundheit"? Ist z.B. die Information, dass eine Person sich gegenwärtig in Quarantäne aufhält, bereits ein Gesundheitsdatum mit allen entsprechenden datenschutzrechtlichen Folgen?

Art. 4 Nr. 15 Datenschutz-Grundverordnung (DSGVO) schreibt: 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 verdeutlicht, dass solche Daten zu den Gesundheitsdaten zählen, „die sich auf den Gesundheitszustand einer betroffenen Person beziehen und aus denen Informationen über →

## Editorial

Ricarda Veidt, Chefredakteurin

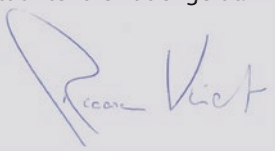
# Kommt der Datenschutz unter die Räder?

Liebe Leserin, lieber Leser! Jetzt hatten sich die anfängliche Aufregung und die Häme über die Datenschutz-Grundverordnung gerade etwas gelegt. Datenschutz an sich war auf einem guten Weg, endlich auch in der breiten Öffentlichkeit zu einem positiver besetzten Begriff zu werden.

Wie in jedem anderen Lebensbereich auch hat die Corona-Krise nun jedoch alles auf den Kopf gestellt. Nun ist der Datenschutz wieder der Bremser, der lästige Bedenkenträger, der für den Gesundheitsschutz grundsätzlich hintanzustehen hat. Übermittlung von Gesundheitsdaten an die Polizei, Corona-Apps in unterschiedlichen Variationen – alles im Namen des Gesundheitsschutzes ohne genaueres Hinschauen gerechtfertigt? Wer darauf weist, es mögen doch bitte solche Dinge wie Zweckbindung und Angemessenheit in die Überlegungen einbezogen werden, wird gern einmal pauschal abgeschmettert mit „Gesundheit geht vor."

Ich hoffe für uns alle – und nicht nur für die, die im Datenschutz tätig sind –, dass der Datenschutz nicht komplett unter die Räder gerät.

Bleiben Sie gesund!
Ihre Ricarda Veidt



den früheren, gegenwärtigen und künftigen körperlichen oder geistigen Gesundheitszustand der betroffenen Person hervorgehen."


Der Gesundheitsbegriff ist daher weit auszulegen. Ausreichend sind Tatsachen, die in irgendeiner Art und Weise einen Rückschluss auf den Gesundheitszustand des Betroffenen ermöglichen.

### Quarantäne und Aufenthalt im Risikogebiet

Ist aber nun die Information, dass sich jemand in Quarantäne befindet, bereits eine Aussage über seinen Gesundheitszustand? Oder weiter gedacht: Wenn sich ein Mitarbeiter (sei es privat oder beruflich) in einem vom Robert-Koch-Institut als „Risikogebiet" eingestuften Land aufgehalten hat: Stellt diese Angabe schon ein Gesundheitsdatum dar?

Trotz der weiten Auslegung des Begriffs der Gesundheitsdaten wird man wohl beide Fragen verneinen müssen. Denn: Quarantäne bedeutet nicht, dass sich eine Person mit dem Virus angesteckt hat. Vielmehr könnte es auch sein, dass sie lediglich Kontakt zu einer mit COVID-19 infizierten Person hatte und sich nun – solange nicht feststeht, ob sie sich selbst angesteckt hat – in Quarantäne aufhalten muss. Und lediglich die Tatsache, dass man möglicherweise Kontakt zu einer infizierten Person hatte, ist keine Aussage über den Gesundheitszustand.

Beim Aufenthaltsort gilt dasselbe: Zwar müssen sich Personen, die sich in einem „Risikogebiet" aufgehalten haben, eventuell weitergehenden Untersuchungen unterziehen. Ein Rückschluss darauf, dass diese Personen auch erkrankt sind, ist aber nicht möglich.

## Was macht der Arbeitgeber mit den Gesundheitsdaten?

Ein Arbeitgeber könnte derzeit durch unterschiedliche Maßnahmen Gesundheitsdaten erfassen:

### Aufforderung, bestimmte Symptome (z.B. hohes Fieber, Erkältungssymptome, starker Husten) zu melden

An dieser Stelle ist hervorzuheben, dass solche Symptome zwar mit dem Covid-19-Virus in Verbindung gebracht werden – ein alleiniger Anhaltspunkt, dass eine Infizierung vorliegt, ist das aber nicht. Somit müssten noch weitere Tatsachen hinzukommen wie ein Aufenthalt in einem Risikogebiet oder der Kontakt zu einer infizierten Person.

### Fiebermessen vor Arbeitsbeginn

Auch hier gilt: Allein die Tatsache, dass jemand Fieber hat, lässt keinen Rückschluss auf eine Infizierung zu. Denkbar wären anderweitige Gesundheitsuntersuchungen. So könnten Arbeitgeber Interesse daran haben, einen Covid-19-Schnelltest an ihren Mitarbeitern durchzuführen, sofern ein solcher zu einem späteren Zeitpunkt verfügbar ist.

### Weitergabe von Gesundheitsdaten an Dritte

Möglich ist zudem, dass der Arbeitgeber Gesundheitsdaten an Dritte weitergeben möchte oder sogar muss (siehe Rechtsgrundlagen weiter unten). In Betracht kommen hier etwa Behörden wie das Gesundheitsamt oder Kollegen und Kolleginnen, die, weil ein Mitarbeiter positiv getestet wurde, sich nun ebenfalls einer

Untersuchung unterziehen müssen, sowie Kunden oder Gäste des jeweiligen Mitarbeiters, die mit ihm Kontakt hatten.

### Bekanntgabe einer Infizierung an weitere Konzerngesellschaften

Um einen Überblick zu haben, wie viele Mitarbeiter im Unternehmen und insbesondere im Konzern von der aktuellen Situation betroffen sind, könnte ein Verantwortlicher daran denken, Gesundheitsdaten an andere Konzerngesellschaften weiterzugeben. Hier dürfte es allerdings ausreichend sein, lediglich eine Anzahl betroffener Personen zu melden, ohne die Namen zu nennen.

Zu beachten ist allerdings, dass trotzdem ein Personenbezug möglich ist, sofern z.B. eine Konzerngesellschaft einen einzigen Erkrankten meldet und zu diesem Zeitpunkt nur ein einziger Mitarbeiter krankheitsbedingt abwesend ist.

## Rechtsgrundlagen

Je nachdem, welche konkrete Maßnahme der Arbeitgeber umsetzen möchte, ob er z.B. eine Gesundheitsuntersuchung an den Mitarbeitern durchführen oder Daten an Dritte weitergeben möchte/muss, greifen unterschiedliche Rechtsgrundlagen.

### DSGVO, BDSG, ArbSchG und IfSG

Die DSGVO, das Bundesdatenschutzgesetz (BDSG) und weitere Gesetze wie das Arbeitsschutzgesetz (ArbSchG) und das Infektionsschutzgesetz (IfSG) ermöglichen es Arbeitgebern, sensible personenbezogene Daten der Beschäftigten im Arbeitsverhältnis zu verarbeiten.

### Wesentlich: die Fürsorgepflicht

Vorangestellt sei an dieser Stelle: Verarbeitet ein Arbeitgeber Gesundheitsdaten für Zwecke des Beschäftigungsverhältnisses, ist dies zulässig, sofern es erforderlich ist, um Rechte auszuüben oder rechtliche Pflichten zu erfüllen aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes und kein Grund zur Annahme besteht, dass das schutzwürdige Interesse des Betroffenen am Ausschluss der Verarbeitung überwiegt.

**WICHTIG**

***Im Arbeitsverhältnis dürfen auch Gesundheitsdaten verarbeitet werden, sofern es für die Zwecke des Beschäftigungsverhältnisses erforderlich ist. Das ist z.B. der Fall, wenn der Arbeitgeber arbeitsrechtlichen Verpflichtungen nachkommen muss. Denn ihn treffen diverse Fürsorgepflichten gegenüber seinen Angestellten. Das ergibt sich u.a. aus § 618 Bürgerliches Gesetzbuch (BGB). Eine dieser Fürsorgepflichten ist die Gesundheitsvorsorge. Dazu hat der Arbeitgeber vermeidbare Schäden für seine Arbeitnehmer abzuwenden. Ein solcher Schaden könnte etwa entstehen, wenn andere Arbeitnehmer sich mit dem Covid-19-Virus anstecken würden, weil der Arbeitgeber Maßnahmen der Gesundheitsfürsorge unterlassen hat.***

Darüber hinaus kommen als weitere Rechtsgrundlagen in Betracht:

### Einwilligung (Art. 6 Abs. 1 Buchst. a DSGVO)

Die Einwilligung ist als Rechtsgrundlage stets das letzte Mittel der Wahl. Doch das oben angesprochene „vorsorgliche Fiebermessen" zu Arbeitsbeginn wäre beispielsweise eine Maßnahme, die der Arbeitgeber schwerlich auf eine andere Rechtsgrundlage als die der Einwilligung stützen könnte.

### Lebenswichtige Interessen (Art. 6 Abs. 1 Buchst. d DSGVO)

Die Verarbeitung personenbezogener Daten kann auch erforderlich sein, um lebenswichtige Interessen der betroffenen Person oder einer anderen natürlichen Person zu schützen. Erwägungsgrund 46 DSGVO erwähnt ausdrücklich die Notwendigkeit, Epidemien und ihre Ausbreitung zu überwachen. Eine Epidemie beschreibt dabei die Ausbreitung einer Erkrankung in örtlich beschränkter Weise. Sofern die Erkrankung auch über die Landes- und Kontinentsgrenzen hinausgeht, wird von einer Pandemie gesprochen. Da der Erwägungsgrund von „Epidemie" spricht, muss sich eine Verarbeitung personenbezogener Daten erst recht im Fall einer Pandemie auf Art. 6 Abs. 1 Buchst. d DSGVO stützen lassen.

Allerdings beschreibt der Erwägungsgrund auch, dass Verantwortliche die Verarbeitung zum Schutz lebenswichtiger Interessen nur dann heranziehen sollen, wenn keine offensichtlich andere Rechtsgrundlage einschlägig ist. Dennoch gilt: Für Notfallsituationen darf sich der Arbeitgeber hierauf stützen.

Für Gesundheitsdaten müssen Verantwortliche auch Art. 9 Abs. 2 Buchst. c DSGVO heranziehen. Er schränkt die Verarbeitung insoweit ein, als der Schutz lebenswichtiger Interessen dann erforderlich sein kann, wenn die betroffene Person aus körperlichen oder rechtlichen Gründen außerstande ist, ihre Einwilligung abzugeben. Die vorher beschriebene Notsituation muss also – sollte man sich auf diese Rechtsgrundlage stützen wollen – bereits so weit eskaliert sein, dass ohne die Verarbeitung der personenbezogenen Daten eine Gefahr für Leib und Leben des Betroffenen besteht.

### Berechtigte Interessen (Art. 6 Abs. 1 Buchst. f DSGVO)

Die Verarbeitung könnte sich je nach Sachverhalt auch darauf stützen, dass sie zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich ist. Interessen oder Grundfreiheiten der betroffenen Person dürfen allerdings nicht überwiegen.

**BEISPIEL**

So wäre denkbar, Auswertungen zu Erkrankungen innerhalb des Unternehmens hierauf zu stützen, um einen Überblick über die Erkrankungssituation zu erhalten.

Erwägungsgrund 48 DSGVO spricht davon, dass ein berechtigtes Interesse gegeben sein kann, wenn personenbezogene Daten – auch von Beschäftigten – für interne Verwaltungszwecke an Konzerngesellschaften übermittelt werden. →

Zu beachten ist jedoch, dass der Betroffene die Möglichkeit hat, jederzeit gegen die Verarbeitung seiner Daten Widerspruch einzulegen. Sollte ein Arbeitnehmer von diesem Recht Gebrauch machen, darf der Arbeitgeber diese Daten nicht mehr verarbeiten, außer er kann zwingende schutzwürdige Gründe für die Verarbeitung nachweisen. Auf ihr Widerspruchsrecht ist die betroffene Person spätestens zum Zeitpunkt der ersten Kommunikation ausdrücklich hinzuweisen. Aus Gründen der Praktikabilität ist diese Rechtsgrundlage daher nur bedingt tauglich.

### Quarantäne und Tätigkeitsverbot (§§ 30, 31 IfSG)

Auch das Infektionsschutzgesetz kann eine Rechtsgrundlage zur Verarbeitung sensibler Daten bieten. So ist dort beispielsweise geregelt, dass die zuständige Behörde Kranken, Krankheitsverdächtigen, Ansteckungsverdächtigen und Personen, die zwar keine Symptome zeigen, aber Erreger übertragen könnten, die Ausübung bestimmter beruflicher Tätigkeiten ganz oder teilweise untersagen kann.

### Rechtliche Verpflichtung (Art. 6 Abs. 1 Buchst. c DSGVO)

Die Datenverarbeitung kann erforderlich sein, um eine rechtliche Verpflichtung zu erfüllen, der der Arbeitgeber unterliegt. Diese Rechtsgrundlage kann z.B. in Verbindung mit Vorschriften des Infektionsschutzgesetzes stehen:

### Abwenden von Gefahren durch übertragbare Krankheiten (§ 16 Abs. 1 und Abs. 2 Satz 3 IfSG)

Hiernach kann die zuständige Behörde (z.B. das Gesundheitsamt) notwendige Maßnahmen treffen, um Gefahren abzuwenden, die durch übertragbare Erkrankungen entstehen. Die hierbei erhobenen personenbezogenen Daten dürfen nur für Zwecke des Infektionsschutzgesetzes verarbeitet werden.

Hierfür kann es erforderlich sein, dass ein Arbeitgeber bestimmte Daten einer zuständigen Behörde übermitteln muss. Denn dann unterliegt der Arbeitgeber gemäß Art. 6 Abs. 1 Buchst. c sowie Abs. 2 und 3 DSGVO einer rechtlichen Verpflichtung, diese Daten zu verarbeiten.

## Art. 13 und 14 DSGVO

## Informationspflichten

Der Verantwortliche muss zum Zeitpunkt der Datenerhebung die betroffene Person entsprechend Art. 13 DSGVO informieren. Liegt eine Anordnung vor, dass der Arbeitgeber Daten z.B. an Behörden wie das Gesundheitsamt übermitteln muss, muss er den Betroffenen auch hierüber ins Bild setzen.

Sofern es darum geht, personenbezogene Daten nicht direkt bei der betroffenen Person zu erheben, muss eine Information entsprechend Art. 14 DSGVO erfolgen. Das kann z.B. der Fall sein, wenn ein infizierter Mitarbeiter Auskunft darüber geben muss, mit welchen Personen er in letzter Zeit Kontakt hatte, um auch diesen Personen zu ermöglichen, weitergehende Maßnahmen zu veranlassen.


Bild: iStock.com/photoguns

## Verzeichnis von Verarbeitungstätigkeiten

Je nachdem, wie ein Arbeitgeber Gesundheitsdaten im Arbeitsverhältnis verarbeitet, muss er diese Verarbeitung als neue Tätigkeit in das Verzeichnis von Verarbeitungstätigkeiten aufnehmen. Wichtig ist, Überlegungen zur Erforderlichkeit und zur Rechtsgrundlage zu dokumentieren. Je nach Fallkonstellation kann die Rechtsgrundlage variieren. Auch die Übermittlung an externe Stellen, etwa an das Gesundheitsamt, muss hier dargestellt sein.

Sofern bereits ähnliche Verarbeitungstätigkeiten existieren, z.B. Gesundheitsuntersuchungen im Beschäftigungsverhältnis, muss der Arbeitgeber prüfen, ob sich die konkret geplanten Maßnahmen im Zusammenhang mit der Covid-19-Situation hierunter subsumieren lassen bzw. ob es notwendig ist, diese Verarbeitungstätigkeit zu überarbeiten und anzupassen.

So ist insbesondere danach zu differenzieren, ob die Maßnahme auf derselben Rechtsgrundlage beruht. Führt der Arbeitgeber beispielsweise arbeitsmedizinische Vorsorgeuntersuchungen durch, weil der Mitarbeiter während seiner Arbeit mit Gefahrstoffen in Berührung kommt, lässt sich darauf kein Fiebermessen stützen.

Bietet ein Unternehmen dagegen freiwillige Untersuchungen an, deren Rechtmäßigkeit eine Einwilligung sicherstellt, ließe sich ein ebenso freiwilliges Fiebermessen hierunter fassen.

## Fazit: Es geht v.a. um Fürsorgepflichten

Der Arbeitgeber hat insbesondere aufgrund seiner Fürsorgepflichten die Möglichkeit, Gesundheitsdaten im Beschäftigungsverhältnis zu verarbeiten. Es können aber auch andere Rechtsgrundlagen infrage kommen. Den Arbeitnehmer seinerseits treffen gewisse Nebenpflichten. Sie können so weit gehen, dass er seine Gesundheitsdaten preisgeben muss – unter sehr engen Voraussetzungen und je nach Konstellation im Einzelfall. Das gilt v.a., wenn er dadurch, dass er die Daten nicht preisgibt, andere gefährden würde.

Doris Kiefer ist Rechtsanwältin, zertifizierte Datenschutzbeauftragte (IHK) und Data Protection Risk Manager (FOM) in München.

Bild: iStock.com/AleksandarNakic

**Einträchtiges Arbeiten von zu Hause aus – derzeit wohl keine seltene Situation**

Mit Richtlinien arbeiten

# Homeoffice und Datenschutz – so passt beides zusammen

**Die Corona-Krise hat dafür gesorgt, dass mehr Beschäftigte im Homeoffice arbeiten als jemals zuvor. In der ersten Not war der Datenschutz oft kein Thema. Das sollte sich nun ändern.**

Viele Unternehmen haben in Rekordzeit ihre Mitarbeiter ins Homeoffice geschickt. Dass dabei sicher nicht der Datenschutz im Vordergrund stand, sondern die Beschäftigten zu schützen und den Betrieb irgendwie aufrechtzuerhalten – verständlich und geschenkt. Doch nun ist es an der Zeit, näher hinzuschauen und für geregelte Bahnen auch in puncto Datenschutz zu sorgen.

## „Homeoffice" ist nicht gesetzlich definiert

Ebenso wie viele andere immer wieder verwendete Begriffe – mobile office, remote work oder mobile Arbeit – ist das „Homeoffice" nicht (gesetzlich) definiert.

Geht es darum, die Arbeitsleistung außerhalb des vereinbarten Dienstorts zu erbringen, ist allein der Begriff „Telearbeit" eindeutig bestimmt. So legt § 2 Abs. 7 der Arbeitsstättenverordnung fest, dass Telearbeitsplätze Bildschirmarbeitsplätze sind, die der Arbeitgeber im Privatbereich des Beschäftigten fest eingerichtet hat. Bei der Telearbeit geht es also ausschließlich um die Arbeit von zu Hause mithilfe eines vom Arbeitgeber eingerichteten Arbeitsplatzes.

Daraus entstehen sowohl für den Arbeitgeber als auch für die Beschäftigten Rechte und Pflichten (Kostentragung, Zutrittsrecht, Vertraulichkeit, Gestaltung des Arbeitsplatzes etc.), die einer ausdifferenzierten Vereinbarung bedürfen. In der aktuellen Situation wünschen sich zwar sowohl Vorgesetzte wie Beschäftigte, „von zu Hause aus zu arbeiten". Keiner der Beteiligten möchte aber deshalb gleich einen Telearbeitsplatz einrichten müssen.

## Mit „Homeoffice" ist nicht nur zu Hause gemeint

Vor diesem Hintergrund wird der Begriff „Homeoffice" vielfach missverständlich und zu eng verwendet. Denn trotz des Wortteils „home" heißt „Homeoffice" nicht zwingend, einen Arbeitsplatz zu Hause zu haben. Es geht vielmehr darum, generell mobil zu arbeiten. Das kann zu Hause sein, aber in den Zeiten vor und nach Corona auch im Zug, am Flughafen oder anderswo.

PRAXIS-TIPP

Dass eine gesetzliche Definition fehlt, macht es möglich, diese mobile Arbeit nach den Wünschen der Beteiligten und den technischen Möglichkeiten des Unternehmens (nahezu) frei und individuell zu gestalten. Diese Ausgestaltung sollte der Arbeitgeber schriftlich festhalten. Geht es nicht nur um eine vorübergehende Einrichtung wie derzeit vielfach, bietet sich beispielsweise ein Zusatz zum Arbeitsvertrag an.

Dabei kommt es den Beteiligten zugute, dass zu den Gebieten, die hierbei zu regeln sind (Arbeitszeit, Arbeitsschutz, Vertraulichkeit, Einbezug der Personal- bzw. Arbeitnehmervertretung etc.), und auch zum Datenschutz vielfach schon Vereinbarungen und Regeln existieren. Auf diese bestehenden Absprachen lässt sich für die Arbeit, die nicht am vereinbarten Dienstort erbracht wird, verweisen. Denn auch mobile Arbeit ist letztlich immer vertragliche Arbeitsleistung!

## Richtlinie für Datenschutz und Datensicherheit

Da der Arbeitgeber als der im datenschutzrechtlichen Sinne „Verantwortliche" in der Pflicht ist, das geltende Datenschutzrecht einzuhalten, haftet er auch für etwaige Datenschutzverstöße, die in seinem Verantwortungsbereich liegen. Vereinbaren Arbeitgeber und Arbeitnehmer also das Arbeiten im Homeoffice, sollte dies in der Regel auf Grundla- →

ge einer existierenden Richtlinie bzw. auf Basis einer entsprechenden Vereinbarung mit dem Beschäftigten erfolgen.

Diese Richtlinie bzw. Vereinbarung sollte mit Blick auf Datenschutz und Datensicherheit zumindest die folgenden Aspekte berücksichtigen:

### Informationen und Equipment sicher aufbewahren

- Arbeiten die Beschäftigten nicht mit privater Ausstattung: Alle Eigentumsrechte an zur Verfügung gestellter Hardware, Software, Apps und Daten liegen beim Arbeitgeber. Er besitzt zu jeder Zeit das Recht, darauf zuzugreifen.
- Die Mitarbeiter dürfen nur genehmigte IT-Systeme, Anwendungen oder Dienste nutzen, um auf Unternehmensinformationen zuzugreifen, sie zu speichern oder zu verarbeiten.
- Unternehmensinformationen dürfen die Mitarbeiter nur auf tragbaren Geräten oder Wechseldatenträgern speichern, bei denen die Verschlüsselung aktiviert ist.

### Zulässige IT-Nutzung

- Die vorinstallierten Sicherheitsfunktionen auf den IT-Systemen dürfen nicht modifiziert, entfernt oder anderweitig umgangen werden.
- Die Beschäftigten dürfen keine unternehmensfremden tragbaren Geräte an die IT-Systeme anschließen und auch keine fremden Geräte direkt mit dem Firmennetzwerk verbinden.
- Das mobile Arbeiten darf drahtlose Internetverbindungen nutzen (z.B. eigener Mobilfunk- oder Kabelanbieter oder Hotel-WLAN). Aber der Zugang zum Unternehmensnetzwerk muss in gesicherter Form erfolgen (z.B. über VPN).
- Unternehmensinformationen und tragbare Geräte, auf denen solche Informationen gespeichert sind, muss der Beschäftigte persönlich bei sich führen oder an einem sicheren Ort verschlossen aufbewahren.

### Clear Desk

- Vertrauliche oder geheime Informationen dürfen niemals unbeaufsichtigt auf dem Schreibtisch liegen bleiben. Die Beschäftigten sollten Informationen sicher in einem verschlossenen Schrank aufbewahren, wenn sie nicht in Gebrauch sind.
- Tragbare Geräte, Sicherheitstoken und Schrankschlüssel müssen nach jedem Arbeitstag weggeschlossen bzw. vor dem Zugriff Dritter geschützt werden.
- Beschäftigte müssen die Bildschirmsperre auf ihrem Computer oder ihrem tragbaren Gerät aktivieren, wenn sie ihren Schreibtisch bzw. das Gerät unbeaufsichtigt lassen.
- Nur legitimierte Personen dürfen vertrauliche oder geheime Informationen auf dem Bildschirm einsehen.

### Vor dem Klicken: nachdenken

- Beschäftigte müssen die Quellen von E-Mails, Nachrichten, Anrufen und Verbindungen in den sozialen Medien überprüfen, bevor sie Informationen weitergeben, auf Links klicken, Anhänge öffnen oder andere Anweisungen befolgen.
- Mitarbeitende müssen Vorsicht walten lassen, bevor sie Anhänge öffnen oder auf Links klicken, die zu Inhalten auf fremden Websites führen.

### Umgang mit ID & Passwörtern

- Passwörter, PINs oder Zugriffscodes dürfen niemals an andere weitergegeben werden.
- Beschäftigte dürfen ihre Unternehmens-Kontennamen, die E-Mail-Adresse oder die Passwörter nicht verwenden, um sich für private Zwecke in externen Diensten anzumelden.

### Sicherheitsvorfall?

- Erlangen Beschäftigte Kenntnis von einer Verletzung des Datenschutzrechts oder der Datensicherheit, informieren sie umgehend ihre Vorgesetzen.

## Privatgeräte im Homeoffice

**Einigen sich Arbeitgeber und Beschäftigte darauf, Privatgeräte betrieblich zu nutzen, ist Vorsicht geboten. Grundsätzlich gehören Privatgeräte zur Privatsphäre der Beschäftigten, in der der Arbeitgeber nichts zu suchen hat.**
**Zugleich muss ein Arbeitgeber sicherstellen, dass betriebliche Daten auf den privaten Geräten seiner Kontrolle unterstehen und dass die Beschäftigten gesetzliche Sicherheitsvorgaben beachten. Hierbei sind im Wesentlichen Art. 32 Datenschutz-Grundverordnung (DSGVO) und das Gesetz zum Schutz von Geschäftsgeheimnissen (GeschGehG) zu berücksichtigen. Ein Arbeitgeber ist verpflichtet, nachzuweisen, dass er die Beschäftigten über die zu beachtenden Sicherheitsmaßnahmen unterrichtet und sich Kontrollrechte hat einräumen lassen.**
**Hat ein Arbeitgeber keine Vereinbarung hierzu getroffen, dann besitzt er keine Kontrollrechte im Hinblick auf die Informationen, die auf den Privatgeräten gespeichert sind, und verstößt somit in der Regel gegen gesetzliche Vorgaben.**
**Kann ein Arbeitgeber zudem nicht nachweisen, dass er die Beschäftigten über mögliche Risiken belehrt und sie verpflichtet hat, sie zu vermeiden, kann er nicht nachweisen, dass er ein hinreichendes Datenschutzniveau gewährleistet.**

## Die passende IT-Ausstattung

Zu den weiteren Aufgaben des Arbeitgebers gehört es, eine IT-Ausstattung bereitzustellen, mit der die datenschutzgerechte Arbeit im Homeoffice möglich ist. Gibt ein Unternehmen z.B. Notebooks heraus, dann nur solche mit verschlüsselter Festplatte. Das gilt auch für die vom Arbeitgeber herausgegebenen USB-Sticks.

Ein Konzept zur Vernichtung sensibler Daten vervollständigt die Liste der Aufgaben des Arbeitgebers.

Arnd Fackeldey ist Geschäftsführer der Digital Compliance Consulting GmbH. Als DSB und Auditor unterstützt er Unternehmen bei Design und Einführung von DS-Prozessen sowie DSB und BR bei Kontrollaufgaben.


Bild: iStock.com/Rawf8

**Auch die Corona-Krise nutzen Cyberkriminelle derzeit, um Nutzer per Trojaner in die Falle zu locken. Umso wichtiger ist es jetzt, die Beschäftigten für diese Gefahr zu sensibilisieren.**

Corona als Köder

# So arbeitet ein Trojaner

**Trojaner der neuesten Generation sind eine möglicherweise existenzbedrohende Gefährdung für Unternehmen. Sensibilisierte Mitarbeiter sind das A & O, um solchen Angriffen keine Chance zu geben.**

Angreifern reicht es mittlerweile, einen Beschäftigten im anvisierten Unternehmen oder im Homeoffice dazu zu bringen, dreimal zu klicken. Wie gehen die Profis dabei vor? Und wie können sich Unternehmen und Behörden vor solchen Angriffen schützen?

## Emoted – professioneller geht es kaum

Der derzeit am schlimmsten wirkende Trojaner ist wohl Emoted. Emoted ist nicht nur ein Trojaner, sondern eine Sammlung von angreifenden Gemeinheiten. Sie ändert sich fast täglich und passt sich an Abwehrstrategien an.

Anders als früher ist eine Infektion in der Regel nicht mehr sofort erkennbar. Moderne Trojaner versuchen, so lange wie möglich auf den Systemen zu bleiben. Sie arbeiten eine ganze Reihe von Spezialaufgaben ab. Gerade Emoted, bei dem vermutet wird, dass er von international kooperierenden Mafiagruppen erstellt und gewartet wird, ist ein wahres Multitalent an schädlichen Einwirkungen.

## Wie wirkt Emoted?

1. **Einnisten:** Emoted manifestiert sich auf dem System und bleibt so lange wie möglich im Hintergrund.
2. **Mailkontakte:** Emoted späht Mailkontakte aus, um später echt wirkende Lockmails aus realen Kundenkontakten zu versenden und so weitere Systeme zu übernehmen.
3. **Informationsabfluss:** Wo möglich, kopiert der Trojaner Dateien und verschickt sie unerkannt „nach Hause".
4. **Bankinformationen:** Emoted ist auch in der Lage, Bankkonten auszuspähen.
5. **Kontrollübernahme:** Der Trojaner breitet sich an strategisch wichtigen Stellen aus, um die spätere Verschlüsselung „wasserdicht" zu bekommen.
6. **Besuch:** Bei wichtigen Angriffszielen kommen die Angreifer auch selbst getarnt in das angegriffene Netzwerk.
7. **Lösegeld:** Erst ganz am Ende erfolgt die Verschlüsselung mit der Lösegeldforderung. Leider merken viele angegriffene Unternehmen erst in diesem Moment, dass sie ungebetenen Besuch haben.
8. **Systemerneuerung:** Oft gelingt es auch nach Lösegeldzahlung nicht mehr, die Angreifer ganz zu vertreiben. Systeme müssen neu aufgesetzt werden.

Anders als frühere Angreifer verschlüsselt Emoted erst zum Schluss die Daten. Nur wenn das Unternehmen, die Behörde oder die Klinik Lösegeld zahlt, erhält es oder sie den Schlüssel, um mit den Daten weiterarbeiten zu können. Leider bemerken viele betroffene Unternehmen erst mit diesem letzten Schritt überhaupt den Angriff. Alles, was vorher geschieht, registrieren die Opfer oft gar nicht.

## Wie läuft ein Angriff ab?

**Schritt 1:** Normalerweise kommen Trojaner über Office-Dateien ins Netzwerk. Über eine E-Mail oder eine andere elektronische Nachricht versuchen die Angreifer, einen Anwender dazu zu bringen, eine Word-Datei, eine Excel-Datei oder eine Datei eines der anderen zahlreichen Formate zu laden, aus denen heraus sich ein Makro, also ein Zusatzprogramm für Word und Excel, einschleusen lässt.

**Schritt 2:** In einem zweiten Schritt muss der Anwender diese Datei öffnen. Bis zu diesem Punkt ist bei den Einstellungen, die für Office-Programme üblich sind, der Trojaner noch nicht aktiv. Erst wenn der Anwender das Programm öffnet, erhält er die Aufforderung, entweder ein Makro nachzuladen oder eine fingierte Fehlermeldung anzuklicken.

**Schritt 3:** Geschieht das, lädt das Makro oder ein durch die Fehlermeldung installiertes Programm den eigentlichen Trojaner nach. Das erfolgt aus Word oder →

Excel heraus und umgeht den Virenscanner. Achtung: Ab jetzt läuft der Angriff von allein ab – kein Eingriff mehr möglich!

## Wirksame Gegenmaßnahmen

Wer verhindern möchte, dass Trojaner über die berühmten drei Klicks ins Netzwerk gelangen, muss

- die Anwender schulen,
- dafür sorgen, dass sich bestimmte Dateien nicht ausführen lassen, und
- informationstechnische Systeme und Netze strukturiert überprüfen.

## Anwender schulen

Die meisten beschäftigten Personen gehen davon aus, dass ihnen diese drei Klicks nicht passieren. Sie denken dabei nur an die üblichen schlecht gemachten Phishing-Mails. In der Tat kommt heute hoffentlich niemand mehr auf die Idee, auf eine E-Mail zu antworten, die einem zehn Prozent eines dreistelligen Millionengewinns aus einer Lotterie verspricht.

### Ein gut gemachter Lockvogel

So plump kommen moderne Trojaner nicht mehr daher. Stellen Sie den Kollegen das unten stehende Beispiel vor, versehen mit Logo, Adresse und weiteren Angaben der eigenen Stadtwerke.

Wer das beigefügte Word-Dokument öffnet, sieht eine Tabelle, die in 50-€-Schritten Beträge zwischen null und 1.500 € angibt. Die Spalten zwischen 650 € und 900 € sind in unterschiedlichen Grüntönen hinterlegt. Dazu erscheint ein Text, der dazu auffordert: „Wenn Sie den genauen Betrag wissen möchten, sollten Sie dieses völlig harmlose Makro einfach öffnen." Tut man das, erscheint der Betrag mit der Zeile „700–750 €" in grüner Farbe. Mehr passiert auf den ersten Blick nicht. Experten gehen davon aus, dass mehr als 70 % in dieser sehr gut gemachten Mail tatsächlich klicken würden.

### Vorsicht bei Mails aus realen Kundenkontakten

Noch schwieriger wird es, wenn Beschäftigte eine Mail erhalten, die aus einem realen Kundenkontakt stammt. Idealerweise – für die Angreifer – ist es zudem üblich, mit dem realen Kundenkontakt regelmäßig Word-Dokumente auszutauschen. In unserer Firma ist das neulich wie folgt geschehen: Ein Mitarbeiter erhält eine E-Mail eines realen Kunden, mit dem er regelmäßig Kontakt hat. Die Mail enthält eine verschlüsselte ZIP-Datei. Diese Vorgehensweise war bei dem Kunden früher an der Tagesordnung, jetzt aber aufgrund des Sicherheitsrisikos nicht mehr.

Sehr geehrte Damen und Herren, herzlichen Glückwunsch!

Sie haben im vergangenen Jahr weniger Energie verbraucht, als Sie Vorauszahlung geleistet haben. Sie bekommen also Geld von uns zurück.

Natürlich teilen wir Ihnen in dieser Mail nicht mit, wie viel Sie genau bekommen. Die meisten Anwender wissen, dass sich auf diesem Weg Angreifer ihr Vertrauen erschleichen wollen. Daher werden wir Ihnen den genauen Betrag der Rückzahlung in einem gesonderten Schreiben an Ihre bei uns hinterlegte Postadresse mitteilen.

Da uns jedoch etliche Kunden wissen ließen, dass sie es gut finden, wenn zumindest der ungefähre Betrag schon vorab bekannt wäre, haben wir uns zu diesem Schritt entschlossen: Öffnen Sie bitte beiliegende Word-Datei, und Sie werden auf 50 € genau ersehen, wie hoch der zu erwartende Rückzahlungsbetrag ist.

Bei Rückfragen wenden Sie sich gern an folgende Telefonnummer: XXXYYZZZ.

Mit freundlichen Grüßen, Ihre Stadtwerke (Unterschrift)

**PRAXIS-TIPP**

***Selbst über reale Kundenkontakte können Angreifer ihren Schadcode verbreiten. Das bedeutet, dass Kolleginnen und Kollegen, die auf diesen Trick nicht hereinfallen sollen, zum einen ihre Prozesse genau kennen und zum anderen wissen müssen, an wen sie sich wenden, wenn ihnen im Prozess etwas seltsam vorkommt.***

### Bei Prozessabweichungen misstrauisch werden!

An diesen Umstand erinnerte sich der Mitarbeiter. Entsprechend vorsichtig entschlüsselte er die ZIP-Datei. Er fand drei Word-Dateien, alle älteren Datums. Jetzt war er endgültig alarmiert. Tatsächlich wurde er beim Öffnen der ersten Word-Datei dazu aufgefordert, eine Fehlermeldung zu bestätigen. Ein Klick auf diese Meldung hätte Emoted installiert.

Dass die IT in der Lage ist, verdächtige Dateien zu untersuchen, sollte in jedem Unternehmen selbstverständlich – und bekannt! – sein. Entscheidend ist, wie Sie die Beschäftigten dazu bringen, den verdächtigen Prozess zu erkennen.

### Konkretes Training wirkt besser

Etlichen Kolleginnen und Kollegen fehlt schlicht und ergreifend die Fantasie, um sich vorzustellen, dass eine einzige angeklickte Mail und eine einzige geöffnete Datei samt installiertem Makro die ganze Firma lahmlegen können. Hier helfen z.B. Dienstleister, über gefakte Mails eine reale Angriffssituation zu simulieren.

### 10 Prozent klicken trotzdem …

Geben Sie sich allerdings keinen Illusionen hin. Untersuchungen zeigen, dass bis zu zehn Prozent der Beschäftigten trotz aller präventiven Bemühungen klicken. Lesen Sie daher im zweiten Teil, welche technischen Maßnahmen sinnvoll sind.

Eberhard Häcker kennt sich als ehemaliger Berufsschullehrer und langjähriger externer DSB bestens mit der Schulung von Beschäftigten aus.

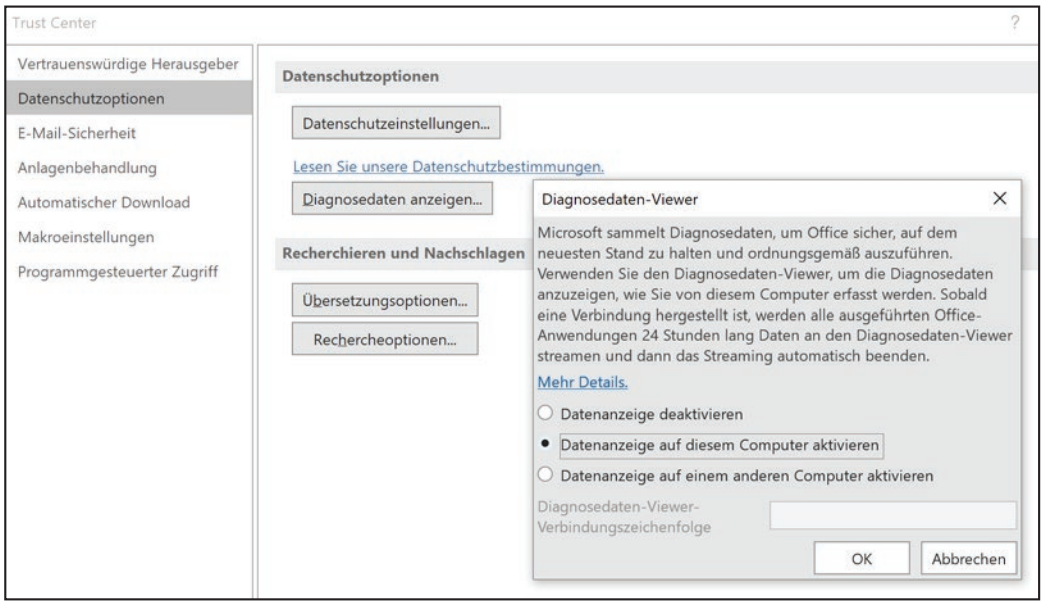



**Abbildung 1: So lassen sich die Diagnosedaten für Microsoft Office 365 aktivieren**

alle Screenshots: Prof. R. Gerling

Telemetriedaten & Analysedienste

# Office 365: ein technisches Datenschutz-Update

**Es wird viel über die Übertragung der Diagnosedaten von Office 365 an Microsoft diskutiert. Mittlerweile gibt es Möglichkeiten, diese Datenübertragung zu deaktivieren. Wir zeigen Ihnen, was sich alles abschalten lässt – und was Sie auch abschalten sollten. Zusätzlich stellen wir die Analytics-Analysedienste vor.**

Im 9. Tätigkeitsbericht 2019 trifft das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) in Kapitel 3.4 „Windows 10 und Telemetriedaten" die Aussage, bei Windows 10 Enterprise Version 1909 lasse sich die Übermittlung der sogenannten Telemetriedaten an Microsoft komplett ausschalten (siehe https://ogy.de/baylda-tb-2019, S. 22). Das BayLDA gibt jedoch keine genauen Hinweise auf die ebenfalls dort zitierten „von Microsoft offiziell zur Verfügung gestellten Informationen und Tools". Der Umkehrschluss ergibt, dass Nutzer die Übermittlung von Messdaten in Windows Home/Professional und Education nicht komplett ausschalten können.

## Diagnosedaten anzeigen lassen

Bei Microsoft Office 365 ist die Situation besser. Hier gibt es die Möglichkeit, die Übermittlung der Telemetriedaten komplett zu deaktivieren. Ein erster Schritt in diese Richtung ist, sich zunächst die Diagnosedaten anzeigen zu lassen.

Um Office-365-Diagnosedaten zu sammeln, gehen Sie in eine beliebige Office-Anwendung und wählen „Datei" ⇨ „Optionen" ⇨ „Trust Center" ⇨ „Einstellungen für das Trust Center" ⇨ „Datenschutzoptionen" aus. Unter „Diagnosedaten anzeigen" schalten Sie die Option „Datenanzeige auf diesem Computer aktivieren" ein (Abbildung 1). Sie können dann in der Diagnosedatenanzeige sehen, welche Daten an Microsoft übertragen wurden, und die Wirksamkeit von Einstellungen direkt überprüfen. Um auch Windows-10-Diagnosedaten zu bekom- →

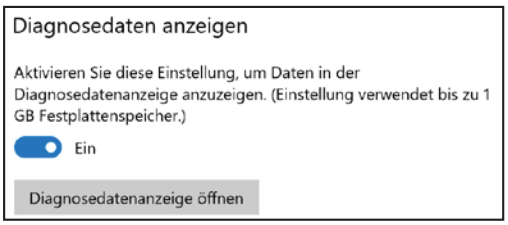



**Abbildung 2: Diagnosedaten für Windows 10 aktivieren**

**PRAXIS-TIPP**

*Sorgen Sie als DSB dafür, dass der Verantwortliche die Beschäftigten deutlich darauf hinweist, dass sie die mobilen Office-365-Apps für iOS und Android nicht einsetzen dürfen. Das Gleiche gilt für die Office-365-Web-Apps, da sich bei ihnen die Übertragung von Diagnosedaten noch nicht abstellen lässt.*

men, suchen Sie in der Anwendung „Microsoft Store" nach „Diagnostic Data Viewer". Dann wechseln Sie in das Startmenü und wählen „Einstellungen" ⇨ „Datenschutz" ⇨ „Diagnose & Feedback" aus. Dort stellen Sie den Schalter unter „Diagnosedaten anzeigen" auf „ein". So werden die Diagnosedaten auch lokal gespeichert.

## Empfehlungen zu Telemetrie-Einstellungen unter Office 365

Um in Office 365 Telemetrie-Einstellungen vornehmen zu können mit dem Ziel, die Menge der übertragenen Daten reduzieren, muss mindestens die Microsoft-Office-365-Version 1905 installiert sein.

### Umfang der Telemetrie-Datenübertragung

Für den Umfang der Telemetrie-Datenübertragung in Microsoft Office 365 gibt es drei Levels:

- keine Telemetriedaten senden (3)
- optionale Daten senden (2)
- erforderliche Daten senden (1)

Diese Einstellungen lassen sich über Gruppenrichtlinien oder Registry-Einstellungen vornehmen. Dabei wird in der Registry der Parameter „SendTelemetry" nutzerspezifisch entsprechend dem Wert in der Klammer gesetzt. Wir empfehlen, den Wert auf „3" („weder noch" bzw. „keine Daten") zu setzen.

### Verbundene Dienste

Darüber hinaus sollte die IT vier weitere Einstellungen zu den verbundenen Diensten (Controller Connected Experiences) setzen (Tabelle 1). Das ist aber nicht immer „nebenwirkungsfrei". Auf dem Rechner des Autors führt der Wert „DisconnectedState=2" zu Problemen mit dem Zugriff auf Office-Dateien auf WebDAV-Freigaben (konkret beim Verschlüsselungsprogram Cryptomator). Insofern muss die IT in der jeweiligen IT-Umgebung des Unternehmens oder der Behörde testen, ob Nebenwirkungen auftreten.

### Customer Experience Improvement Program

Auch das „Customer Experience Improvement Program (CEIP)" sollte die IT deaktivieren. Dazu muss sie einen Registry-Eintrag „`CEIPEnable`" erstellen und auf null setzen (siehe Listing 1). Gleichzeitig gilt es, zwei Aufgaben zu deaktivieren. Dazu startet man die „Aufgabenplanung", sucht unter „Aufgabenplanungsbibliothek" ⇨ „Microsoft" ⇨ „Windows" ⇨ „Customer Experience Improvement Program" nach den beiden Aufgaben „Consolidator" und „UsbCeip" und deaktiviert sie über das Kontextmenü. Diese beiden Programme sammeln und übertragen regelmäßig die Daten zum CEIP.

### LinkedIn-Integration

Dann ist empfehlenswert, die LinkedIn-Integration für Office 365 auszuschalten. Dazu wählt man in der Administrationsoberfläche von Office 365 („Das neue Admin Center" aktivieren) das „Azure Active Directory Admin Center" aus und dann unter „Benutzer" die „Benutzereinstellungen". Dort dann unter LinkedIn-Kontoverbindungen den „Nein"-Button auswählen. Diese Funktionalität ist für deutsche Kunden derzeit anscheinend per Default deaktiviert. Ob das tatsächlich so ist, sollte die IT aber überprüfen.

| Richtlinieneinstellung | Registrierungseinstellung | Werte |
|---|---|---|
| Umfang der von Office 365 an Microsoft gesendeten Diagnosedaten | SendTelemetry | 1 = erforderlich<br>2 = optional<br>3 = weder noch |
| verbundene Dienste, die Inhalte analysieren, in Office 365 erlauben | UserContentDisabled | 1 = aktiviert<br>2 = deaktiviert |
| verbundene Dienste, die Online-Inhalte herunterladen, in Office 365 erlauben | DownloadContentDisabled | 1 = aktiviert<br>2 = deaktiviert |
| zusätzliche optionale verbundene Dienste in Office 365 erlauben | ControllerConnectedServicesEnabled | 1 = aktiviert<br>2 = deaktiviert |
| verbundene Dienste in Office 365 zulassen | DisconnectedState | 1 = aktiviert<br>2 = deaktiviert |

**Tabelle 1: Einstellungen zum Datenschutz für Microsoft Office 365**

```
Windows Registry Editor Version 5.00

[HKEY_CURRENT_USER\Software\Policies\Microsoft\Office\16.0\Common\Privacy]
"DisconnectedState"=dword:00000002
"UserContentDisabled"=dword:00000002
"DownloadContentDisabled"=dword:00000002
"ControllerConnectedServicesEnabled"=dword:00000002

[HKEY_CURRENT_USER\Software\Policies\Microsoft\office\common\clienttelemetry]
"SendTelemetry"=dword:00000003

[HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\SQMClient]
"CEIPEnable"=dword:00000000
```

**Listing 1: Die Registry-Einstellungen, um die Telemetrie (Tabelle 1) und den CEIP-Client zu deaktivieren, als Input-Datei für den Registry-Editor. Zu den Nebenwirkungen siehe Seite 10.**

## Analytics-Analysen

Neben den bisher angesprochenen datenschutzrelevanten Funktionalitäten hat Microsoft Anfang 2020 begonnen, die Analytics-Analysen breiter zur Verfügung zu stellen. Seit Kurzem stehen einige der Funktionen auch in den Business-Lizenzen zur Verfügung, nicht nur in den Enterprise-Lizenzen.

### Microsoft MyAnalytics

Den Analysedienst „MyAnalytics" gibt es in der Office-365-Version E5 schon länger. Mittlerweile ist er auch in Microsoft 365 und allen Office-365-Business-Paketen mit E-Mail-Hosting (Exchange Online) enthalten. Microsoft wirbt damit, dass die Mitarbeiter durch die Einblicke in die persönliche Arbeitsweise mit Microsoft 365 produktiver werden. Unter anderem analysiert das Tool, wie viel Zeit ein Mitarbeiter damit verbringt, E-Mails zu lesen und zu schreiben, und zwar sowohl innerhalb als auch außerhalb der Dienstzeit. Außerdem wertet MyAnalytics aus, mit welchen Kollegen man die Zeit in Besprechungen verbringt.

Man kann sich wöchentlich E-Mails zusenden lassen, die das Zeitverhalten aufbereitet darbieten. Diese E-Mails enthalten auch personenbezogene Daten Dritter. So nennt die Analyse die Top-Kommunikationspartner namentlich. MyAnalytics ist daher datenschutzrechtlich kritisch. Das Tool verarbeitet zwar überwiegend eigene Daten. Doch es geht auch darum, Daten Dritter auszuwerten: Mit wem verbringe ich Zeit in Besprechungen? Außerdem ist der Einsatz von MyAnalytics mitbestimmt.

Beschäftigte können die Einstellungen selbst über das Portal https://myanalytics.microsoft.com verwalten. Das ist für Freiberufler und kleinste Unternehmen ein gangbarer Weg. In Unternehmen können die Administratoren für →

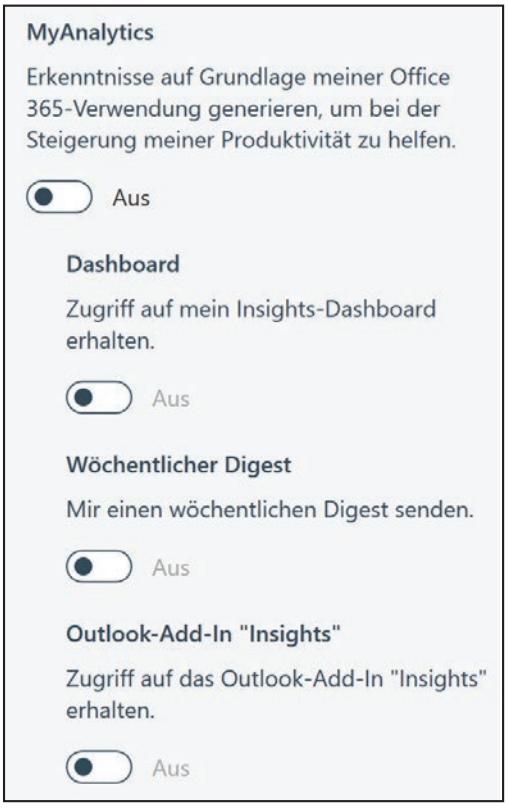



**Abbildung 3: Microsoft MyAnalytics bitte komplett deaktivieren!**

**ACHTUNG!**

*Da die Auswertungen zu MyAnalytics auf dem Exchange-Server stattfinden, ist eine Konfiguration auf dem Klienten (z.B. durch Gruppenrichtlinien) nicht möglich. Microsoft stellt unter https://ogy.de/myanalytics eine Anleitung zur Verfügung, wie sich die Einstellungen über PowerShell-Befehle deaktivieren lassen.*

## Das Outlook-Add-in Insights

**Zusätzlich lässt sich unter „MyAnalytics" das Plug-in „Insights" installieren. Dieses Plug-in für Outlook sollte jedoch nicht installiert werden, da es weitere Daten für die Analytics-Analyse sammelt.**

**ONLINE-TIPP**

- *Zusammenfassung der Datenerfassung in Office: https://privacy.microsoft.com/de-de/data-collection-Office*
- *Datenschutz-Folgenabschätzung zu Microsoft Office und Windows-Software: https://ogy.de/dpia-ms-office*

**Microsoft-Office-Produkte**

# Konfigurationsempfehlungen des BSI

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im Herbst 2019 Empfehlungen zur sicheren Konfiguration von Microsoft-Office-Produkten herausgebracht (siehe https://ogy.de/bsi-empfehlungen-ms-office). In insgesamt sieben PDF-Dateien mit einer übergreifenden Richtlinie und Einzeldokumenten zu Access, Excel, Outlook, PowerPoint, Visio und Word gibt das BSI detaillierte Einstellungsempfehlungen zu den Versionen 2013, 2016 und 2019. Insgesamt handelt es sich um 457 Einzeleinstellungen, die sich per Gruppenrichtlinie vornehmen lassen. Viele dieser Einstellungen sind per Microsoft-Default nicht konfiguriert. Das BSI empfiehlt, diese Einstellungen trotzdem auf einen festen Wert zu setzen, falls sich die Default-Werte einmal ändern.

alle Beschäftigten MyAnalytics konfigurieren – und am besten deaktivieren. Wer im Microsoft-365-Admin-Center (neue Version) angemeldet ist, kann über das „Zahnrad" die Einstellungen einblenden und dann nach einem Klick auf den Link „Einstellungen" (direkt unter der Überschrift „MyAnalytics") zu den Feature-Einstellungen wechseln. Abbildung 3 zeigt, wie sich MyAnalytics vollständig abschalten lässt.

## Microsoft Workplace Analytics

Microsoft wirbt für Workplace Analytics mit dem Satz: „Nutzen Sie das volle Potenzial Ihrer Daten durch Einblicke in die tägliche Nutzung von Office 365." Dahinter steckt eine Auswertung der Zusammenarbeit der Beschäftigten mit Office 365. Das Analysetool wertet ähnlich wie MyAnalytics gemeinsame Kalendereinträge und die Nutzung der Office-Programme aus.


**Abbildung 4: Ein (nicht personenbezogener) Ausschnitt aus einer MyAnalytics-Mail. Die E-Mail enthält auch Namen und E-Mail-Adressen von Kommunikationspartnern und Mitarbeitern.**

Workplace Analytics ermittelt z.B. die Stunden, die ein Beschäftigter durchschnittlich in Besprechungen verbringt, die Anzahl von Terminen und wie stark Mitarbeiter per E-Mail oder durch gemeinsame Meetings interagieren. Workplace Analytics wertet allerdings die Daten in der Software aus. Bei einem Termin geht es also um die eingetragene Dauer des Termins und nicht um die tatsächliche Dauer.

Das Arbeitsverhalten und die Zusammenarbeit von Teams und einzelnen Beschäftigten auszuwerten und zu vergleichen, soll die Produktivität und Effizienz des Unternehmens steigern. Diese Auswertung ist jedoch nur sinnvoll, wenn die Mitarbeiter die Kalendereinträge einheitlich nutzen. Der eine Mitarbeiter trägt nur echte Termine ein, der andere Platzhalter, um Zeiten für die ungestörte Arbeit zu blockieren. Beide Verhalten sind legitim, aber nicht vergleichbar.

Die Empfehlung: Wir bewegen uns hier im Bereich der Mitbestimmung. Verantwortliche sollten das Thema daher zuerst mit den Personalvertretungsgremien diskutieren. Ob das Werkzeug den versprochenen Nutzen bringt, sehen zudem viele Experten kritisch.

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.

**Handreichung aus Hessen**

# Datenschutz in MVZ

Medizinische Versorgungszentren (MVZ) sind gesetzlich definiert als fachübergreifende, ärztlich geleitete Einrichtungen, die über die strukturierte Zusammenarbeit mindestens zweier Ärzte mit unterschiedlichen Facharzt- oder Schwerpunktbezeichnungen eine interdisziplinäre Versorgung aus einer Hand gewährleisten (siehe § 95 Sozialgesetzbuch V). Angelehnt an das Vorbild der früheren DDR-Polikliniken wurden sie erst 2004 im Gesundheitssystem der Bundesrepublik etabliert.

## Basis: Austausch von Patientendaten

Der Ansatz „interdisziplinäre Versorgung aus einer Hand" ist darauf angelegt, dass die beteiligten Ärzte Daten über Patienten des MVZ austauschen. Leider enthält das Sozialgesetzbuch keine konkreten Regelungen dafür, unter welchen Voraussetzungen dies möglich sein soll. Daraus entstehen in der Praxis erhebliche Unsicherheiten.

## Wann ist eine Einwilligung erforderlich?

In einer „Handreichung MVZ" versucht die Datenschutzaufsicht Hessen, die maßgeblichen Fragen zumindest ansatzweise zu klären. Im Mittelpunkt steht die Frage, wann eine Einwilligung des Patienten erforderlich ist, damit verschiedene Ärzte die personenbezogenen Daten des Patienten innerhalb des Medizinischen Versorgungszentrums weitergeben dürfen.

Bild: iStock.com/Jane_Kelly

## Patient umfassend informieren

Im Ergebnis schlägt die Handreichung eine Struktur vor, die von einer umfassenden Information des Patienten ausgeht. Darauf aufbauend hat er die Möglichkeit, Sperrvermerke hinsichtlich der Weitergabe an andere Ärzte zu bewirken. Ob MVZ diesen Ansatz als praxistauglich empfinden, bleibt abzuwarten.

Die Handreichung bildet einen Teil des Onlineauftritts der Datenschutzaufsicht Hessen und ist abrufbar unter https://ogy.de/handreichung-mvz. Die Darstellung ist nicht mit einem Datum versehen.

Neue Broschüre

# Datenverarbeitung in Inkassounternehmen

Das Misstrauen gegenüber der Verarbeitung von Daten durch Inkassounternehmen ist oft erheblich. Die Datenschutzaufsicht Nordrhein-Westfalen greift in einer Broschüre die wichtigsten Fragen hierzu auf. Die Antworten sind überwiegend kurz und knapp. Lediglich das Thema „Eintreiben von Forderungen für im Ausland begangene Straßenverkehrsverstöße" ist mit einem Umfang von zwei Seiten recht ausführlich behandelt.

## Kurze Antworten auf 16 wichtige Fragen

Die Broschüre ist auf dem Stand von März 2020 und umfasst 16 Fragen mit Antworten auf insgesamt 14 Seiten. Hinzu kommt ein Anhang von zwei Seiten. Er besteht aus dem Beschluss der Datenschutzkonferenz vom 23.3.2018 zum Thema „Einmeldung offener und unbestrittener Forderungen in eine Wirtschaftsauskunftei unter Geltung der DS-GVO". Die Broschüre ist abrufbar unter https://ogy.de/Datenverarbeitung-Inkassounternehmen.

Landesamt Bayern

# Mitteilung von Überstunden an Vorgesetzte

Es ist datenschutzrechtlich nicht zu beanstanden, wenn die Personalbuchhaltung den jeweiligen Vorgesetzten und der Geschäftsführung Mitteilungen über Überstunden von Mitarbeitern zur Verfügung stellt. Diese Auffassung vertritt das Bayerische Landesamt für Datenschutzaufsicht.

## Erforderlich, um das Beschäftigtenverhältnis durchzuführen

Seine Begründung: Der Arbeitgeber darf mit Mitarbeiterdaten umgehen, wenn dies erforderlich ist, um das Beschäftigungsverhältnis durchzuführen (§ 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG)). Dass die Personalbuchhaltung Vorgesetzten und der Geschäftsführung die Überstunden der ihnen unterstehenden Mitarbeiter mitteilt, hält das Landesamt jedenfalls für vertretbar. Denn – so sein Argument – anhand der Überstunden können die Vorgesetzten erkennen, wie stark die einzelnen Mitarbeiter belastet sind.

Nötigenfalls könnten sie Aufgaben umverteilen. Bei einer großen Zahl von Überstunden könnten die Vorgesetzten auf deren Abbau hinwirken. Gegebenenfalls könnte auch in Betracht kommen, neue Mitarbeiter für bestimmte, besonders belastete Bereiche als zusätzliche Abhilfe einzustellen.

Quelle: Bayerisches Landesamt für Datenschutzaufsicht, Tätigkeitsbericht 2019, Seite 46. Der Bericht ist abrufbar unter https://ogy.de/baylda-tb-2019.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken (Bayern). Er befasst sich seit Jahren mit Fragen des Datenschutzes in Unternehmen und Behörden.

Bild: iStock.com/karandaev

**Die Hürden, die die DSGVO in Bezug auf Geburtstagslisten bereithält, lassen sich gut beherrschen**

Datenschutzklassiker in Unternehmen & Behörden

# Geburtstagslisten und die Datenschutz-Grundverordnung

**Sind Geburtstagslisten zulässig? Und wenn ja, welche Fallstricke sind zu beachten? Diese Fragen gehören zu den Klassikern des „Alltags-Datenschutzes". Die DSGVO bereichert die Antworten um neue Aspekte.**

Geburtstage sind Gegenstand sozialer Erwartungen. So hat es der Bayerische Landesbeauftragte für den Datenschutz (BayLfD) treffend formuliert. Das gilt v.a. für „runde Geburtstage". Selbst wenn jemand nach außen behauptet, diese Dinge seien ihm nicht so wichtig – Glückwünsche von Vorgesetzten und Kolleginnen/Kollegen erwartet er in der Regel doch. Andererseits empfinden viele ihren Geburtstag als eine mehr oder weniger vertrauliche Sache. Das betrifft v.a. das Geburtsjahr. Ein gedankenloser Umgang mit Geburtstagsdaten kann deshalb eine nachhaltige Verstimmung auslösen.

## Geburtstagsliste als rein private Angelegenheit?

Vorsicht ist mit der Aussage geboten, eine bestimmte Geburtstagsliste falle überhaupt nicht in den Anwendungsbereich der DSGVO. Das ist zwar prinzipiell denkbar. Voraussetzung wäre, dass die Liste durch eine natürliche Person „zur Ausübung ausschließlich persönlicher oder familiärer Tätigkeiten" geführt wird (siehe Art. 2 Abs. 2 Buchst. c DSGVO). Das kann auch eine Person sein, die im Unternehmen arbeitet und für sich selbst eine Liste mit Geburtstagen von Kollegen führt. Sobald sie diese Informationen aber im Kollegenkreis teilt, handelt es sich nicht mehr ausschließlich um eine persönliche Tätigkeit. Im Regelfall gilt deshalb: Auch bei scheinbar privaten Listen kommt die DSGVO zur Anwendung.

## Verantwortlichen klären

Zunächst ist zu klären, wer im Hinblick auf eine konkrete Geburtstagsliste als Verantwortlicher im Sinn der DSGVO anzusehen ist. Das kann das Unternehmen sein, zwingend ist das aber nicht. Das Unternehmen ist dann als Verantwortlicher gemäß Art. 4 Nr. 7 DSGVO anzusehen, wenn

- Vorgesetzte die Liste führen oder dies veranlassen,
- Vorgesetzte auf eine Eintragung in die Liste hinwirken oder in irgendeiner Art und Weise Anreize für die Eintragung schaffen oder
- die Personalstelle die Liste mit Daten befüllt.

Diese alternativen Kriterien wendet der BayLfD an. Falls keines von ihnen erfüllt ist, gilt das Unternehmen nicht als Verantwortlicher. Dann muss es einen anderen Verantwortlichen geben. Das kann beispielweise ein Mitarbeiter sein, der eine Liste von sich aus führt.

## Ins Verzeichnis der Verarbeitungstätigkeiten aufnehmen

Offenbleiben darf die Frage der Verantwortlichkeit nicht. Wo es eine Liste gibt, existiert immer auch ein Verantwortlicher. Denn irgendjemand muss sich um die Fragen kümmern, die sich aus der DSGVO ergeben. Das gilt auch im Hinblick auf das Verzeichnis der Verarbeitungstätigkeiten:

- Falls das Unternehmen als Verantwortlicher anzusehen ist, gehört die Geburtstagsliste in dessen Verzeichnis.
- Ansonsten muss derjenige, der die Liste führt, die entsprechenden Angaben in eigener Verantwortung festhalten. Sie müssen schriftlich oder „in einem elektronischen Format" fixiert sein (so Art. 30 Abs. 3 DSGVO).

## Löschungsfrist angeben

Probleme bereitet es, eine Löschungsfrist im Verzeichnis der Verarbeitungstätigkeiten anzugeben (Art. 30 Abs. 1 Buchst. f DSGVO). Eine konkrete Frist lässt sich normalerweise nicht festlegen. Niemand weiß, wie lange jemand Mitarbeiter des Unternehmens bleibt. Auch gibt es innerhalb ei-

nes Unternehmens immer wieder Versetzungen von einer Organisationseinheit in eine andere. Die DSGVO schränkt die Pflicht zur Angabe einer Löschungsfrist jedoch ein. Eine Löschungsfrist muss nur „wenn möglich" angegeben sein.

## Pflicht zur Löschung aus der Liste

Verlässt ein Mitarbeiter die Organisationseinheit, auf die sich die Geburtstagsliste bezieht, sind seine Daten zu löschen. Ob er völlig aus dem Unternehmen ausscheidet oder nur in eine andere Organisationseinheit wechselt, spielt keine Rolle.


„Löschen" bedeutet, dass der Eintrag aus der Liste verschwinden muss. Es genügt also nicht, den Namen durchzustreichen. Vielmehr muss die Liste ohne den ausgeschiedenen Mitarbeiter neu gefasst werden. Das mag kleinlich erscheinen. Man sollte jedoch bedenken, dass ein Verstoß gegen die Pflicht zur Löschung (Art. 17 Abs. 1 Buchst. a DSGVO) zu einer Geldbuße führen kann (Art. 83 Abs. 5 Buchst. b DSGVO). Das kann sich v.a. dann als offene Flanke erweisen, wenn ein Mitarbeiter im Zorn ausgeschieden ist.

## Liste für Vorgesetzte

Oft ist die Behauptung zu hören, als Rechtsgrundlage für die Aufnahme in eine Geburtstagsliste komme nur eine Einwilligung in Betracht. Das vereinfacht die Dinge zu sehr. Es kommt darauf an, wer die Geburtstagsliste führt und wie sie konkret genutzt wird. Typischerweise erwarten Mitarbeiter von Vorgesetzten, dass sie zum Geburtstag gratulieren. Das gilt besonders für runde Geburtstage. Gerade dann sind auch Geschenke üblich. Deshalb sind Geburtstagslisten für Vorgesetzte erforderlich.

Rechtsgrundlage ist in diesen Fällen bei Privatunternehmen § 26 Abs. 1 Satz 1 Bundesdatenschutzgesetz (BDSG; „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses"). Die Liste ist für die Durchführung des Beschäftigungsverhältnisses erforderlich. Dabei muss sie

**ONLINE-TIPP**

*Die „Aktuelle Kurzinformation 26: Beschäftigten-Geburtstagslisten bei bayerischen öffentlichen Stellen" des Bayerischen Landesbeauftragten für den Datenschutz ist abrufbar unter https://ogy.de/geburtstagslisten.*

wegen „runder Geburtstage" auch das Geburtsjahr enthalten.

### Widerspruchsrecht

Selbstverständlich gibt es Einzelfälle, in denen Mitarbeiter keinerlei Glückwünsche zum Geburtstag möchten. Manchmal hat dies religiöse Hintergründe. So gibt es Glaubensgemeinschaften, die das Feiern von Geburtstagen nicht kennen oder sogar ausdrücklich ablehnen. Das rechtfertigt es jedoch nicht, Geburtstagslisten für Vorgesetzte generell als nicht erforderlich anzusehen.

Ein Betroffener kann der Datenverarbeitung jederzeit widersprechen (Widerspruchsrecht gemäß Art. 21 DSGVO). Das führt nicht dazu, dass er aus der Geburtstagsliste des Vorgesetzten zu streichen wäre. Vielmehr ist es erforderlich, dass sein Name in der Liste bleibt. Dazu gehört der Hinweis, dass er Glückwünsche ablehnt. Tag und Jahr des Geburtstags müssen entfallen. Sie sind nicht erforderlich.

## Listen für den Kollegenkreis

Für Geburtstagslisten, die innerhalb einer Organisationseinheit für die Mitarbeiter zur Verfügung stehen, gelten andere Überlegungen. „Kollegenlisten" sollen ein „anlassbezogenes Gemeinschaftserlebnis" ermöglichen, wie es der BayLfD formuliert. Seine zutreffende Schlussfolgerung: „Bei alldem handelt es sich um Akte der kollegialen Beziehungspflege, nicht aber um vom Dienstherrn zu veranlassende … Maßnahmen." Solche Listen sind daher für die Durchführung des Beschäftigungsverhältnisses nicht erforderlich. Der Begriff „Dienstherr" entspricht in Unternehmen übrigens dem des Arbeitgebers. Er kommt aus dem Beamtenrecht.

### Notwendigkeit einer Einwilligung

Rechtsgrundlage für „Kollegenlisten" kann nur eine Einwilligung sein. Die Einwilligung muss den allgemeinen Anforderungen genügen. Der Maßstab für Einwilligungen im Arbeitsverhältnis (§ 26 Abs. 2 BDSG) spielt dabei keine Rolle. Denn mit dem Arbeitsverhältnis an sich haben solche Listen nichts zu tun. Heranzuziehen sind daher die allgemeinen Maßstäbe der DSGVO, v.a. die Vorgaben von Art. 7 DSGVO.

### Anforderungen an die Einwilligung

Eine schriftliche Einwilligung ist nicht erforderlich, wohl aber muss eine „eindeutige bestätigende Handlung" vorliegen (siehe Erwägungsgrund 32 Satz 1 zur DSGVO). Das ist etwa der Fall, wenn sich die betroffene Person selbst in die Liste einträgt. „Eindeutig" ist es ebenfalls, wenn sie auf Nachfrage von Kollegen ihren Geburtstag nennt. Voraussetzung dabei: Sie muss wissen, dass es darum geht, dieses Datum in die Geburtstagsliste einzutragen.

## Informationspflicht

Die Informationspflicht gemäß Art. 13 DSGVO zu erfüllen, verursacht im Ergebnis keinen besonderen Aufwand. Für Listen, die der Arbeitgeber führt oder für die er die Daten liefert, sollte man sich folgender Argumentation des BayLfD anschließen:

- Die Aufnahme von Daten eines Beschäftigten in eine Geburtstagsliste ist als Weiterverwendung der bereits vorhandenen Beschäftigtendaten anzusehen (Fall des Art. 13 Abs. 3 DSGVO).
- Dieser Vorgang stellt für den Beschäftigten keine Überraschung dar, wenn schon die allgemeinen Datenschutzhinweise, die er zu Beginn des Beschäftigungsverhältnisses erhalten hat, Geburtstagslisten berücksichtigen.
- Damit ist er ausreichend im Bild. Eine gesonderte Information ist deshalb entbehrlich (Fall des Art. 13 Abs. 4 DSGVO).

Dr. Eugen Ehmann ist als Regierungspräsident von Unterfranken derzeit sehr aktiv in die Geschehnisse rund um Corona eingebunden. Dieser Beitrag ist glücklicherweise noch vorher entstanden.

Bild: iStock.com/scanrail

**Wie spielt was zusammen? Nur wer das weiß, kann seine Datenschutz- und IT-Organisation optimal aufstellen.**

DSB & ISB

# So arbeiten Datenschutz und Cybersicherheit zusammen

**Ereignisse wie die Corona-Pandemie zeigen, wie wichtig es ist, in der IT auf Krisen und Angriffe vorbereitet zu sein, statt hektisch reagieren zu müssen. Eine gute Grundorganisation ist dabei als Basis unabdingbar.**

Komme ich als Beraterin in Unternehmen, dann meist, weil entweder „etwas passiert ist" oder weil das Unternehmen eine Zertifizierung zu IT-Sicherheit benötigt. Und seit Mitte Januar 2020 die ersten Meldungen zu den Infektionen mit dem Corona-Virus aus China nach Europa kamen, habe ich mit den von mir betreuten Unternehmen über Pandemie-Planung gesprochen.

Zu Beginn hat das keines der Unternehmen besonders ernst genommen. Heute sieht die Lage anders aus. Wer schon vorher eine solide und transparente IT-Organisation hatte, ist derzeit klar im Vorteil. Und wer feststellen musste, dass er hier Schwachstellen hat, sollte nachbessern.

## Zwei wichtige Akteure: DSB und ISB

In den meisten Unternehmen treffe ich inzwischen auf gut ausgebildete Datenschutzbeauftragte (DSB). Und immer öfter auch auf die Rolle des Informationssicherheitsbeauftragten (ISB). Damit gibt es zwei Personen, die unterschiedliche „Brillen", d.h. jeweils eine andere Perspektive auf dasselbe Thema haben. Beide sind jedoch zuständig dafür, die Prozesse und die Organisation rund um die sichere Datenverarbeitung zu unterstützen, zu steuern, zu überprüfen und den Verantwortlichen zu beraten.

Für kleine Unternehmen ist es eine Herausforderung, beide Rollen zu besetzen. Doch auch für sie ist die Besetzung dieser beiden Rollen wichtig. Das sogenannte „Vier-Augen-Prinzip" sorgt für ein nachhaltiges IT- und Datenschutzniveau im Unternehmen. Zudem können sich diese beiden Rollen gegenseitig unterstützen mit der Zielsetzung, die Werte im Unternehmen zu schützen.

## Die Basis: Prozesse und Unternehmenskultur durchleuchten

Bei den Prozessen der Informationssicherheit und den Mechanismen der technischen IT-Sicherheit ist es wichtig, Schritt für Schritt vorzugehen. In der Regel analysiert der ISB in Zusammenarbeit mit dem DSB zunächst die vorhandenen Sicherheitsprozesse. Dann geht es darum, eine Sicherheitsorganisation und ihre Koordination zu definieren. Achten Sie darauf, dass Sie als Datenschutzbeauftragter eng in die Gestaltung der Organisation eingebunden sind.

### Zentral: Kommunikation & Führungskultur

Kümmern Sie sich rechtzeitig gemeinsam mit dem ISB um die Kommunikation innerhalb des Unternehmens. Diese Bestandteile sind intern im Alltag wichtig und erst recht nach außen im Krisenfall. Es ist sehr wichtig, dass auch die Kollegen aus der Unternehmensführung Vorbild sind und die Regelungen des Datenschutzes einhalten.

Es ist empfehlenswert, einen begleitenden Prozess zu durchlaufen, der die Führungskultur aus der Sicht von DSB und ISB

**PRAXIS-TIPP**

***Wie sieht eine solide Sicherheitsorganisation konkret und im Detail aus? Auf der Seite des Bundesamts für Informationssicherheit (BSI) finden Sie einige gute Beispiele: https://ogy.de/IS-Management-Team.***

unter die Lupe nimmt. Machen Sie Vorstand bzw. Geschäftsführer zudem klar, dass sie ihre Verantwortung besser wahrnehmen können, wenn sie Fachpersonal mit dem notwendigen Sachverstand und aktuellem Fachwissen an Bord haben.

Entscheidend ist, dass sich Datenschutzprozesse und Organisation der Informationssicherheit in der Praxis wiederfinden. Günstig ist, wenn ein Unternehmen soweit möglich die Prozesse an die gelebte Praxis anpasst – nicht umgekehrt.

### ITIL, IT-Service-Design und IT-Produkte

Doch wie gelingt es, bei den Prozessen und der Organisation konkreter zu werden? Zwei Ansätze seien kurz zur eigenen weiteren Recherche vorgestellt.

Dass ITIL einen professionellen IT-Betrieb unterstützt und transparent macht, hat sich inzwischen etabliert. Die Information Technology Infrastructure Library, abgekürzt ITIL, bietet eine Sammlung vordefinierter und für mittlere bis große IT-Infrastrukturen typischer Prozesse, Funktionen und Rollen. Diese Best-Practice-Vorschläge sind an das jeweilige Unternehmen anzupassen.

Ein weiterer Ansatz ist, dass die IT-Organisation ihre Leistungen als sogenannte IT-Services und IT-Produkte definiert. Das Ergebnis ist eine digitale Landkarte, die das Zusammenwirken der Services zeigt. So ist es möglich, die geleisteten IT-Services transparent, messbar und vergleichbar zu machen. Dabei wird pro IT-Service definiert, aus welchen Teilen – sogenannten IT-Produkten – dieser Service zusammengesetzt ist. Jedes Detail ist wichtig, um ein vollständiges Bild zu erhalten.

Gleichzeitig macht das Abhängigkeiten der IT-Services untereinander sichtbar, etwa wenn ein Sicherheitsupdate einer Komponente erforderlich ist. In diesem Fall ist zu prüfen, wie die angrenzenden Systeme und Komponenten auf das Update reagieren. Mit dieser Grundlage lässt sich z.B. ein geordnetes Patchmanagement leichter organisieren.

**Präventions- und Notfall-Team**

## Schaltzentrale: das Cyber-Defense-Team

Das Cyber-Defense-Team ist eine Schaltzentrale der Verteidigung und für Krisen. Es benötigt Weisungsbefugnisse über die klassische Linienorganisation hinaus. Dabei sind DSB und ISB Teil dieses Teams. Sollte es notwendig sein, Server oder Systeme vom Netz zu nehmen oder Laptops und Desktops wegen Schadware-Befall einzuziehen, muss das Cyber-Defense-Team sofort handlungsfähig sein. Darüber hinaus ist ratsam, dieses Team zusätzlich als internes Präventionsteam auf- und auszubauen. Es trägt erfahrungsgemäß sehr gut dazu bei, die Prozesse und umzusetzenden Maßnahmen im Unternehmen nachzuhalten und zu begleiten. Außerdem ist das Team auf diese Weise während der Phasen ohne Krisen- und Sicherheitsvorfälle aktiv und eingespielt. Wichtig ist, dass DSB, ISB und das Team laufend Hand in Hand arbeiten und dass alle Präventionsmaßnahmen in den technischen und organisatorischen Maßnahmen dokumentiert sind.


Damit ergibt sich zudem eine solide Basis, um die technischen und organisatorischen Maßnahmen umfassend zu beschreiben.

### Neue Methoden anwenden: Agilität im Unternehmen

Agile Methoden leisten gute Dienste, insbesondere bei Cyber-Defense-Teams und bei der Organisation von Datenschutz- und Informationssicherheits-Themen. Agile Methoden empfehlen sich im Unternehmen immer dann, wenn sehr komplexe Sachlagen vorhanden und viele Faktoren unklar sind. Die Wurzeln der agilen Methoden liegen in der sogenannten Lean-Bewegung, die aus Japans Autoindustrie in den Westen kam.

Bei den agilen Methoden sind besonders Scrum oder Kanban geeignet, um zu starten.

## Für Notfälle stets einsatzbereit

Argumentieren Sie gegenüber der Geschäftsleitung, dass sie sich das vorstellen muss wie bei der Feuerwehr. Jede Stadt und jede Gemeinde finanziert die Feuerwehr. Die Kolleginnen und Kollegen, die dort im Einsatz sind, sind gut ausgebildet, regelmäßig trainiert und gut ausgestattet mit technischem Material. Das kostet Geld. Oft stehen keine akuten Einsätze an. Doch wenn einmal ein Haus oder Unternehmensgebäude brennt, kommt die Feuerwehr und löscht den Brand. Sie verhindert, dass sich das Feuer ausbreitet, rettet Menschenleben und sorgt dafür, dass der Schaden möglichst gering ist.

So sollte das auch in jedem Unternehmen sein. Falls es einer Cyber-Attacke ausgesetzt ist oder einer anderen Krisensituation, muss es in der Lage sein, das „virtuelle Feuer" so schnell wie möglich zu löschen.

- Dazu ist zum einen eine Technik nötig, die zum Unternehmen passt und gut eingesetzt ist. Voraussetzung dafür ist, einen Überblick zu haben, was überhaupt vorhanden ist und wie alles zusammenspielt.
- Außerdem sind Training und Weiterbildung wichtig, um im Fall des Falls professionell reagieren zu können.

Idealerweise stehen Sie in einer Krisensituation nicht da und diskutieren, wer jetzt was macht. Das muss vorher klar sein!

Christine Deger arbeitet seit 18 Jahren in der IT-Branche, die meiste Zeit intensiv mit dem Thema Cybersicherheit befasst. Seit 2017 hat sie ihr eigenes Unternehmen changeboxx (https://changeboxx.de/), das Betriebe rund um die Themen Cybersecurity und agile Methoden berät.

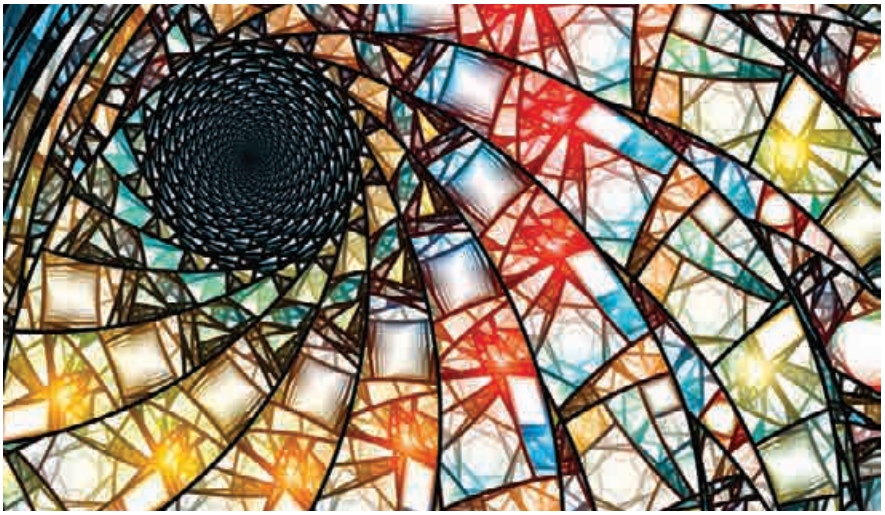


Bild: iStock.com/sakkmesterke

**Die DSGVO besteht aus insgesamt 99 Artikeln und das KDG aus lediglich 58 Paragrafen. Das erklärt sich aus den unterschiedlichen Anwendungsgebieten.**

Kirchlicher Datenschutz

# Berührungspunkte zwischen DSGVO und KDG

**Die DSGVO verwenden die meisten Menschen in Europa als Synonym für Datenschutz. Doch es gibt u.a. in den großen Kirchen Deutschlands eigene, autonome Datenschutzgesetze.**

Bereits einen Tag vor dem 25. Mai 2018 trat für die Diözesen Deutschlands ein neues Datenschutzgesetz in Kraft: das Gesetz über den Kirchlichen Datenschutz, kurz KDG.

## Warum ein Spezialgesetz?

Art. 91 Abs. 1 Datenschutz-Grundverordnung (DSGVO) räumt Kirchen und religiösen Vereinigungen das Recht ein, eigene Regeln anzuwenden. Voraussetzung: Es existieren zum Zeitpunkt des Inkrafttretens der DSGVO umfassende Regeln zum Schutz natürlicher Personen bei der Verarbeitung, und diese Regeln wurden mit der DSGVO in Einklang gebracht. Die katholische Kirche in Deutschland hat aufgrund dessen ihre bestehende Verordnung angepasst und zum 24. Mai 2018 in Kraft gesetzt.

Dieses Gesetz sowie alle Gesetze von anderen Kirchen, religiösen Vereinigungen und Gemeinschaften, die sich aus Art. 91 DSGVO ergeben, sind autonome Gesetze. Sie fügen sich daher nicht in die Hierarchie von Europa, Bund und Ländern ein.

Neben der katholischen Kirche haben u.a. auch die evangelische Kirche und die Ordensgemeinschaft päpstlichen Rechts dieses Recht in Anspruch genommen.

## Kurzer geschichtlicher Exkurs

Aber warum räumt die DSGVO den Kirchen eigentlich das Recht ein, eigene Regeln zu verfassen und sie dann auch noch unabhängig von der DSGVO anzuwenden?

Das Ganze ist begründet im „kirchlichen Selbstbestimmungsrecht" bzw. in der „Kirchenfreiheit". Sie findet sich erstmals in einem Satz der Paulskirchenverfassung aus dem Jahr 1849. Viele der darauffolgenden Verfassungen enthalten ebenfalls diesen Satz so oder so ähnlich. Zuletzt Artikel 137 der Weimarer Verfassung von 1919, der heute in Artikel 140 des Grundgesetzes zum geltenden Recht gehört.

Die Geschichte des Datenschutzes in der katholischen Kirche beginnt mit dem Beichtgeheimnis, das seit 1215 Bestandteil des Kirchenrechts ist.

Kurz nachdem in Deutschland in den 1970er-Jahren das erste Bundesdatenschutzgesetz in Kraft trat, verabschiedete auch die katholische Kirche die Anordnung über den kirchlichen Datenschutz, kurz KDO. Die KDO wurde in regelmäßigen Abständen angepasst, wenn sich im Bereich der staatlichen Regelungen etwas veränderte. Schließlich wurde dann 2017 aus der „Anordnung" das „Gesetz", das sich an der DSGVO orientiert. Die Kirche hat somit immer dafür gesorgt, dass das geltende Recht auch in ihrem Bereich zur Anwendung kommt.

## Unterschiede und Überschneidungen

Wo unterschieden sich nun DSGVO und KDG? Gibt es auch Überschneidungen?

### Viele Inhalte sind gleich

Grundlegend besagt Art. 91 DSGVO, dass bestehende Regelungen mit der DSGVO in Einklang zu bringen sind. Daher ist der allgemeine Spielraum eher begrenzt. Legt man die Gesetzestexte nebeneinander, fällt auf, dass das KDG viele Inhalte wortgleich übernommen hat. Einige Abschnitte unterscheiden sich in Umfang und Wortwahl. Das ist auf den unterschiedlichen Anwendungsbereich zurückzuführen und macht in der Praxis keinen allzu großen Unterschied.

### Übergangsbestimmungen

Da der Beschluss zum KDG erst verhältnismäßig spät erlassen wurde, nämlich gut eineinhalb Jahre nachdem die DSGVO verabschiedet wurde, enthält das KDG Übergangsbestimmungen. Zum einen hatten die betroffenen Einrichtungen bis Ende 2018 Zeit, bestehende Verträge

zur Auftragsverarbeitung anzupassen. Und erst zum Ende des zweiten Quartals 2019 musste ein Verzeichnis von Verarbeitungstätigkeiten vorliegen.

### Aufsichtsbehörden

Wer seine Rechte vor einer Aufsichtsbehörde geltend machen möchte, kann sich im kirchlichen Bereich an eine von fünf Aufsichtsbehörden, sogenannte katholische Datenschutzzentren, wenden. Sie sind über ganz Deutschland verteilt und richten sich nach den Grenzen der Diözesen.

### Datengeheimnis

Anders als in der DSGVO hat das Datengeheimnis im KDG einen eigenen Absatz. Die Verpflichtung ist in schriftlicher Form vorzunehmen. Auch Einwilligungen sind in Schriftform abzugeben. Diese Hinweise allein auf die Schriftform finden sich weder in der DSGVO noch im BDSG.

Alles in allem sind die Unterschiede überschaubar. In der Praxis sollte man sich trotzdem der Tatsache bewusst sein, dass kirchliche Einrichtungen unter einem anderen Datenschutzgesetz stehen. Das ist v.a. dann wichtig, wenn weltliche Stellen mit kirchlichen zusammenarbeiten, etwa bei der Auftragsverarbeitung.

## Was ist für die Praxis wichtig?

Den größten Einfluss haben diese Unterschiede auf den Austausch von Dienstleistungen. Das gilt unabhängig davon, ob die kirchliche Stelle Auftragnehmer oder Auftraggeber ist.

### Auftragsverarbeitung

Das Stichwort hierbei ist die Auftragsverarbeitung. Viele Produktionen und Dienstleistungen, die über Maßnahmen zur Teilhabe am Arbeitsleben unterstützt werden und in denen Menschen mit Einschränkungen arbeiten, befinden sich in kirchlicher Hand. Bei einer Zusammenarbeit müssen die Verträge immer sowohl die DSGVO als auch das KDG berücksichtigen. Klassische Beispiele hierfür sind der Versand von personalisierten Grußkarten oder die Aktenvernichtung.

**PRAXIS-TIPP**

***Erbringt ein Unternehmen Dienstleistungen für kirchliche Einrichtungen, z.B. IT-Leistungen oder die Personal- bzw. Buchhaltung, wird der Vertrag zur Auftragsdatenverarbeitung einen Passus enthalten, der den Auftragnehmer dazu anhält, die von ihm eingesetzten Mitarbeiter auf das Datengeheimnis zu verpflichten. Denn so fordert es das KDG.***

### Datenschutzbeauftragter

Wer in einer kirchlichen Einrichtung Datenschutzbeauftragter werden möchte, muss einen separaten Fachkundenachweis ablegen. Denn da das KDG ein autonomes Gesetz ist, ist die DSGVO-Fachkunde nur ein Teil des nötigen Wissens.

### Kirchenblätter

Nicht nur im Arbeitsalltag kann es Berührungspunkte geben, sondern auch im privaten Umfeld. Das gilt z.B. für Veröffentlichungen im Kirchenblatt bei der Erstkommunion, bei Eheschließungen und Taufen. Wer in der Heimatgemeinde aktiv ist, wird vielleicht mitbekommen haben, dass sich dort etwas in Sachen Datenschutz getan hat.

Mindestens einmal jährlich veröffentlichen die Kirchblätter eine Widerspruchserklärung. Sie weist die Bürger darauf hin, dass sie den oben genannten Veröffentlichungen und Bekanntgaben zu Jubiläen jederzeit widersprechen können. Diesen Widerspruch müssen sie schriftlich oder in sonstiger geeigneter Form bei der zuständigen Pfarrei oder bei der Meldestelle des Bistums einreichen. Für Veröffentlichungen, die außerhalb der kircheneigenen Medien stattfinden sollen, müssen die Gemeinden, Diözesen etc. die Einwilligungserklärungen bei den betroffenen Personen einholen.

Nathalie Jung war Datenschutzbeauftragte für einen großen deutschen Diözesancaritasverband und seine angeschlossenen Orts- und Fachverbände.

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, Werner Pehland

**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)

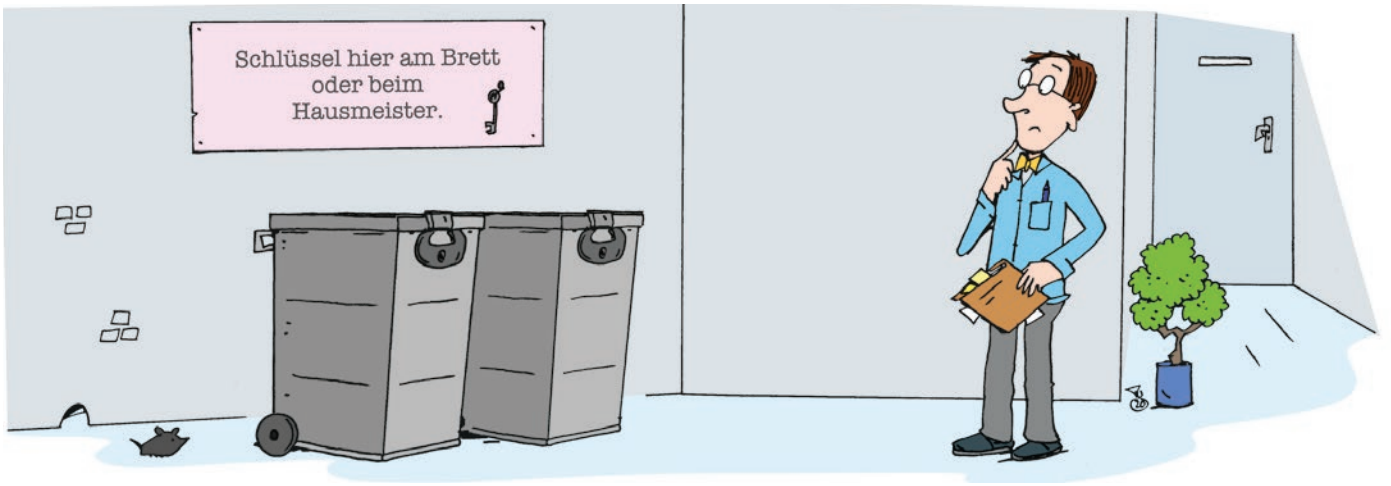
**Druck:**
Geiselmann Printkommunikation GmbH
Leonhardstraße 23, 88471 Laupheim

**Layout & Satz:**
metamedien
Spitzstraße 31, 89331 Burgau

**Bestell-Nr.:**
09100-4076

**ISSN-Nr.:**
1614-6867

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




Datenträger sicher entsorgen

# Verlässlich verschlossen!?

**Datentonnen sind dazu da, Datenträger wie Papier sicher zu entsorgen. Damit das datenschutzkonform klappt, sind allerdings einige Voraussetzungen zu erfüllen.**

Die Idee hinter den Datentonnen: Die Tonnen stehen an zentralen Stellen im Unternehmen oder in der Behörde. Im Idealfall so, dass jeder, der den Bereich oder das Unternehmen verlässt, daran vorbeikommt. Auf diese Weise können die Beschäftigten Papier mit personenbezogenen Daten, das nicht für den Papierkorb bestimmt ist, dort entsorgen.

## Sicher verschlossene Tonnen

Die Tonnen sind sicher verschlossen. Sind sie voll, kommt der beauftragte Dienstleister und entsorgt den Inhalt datenschutzkonform. Das spart Schredder und ist insgesamt eine praktische Sache. Voraussetzung ist allerdings, dass die Tonne bis zur Leerung verlässlich verschlossen ist. Da die meisten Datentonnen ein Schloss haben, treffen Verantwortliche mit dem Dienstleister am besten die Vereinbarung, dass kein Schlüssel im Betrieb verbleibt. Sicher ist sicher.

## Warum hat der Hausmeister einen Schlüssel?

Eines Tages beobachtet der Datenschutzbeauftragte, wie sich der neue Hausmeister über eine Datentonne beugt und sie – aufschließt! Wie kann das bitte sein? Der Datenschutzbeauftragte ist neugierig. „Wo haben Sie den Schlüssel her?", will er wissen. „Den hat mir mein Vorgänger gegeben!", so die Antwort.

Man stellt ausgiebige Nachforschungen an. Der Vorgänger des neuen Hausmeisters, auf den Schlüssel angesprochen, verweist auf eine wichtige Person: „Ich habe den Schlüssel für die Datentonnen vom Assistenten des Vorstands!" Und woher hatte der ihn?

## Der Vorstand war's

Des Rätsels Lösung: Der Vorstand hatte selbst Unterlagen entsorgt, da sonst niemand mehr da war. Dabei kam versehentlich eine wichtige Unterlage in die Datentonne, die nicht vernichtet werden durfte.

Der Assistent wurde zum 30 Kilometer entfernten Dienstleister geschickt, holte dort mit Unterschrift des Vorstands den Schlüssel ab und öffnete die Tonne. Dann gab er den Schlüssel dem Hausmeister. Und der? Einen Schlüssel, der nun schon einmal da ist, gibt man doch nicht mehr her – man kann ja nie wissen!

Eberhard Häcker ist externer Datenschutzbeauftragter. Sein Credo: Wer in einem Unternehmen regelmäßig unterwegs ist, sieht mehr Schwachstellen, die sich in der Praxis eingeschlichen haben, als andere.

**IN DER NÄCHSTEN AUSGABE**

### Was tun gegen Trojaner (2)?

Cyberkriminelle scheuen sich nicht, Corona als Köder zu nutzen. Lesen Sie daher, welche technischen Maßnahmen wirken.

### Anfragen der Aufsichten

Meldet sich eine Aufsichtsbehörde bei Ihnen, müssen Sie die DSGVO-Regelungen kennen, um Stolperfallen zu vermeiden.

### Cookie-Banner – überall nötig?

Es ist kein Hexenwerk, zu entscheiden, ob ein Cookie-Banner nötig ist, und wenn ja, wie man ihn rechtskonform gestaltet.