www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT | Juli 2020

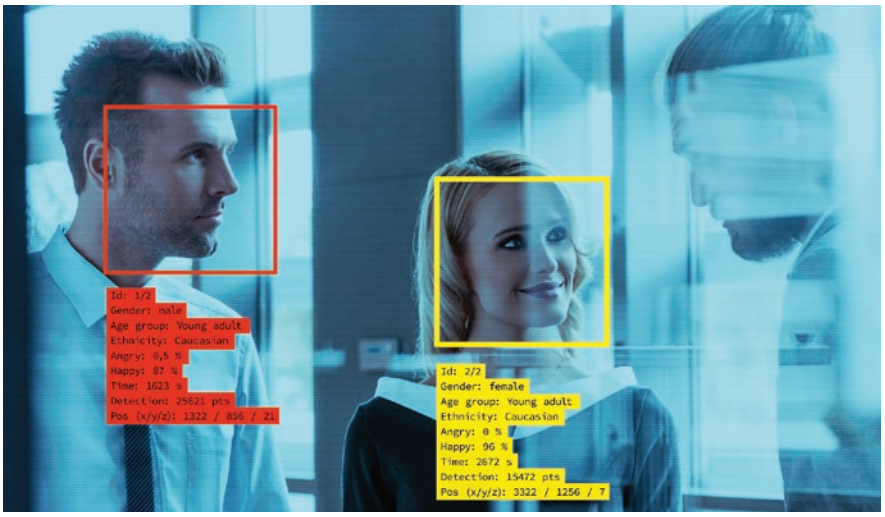


Bild: iStock.com/izusek

Verstößt eine Verarbeitung personenbezogener Daten gegen die DSGVO, kann eine Aufsichtsbehörde diese Verarbeitung sogar komplett untersagen

Mehr als Geldbußen

Die Abhilfebefugnisse der Aufsichtsbehörden

Geht es um Sanktionen der Aufsichtsbehörden, gilt meist der erste Gedanke den Geldbußen. Doch es gibt weit mehr Möglichkeiten, wie eine Aufsichtsbehörde gegen Verantwortliche vorgehen kann.

Auch wenn die zunächst befürchtete Abmahnwelle weitgehend ausblieb, ist eines sicher, seit die Datenschutz-Grundverordnung (DSGVO) anwendbar ist: Jeder, der – sei es privat oder öffentlich – personenbezogene Daten verarbeitet, tut gut daran, die datenschutzrechtlichen Vorgaben zu beachten. Das gilt allein schon wegen des immens erhöhten Bußgeldrahmens und der vielfältigen Befugnisse der Datenschutzaufsichtsbehörden.

Der europäische Gesetzgeber formuliert ausdrücklich, dass Sanktionen „wirksam, verhältnismäßig und abschreckend" sein müssen. Nach Art. 83 DSGVO können die Aufsichtsbehörden bei schweren Verstößen Geldbußen von bis zu 20 Millionen Euro bzw. vier Prozent des Jahresumsatzes verhängen. Es gibt jedoch auch zahlreiche andere Maßnahmen, mit denen Betroffene konfrontiert werden können. Der Datenschutz in Europa ist damit zu einem scharfen Schwert geworden.

Die Aufgaben der Aufsichtsbehörden im Überblick

Wer sich den Befugnissen der Datenschutzaufsichtsbehörden widmet, muss zunächst Klarheit darüber haben, welche Aufgaben die Aufsichten erfüllen sollen. Art. 57 DSGVO regelt detailliert, welche Aufgaben den Datenschutzaufsichtsbehörden obliegen.

Allein Art. 57 Abs. 1 DSGVO enthält 22 Aufgaben. Es lohnt sich für alle Verantwortlichen und Auftragsverarbeiter, diese Liste im Einzelnen durchzugehen. Im Wesentlichen betreffen die Aufgaben die folgenden Punkte:

- die Anwendung der Datenschutz-Grundverordnung zu überwachen und durchzusetzen
- Anfragen und Beschwerden von betroffenen Personen zu bearbeiten →

Editorial

Ricarda Veidt, Chefredakteurin

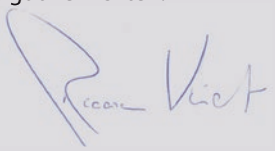
Ein Trauerspiel

Liebe Leserin, lieber Leser! Letztens war ich endlich wieder in einem Biergarten, halleluja! Und war ganz gespannt, wie der Betreiber das Thema „Erhebung von Gästedaten" umgesetzt hatte. Leider bot sich mir ein Bild, das wohl einem sehr verbreiteten Vorgehen entspricht: ein einziger Zettel am Eingang, darauf alle Daten der Vorgänger. „Bewacht" wurde die Liste nicht, jeder hätte sie mitnehmen oder abfotografieren können.

Na prima, gleich wieder kehrt machen? Sich selbst nicht eintragen (hat ja eh niemand überprüft)? Den Biergartenbetreiber freundlich darauf hinweisen, dass es da bessere Lösungen gibt? Diverse Hinweise ließen mir das jedoch nicht ratsam erscheinen, wenn wir wirklich etwas zu essen und zu trinken haben wollten ...

Immerhin, bei aller Unterschiedlichkeit der Corona-Regelungen in den einzelnen Bundesländern: Gemeinsamkeiten gibt es doch – allerorten liegen die Listen mit den Gästedaten offen herum. Auf diese Ahnungslosigkeit oder einfach Gleichgültigkeit dem Datenschutz gegenüber könnte ich allerdings gut verzichten.

Bleiben Sie gesund!
Ihre Ricarda Veidt



- Unternehmen für den Datenschutz zu sensibilisieren
- Untersuchungen über die Anwendung der Vorschriften durchzuführen

Die DSGVO adressiert ganz ausdrücklich eine Vielzahl von Interessengruppen, für die die Datenschutzaufsichtsbehörden die genannten Aufgaben wahrnehmen sollen. Dazu gehören:

- die Öffentlichkeit (Art. 57 Abs. 1 Buchst. b)
- alle betroffenen Personen und Beratungssuchenden (Art. 57 Abs. 1 Buchst. d, e, f, l)
- nationale Parlamente, Regierungen und andere Einrichtungen und Gremien (Art. 57 Abs. 1 Buchst. c)
- andere Aufsichtsbehörden (Art. 57 Abs. 1 Buchst. g)
- alle Verantwortlichen und Auftragsverarbeiter (Art. 57 Abs. 1 Buchst. d)

Die Aufsichtsbehörden sind sogar angehalten, maßgebliche Entwicklungen in der schnelllebigen Wirtschafts- und Digitalwelt zu verfolgen. Das betrifft etwa Informations- und Kommunikationstechnologien und neue Geschäftspraktiken (Art. 57 Abs. 1 Buchst. i).

Die Befugnisse der Aufsichtsbehörden im Überblick

Gerade die scharfen Geldbußen von Art. 83 DSGVO und die Befugnisse der Datenschutzaufsichtsbehörden haben das Datenschutzrecht zu einem der wichtigsten betrieblichen Compliance-Themen aufgewertet. So sehr der Fokus auch darauf gerichtet sein mag, Geldbußen zu verhindern: Es geht nicht nur um die enorme Durchsetzungskraft der Datenschutzaufsichtsbehörden und ihrer Sanktionen.

Artikel 58 DSGVO sieht insgesamt 26 Einzelbefugnisse vor, die kumulativ nebeneinander bestehen. Sie schließen sich also nicht gegenseitig aus, sondern können allesamt zum Einsatz kommen. Sie sollen die Aufsichtsbehörden in die Lage versetzen, ihre gesetzlichen Aufgaben gemäß Art. 57 DSGVO zu erfüllen. Es ist für alle Verantwortlichen und Auftragsverarbeiter unbedingt zu empfehlen, sich die Systematik der Sanktionen und aufsichtsbehördlichen Befugnisse klar zu machen.

Zu den Befugnissen der Aufsichtsbehörden gemäß Art. 58 DSGVO gehören

- Untersuchungsbefugnisse (Abs. 1),
- Abhilfebefugnisse (Abs. 2),
- Genehmigungs- und Beratungsbefugnisse (Abs. 3) sowie
- Klagerecht bzw. Anzeigebefugnis (Abs. 4).

Während die Genehmigungs- und Beratungsbefugnisse eher präventive Maßnahmen vorsehen, setzt die Ausübung von Abhilfebefugnissen nach Abs. 2 voraus, dass ein Datenschutzverstoß vorliegt oder bevorsteht. Ihre Untersuchungsbefugnisse können Aufsichtsbehörden demgegenüber unabhängig vom Anlass ausüben, da sie dazu dienen, einen Datenschutzverstoß zu ermitteln.

Diese Befugnisse kommen grundsätzlich sowohl gegenüber Unternehmen als auch gegenüber Behörden und anderen öffentlichen Stellen zur Anwendung. Selbst wenn also nach § 43 Abs. 3 Bundesdatenschutzgesetz öffentliche Stellen von Geldbußen ausgenommen sind, können sie Gegenstand der anderen Befugnisse werden.

Die Abhilfebefugnisse im Detail (Art. 58 Abs. 2 DSGVO)

Im Folgenden seien die Abhilfebefugnisse der Datenschutz-Aufsichtsbehörden gemäß Art. 58 Abs. 2 DSGVO beleuchtet. Neben der Befugnis, Geldbußen wegen Verstößen gegen die DSGVO zu verhängen (Art. 58 Abs. 2 Buchst. i in Verbindung mit Art. 83 DSGVO), zählen zu den Abhilfebefugnissen weitreichende Befugnisse, die gravierende Konsequenzen in Form von Abhilfemaßnahmen haben können. Sie sollen es den Behörden ermöglichen, rechtmäßige Zustände herzustellen.

1. Warnung (Buchst. a)

Die Datenschutz-Aufsichtsbehörde kann einen Verantwortlichen bzw. einen Auftragsverarbeiter warnen, wenn sie in der Datenverarbeitung voraussichtlich einen Verstoß gegen die DSGVO sieht. Im Gegensatz zu den sonstigen Befugnissen von Art. 58 Abs. 2 DSGVO handelt es sich bei der Warnung um eine präventive Maßnahme. Sie erfolgt zu einem Zeitpunkt, zu dem die Datenverarbeitung noch nicht stattgefunden hat.

BEISPIEL

Ein Verantwortlicher kann sich an die Datenschutzbehörde wenden, wenn er Zweifel an der Rechtmäßigkeit einer geplanten Verarbeitung hat. Die Behörde gibt dann eine Prognose ab, die auf einer summarischen Prüfung der Sach- und Rechtslage beruht. Insoweit entspricht die Warnung einem strengen Hinweis des Schiedsrichters.

2. Verwarnung (Buchst. b)

Die Verwarnung ist dagegen schon eine datenschutzrechtliche „Gelbe Karte". Die Aufsichtsbehörde kann verwarnen, wenn eine Daten verarbeitende Stelle gegen die DSGVO verstoßen hat. Die Verwarnung beschränkt sich allerdings lediglich darauf, den Verstoß objektiv festzustellen. Aussagen über subjektive Merkmale bei den handelnden Personen und die Vorwerfbarkeit sind mit der Verwarnung nicht verbunden.

3. Anweisung (Buchst. c)

Die Aufsichtsbehörde kann die Daten verarbeitende Stelle zudem anweisen, den Anträgen von Betroffenen zu entsprechen. Damit sind v.a. Anträge auf Auskunft gemäß den ersten beiden Abschnitten des Kapitels 3 der DSGVO gemeint (vgl. Art. 12 Abs. 1 Satz 2, Abs. 3 Satz 1, Art. 15 Abs. 1, Abs. 2 und 3 DSGVO). In Bezug auf die Antragsrechte von betroffenen Personen im Bereich der Berichtigung und Löschung enthält Art. 58 Abs. 2 Buchst. g eine speziellere Vorschrift.

4. Allgemeine Anordnungsbefugnis (Buchst. d)

Zu den wichtigsten Befugnissen der Datenschutz-Aufsichtsbehörden zählt die allgemeine Anordnungsbefugnis. Danach kann die Aufsichtsbehörde anordnen, dass der Verantwortliche bzw. der Auftragsverarbeiter seine Datenverarbeitungsvorgänge mit der DSGVO in Einklang bringen muss.

Diese Befugnis bezieht sich nicht darauf, eine bestimmte Vorschrift durchzusetzen. Es geht vielmehr um die Anordnung, dass die datenverarbeitende Stelle ihre Verarbeitungsprozesse mit jeder Vorschrift der DSGVO in Einklang bringt, also mit allen rechtlichen, technischen und organisatorischen Vorschriften. So kann die Behörde etwa anordnen, dass ein Arzt eine Überwachungskamera in seiner Praxis so ausrichten muss, dass sie keine Bereiche abdeckt, die Besuchern während der allgemeinen Öffnungszeiten offen stehen.

Zur Umsetzung kann die Aufsichtsbehörde bestimmte Fristen setzen und auch vorgeben, welche Maßnahmen ein Unternehmen oder eine öffentliche Stelle konkret zu treffen hat. Letzteres kann aus Gründen der Bestimmtheit auch geboten sein. Bei mehreren gleich geeigneten Mitteln muss die Behörde dem Adressaten aus Gründen der Verhältnismäßigkeit die Wahl lassen, wie er seine Datenverarbeitung rechtskonform gestaltet. →

5. Beschränkung oder Verbot der Verarbeitung (Buchst. f)

Den Verhältnismäßigkeitsgrundsatz müssen die Datenschutzaufsichtsbehörden insbesondere bei der Befugnis beachten, eine Verarbeitung zu beschränken oder zu verbieten.

- Die Behörde hat zunächst zu prüfen, ob eine Beschränkung der Verarbeitung ausreicht, damit der Verantwortliche den Verarbeitungsvorgang insgesamt rechtmäßig fortsetzen kann. Beispiel: Er verzichtet darauf, bestimmte personenbezogene Daten zu erheben.
- Sollte dies nicht der Fall sein, berechtigt Art. 58 Abs. 2 Buchst. f DSGVO die Aufsicht auch dazu, die Verarbeitung komplett zu untersagen.

Insoweit ist nicht erforderlich, dass ein besonders schwerwiegender Verstoß vorliegt. Allerdings kann die Behörde aus Gründen der Verhältnismäßigkeit ein Verbot nur als Ultima Ratio verhängen, wenn also andere, weniger einschneidende Maßnahmen keinen Erfolg versprechen.

6. Berichtigung und Löschung bestimmter Daten sowie Einschränkung von deren Verarbeitung (Buchst. g)

Darüber hinaus können die Datenschutzaufsichtsbehörden die Berichtigung und Löschung bestimmter Daten sowie eine Einschränkung der Verarbeitung solcher Daten anordnen. Und zwar unabhängig von einem Antrag der betroffenen Person. Die Behörde kann ferner anordnen, die Empfänger personenbezogener Daten im Sinne von Art. 17 Abs. 2 und Art. 19 DSGVO zu unterrichten.

7. Spezielle Anordnungsbefugnisse (Buchst. h–j)

Artikel 58 Abs. 2 Buchst. h bis j enthalten spezielle Anordnungsbefugnisse. Buchst. h regelt die Besonderheit, dass die Aufsichtsbehörde eine Anordnung nicht nur an den Verantwortlichen oder Auftragsverarbeiter, sondern an die Zertifizierungsstelle gemäß Art. 43 DSGVO richten kann. Die Behörde kann die Zertifizierungsstelle anweisen, erteilte Zertifizierungen zu widerrufen oder keine neuen Zertifizierungen zu erteilen, falls die Voraussetzungen dafür nicht oder nicht mehr vorliegen.

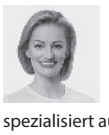
Buchst. i betrifft die Befugnisse der Aufsichtsbehörden, Bußgelder gemäß Art. 83 DSGVO zu verhängen. Nach Buchst. g können Datentransfers in Drittstaaten und an internationale Organisationen nach Kapitel V ausgesetzt werden.

Aber mit den vorgestellten Einzelmaßnahmen ist es nicht getan. Die Datenschutzaufsichtsbehörden können mehrere der genannten Maßnahmen kombinieren und hintereinander gestaffelt anwenden. Darauf müssen sich Verantwortliche und Auftragsverarbeiter einrichten.

Fazit und Ausblick

Das Schwert des Europäischen Datenschutzes hat sich als scharf erwiesen. Die Ahndung von Verstößen hat deutlich zugenommen, ebenso die Höhe der Bußgelder. Wer unter die weiten Begriffe von Art. 4 DSGVO fällt, muss den Datenschutz und die mit ihm zusammenhängende Compliance sehr ernst nehmen. Das betrifft v.a. in Unternehmen fast sämtliche Bereiche, von der Dokumentation über die Prozesse, das Marketing und die Webseite bis hin zum Arbeitsrecht.

Datenschutz-Compliance ist zudem in Anbetracht der weitreichenden Befugnisse der Datenschutzaufsichtsbehörden, speziell der Abhilfebefugnisse gemäß Art. 58 Abs. 2 DSGVO, von zentraler Bedeutung. Und das muss sich dann auch der öffentliche Bereich vor Augen halten.



Dr. Sabine Stetter, Fachanwältin für Strafrecht und Fachanwältin für Steuerrecht, leitet die von ihr gegründete Kanzlei stetter Rechtsanwälte. Die Kanzlei ist spezialisiert auf Wirtschaftsstrafrecht. Spezialgebiete umfassen u.a. internationale Verfahren und die Verteidigung gegen Unternehmensgeldbußen.

Die Effektivität entscheidet

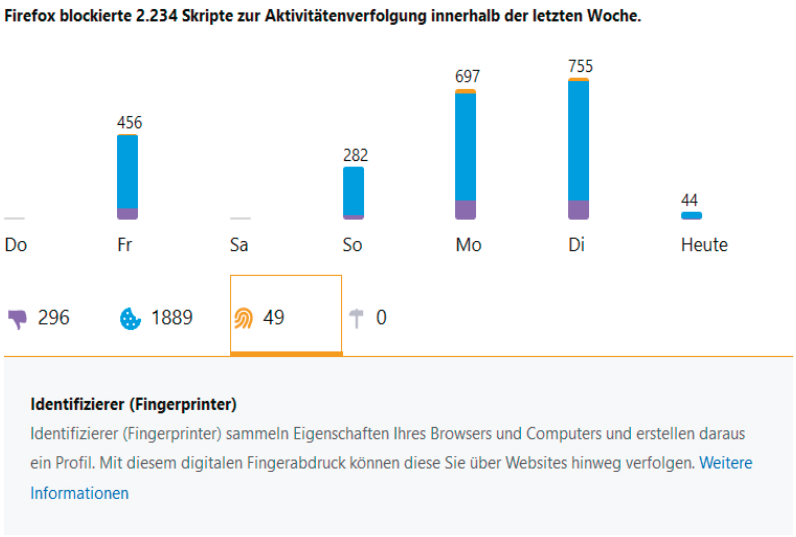
Keine Reihenfolge vorgegeben

Bei der Systematik von Art. 58 Abs. 2 DSGVO könnte man meinen, der Gesetzgeber habe die Intensität der Maßnahmen allmählich gesteigert:

- Der Katalog beginnt mit einer eingriffsschwachen Warnung in Bezug auf voraussichtliche Verstöße (Art. 58 Abs. 2 Buchst. a).
- Und er endet mit der endgültigen Untersagung der Datenverarbeitung (Art. 58 Abs. 2 Buchst. f).

Doch das täuscht. Eine Rangfolge der Befugnisse ist damit nicht verbunden. Die Datenschutzaufsichtsbehörde ist nicht etwa verpflichtet, stets den gesamten Katalog beginnend mit der mildesten Maßnahme abzuarbeiten. Entscheidend ist allein die Effektivität des Vorgehens. Die Datenschutzaufsichtsbehörden verfügen im Rahmen des Grundsatzes der Verhältnismäßigkeit über ein Ermessen, in welchem Verfahrensstadium sie welche Maßnahmen ergreifen.

Das bedeutet, dass die Aufsichtsbehörde beispielsweise nicht gehalten ist, zunächst weniger eingriffsintensive Anordnungen zu treffen, etwa eine Verwarnung, bevor sie eine Beschränkung der Verarbeitung verhängt. Sie ist jedoch verpflichtet, in jedem Einzelfall zu prüfen, ob die jeweilige Maßnahme erforderlich und verhältnismäßig ist und ob sie dabei insbesondere mildere Eingriffsmittel anwenden müsste. Das betont Erwägungsgrund 129 zur DSGVO.



Screenshot: O. Schonschek

Device Fingerprinting ist eine mögliche Alternative zu Cookies: Der Gerätefingerabdruck macht sich zunutze, dass ein Browser auf jedem Endgerät individuell konfiguriert ist.

Alternative Cookies

Was nach den Third-Party-Cookies kommt

Verschiedene Webbrowser werden in Zukunft Drittanbieter-Cookies nicht nur blockieren, sondern die Unterstützung komplett einstellen. Die Werbeindustrie sucht nun Alternativen. Für den Datenschutz ist es wichtig, dass alternative Cookies ihn nicht unterwandern.

Immer mehr Browser – nach Safari auch Firefox und Chrome – planen, zukünftig keine Third-Party-Cookies mehr zuzulassen. Von Fristen wie „innerhalb der nächsten zwei Jahre" ist die Rede, so der Bundesverband Digitale Wirtschaft (BVDW). Im Online-Marketing herrscht deshalb Unsicherheit. Denn die Third-Party-Cookies haben eine große Bedeutung für die Werbewirtschaft.

Was sind Third-Party-Cookies?

Third-Party-Cookies werden nicht von der Website platziert, auf der man sich als Besucher befindet, sondern von Dritten. Beispielsweise kann die besuchte Website eine Partnerschaft mit einem Werbenetzwerk haben. Oder der Betreiber der Website arbeitet mit einem Analyseunternehmen zusammen, das Daten sammelt und auswertet. Diese Drittanbieter können bisher Cookies über Browser platzieren. Das Problem für den Datenschutz: Im Laufe der Zeit entwickeln die Drittanbieter möglicherweise eine detaillierte Historie derjenigen Websites, die ein Besucher häufig ansteuert.

Im Gegensatz zu den Website-Betreibern selbst sammeln die Drittanbieter dabei Informationen von zahlreichen verschiedenen Webseiten. Sie können dadurch ein übergreifendes Online-Profiling durchführen und anbieten.

Browser unterstützen Drittanbieter-Cookies bald nicht mehr

Nun aber naht das Ende der Third-Party-Cookies. „Wir planen, die Unterstützung für Cookies von Drittanbietern in Chrome einzustellen", erklärte Justin Schuh, Director Chrome Engineering bei Google.

„Benutzer fordern mehr Datenschutz einschließlich Transparenz, Auswahl und Kontrolle darüber, wie ihre Daten verwendet werden – und es ist klar, dass sich das Web-Ökosystem weiterentwickeln muss, um diesen steigenden Anforderungen gerecht zu werden."

Einige Browser haben bereits reagiert, indem sie Cookies von Drittanbietern blockieren. In Zukunft aber werden führende Browser wie Chrome überhaupt keine Drittanbieter-Cookies mehr ausliefern. Der Weg zum Endgerät der Nutzer ist damit für diese Cookies versperrt. Deshalb sucht die Werbewirtschaft vermehrt Alternativen zu Cookies und setzt sie teilweise auch schon ein. Diese Alternativen sind aber weniger bekannt als Cookies und bisher nicht so einfach zu kontrollieren.

Kritiker warnen zudem davor, dass es ohne Third-Party-Cookies kaum noch Konkurrenz für das Google-Werbenetzwerk geben werde. Es gehe Google weniger um den Datenschutz als vielmehr darum, den Wettbewerb zu verdrängen.

Ganz gleich, welche Motive Browser-Anbieter wie Google haben: Die Nutzer der Browser müssen nun lernen, wie sie mit den Cookie-Alternativen umgehen, um sich in Zukunft gegen Online-Tracking schützen zu können.

Wie Cookie-Alternativen aussehen

Es gibt bereits verschiedene Alternativen zu den klassischen Cookies, die verstärkt zum Einsatz kommen werden. Einige stellen wir im Folgenden vor. →

Device Fingerprinting

Device Fingerprinting („Gerätefingerabdrücke") kann Geräte im Laufe der Zeit basierend auf den Konfigurationen und Einstellungen des Browsers verfolgen. Da jeder Browser mit all seinen Erweiterungen und Einstellungen einzigartig ist, kann der Gerätefingerabdruck ein Gerät identifizieren, ohne Cookies zu verwenden. Da der Fingerabdruck des Geräts die Merkmale der Browser-Konfiguration verwendet, hilft es nicht, Cookies zu löschen.

Gerätefingerabdruck-Technologien lassen sich verwenden, um Nutzer auf allen Arten von Geräten mit Internetverbindung zu verfolgen, die über Browser verfügen, z.B. auf Smartphones, Tablets, Laptops und Desktop-Computern.

IDFA und Advertising ID

Mobile Endgeräte nutzen vermehrt viele verschiedene Apps und nicht einen mobilen Browser, der nur eine App unter vielen ist. Deshalb verwenden Werbe- und Analyseunternehmen von Drittanbietern Gerätekennungen, z.B. IDFA (Apple iOS Identifiers for Advertisers) und Advertising ID von Google Android, um die verschiedenen Anwendungen, die auf einem bestimmten Gerät laufen, zu überwachen.

Advertising Identity

Vor dem Hintergrund der Einschränkungen bei der Nutzung von Third-Party-Cookies hat der Bundesverband Digitale Wirtschaft ein Grundlagenpapier zu alternativen Ansätzen zur Auslieferung von zielgerichteter Werbung veröffentlicht (siehe https://ogy.de/advertising-identity). Das Papier enthält u.a. die erste Definition von „Advertising Identity":

„Die ‚Advertising Identity' soll die Wiedererkennung eines pseudonymisierten Profils zum Zwecke der effizienten Werbeaussteuerung in Form von Personalisierung, Lokalisierung, Verifizierung, Erfolgsmessung und kontakt- und reichweitenoptimierter Budgetallokation von Werbemitteln ermöglichen. Mit ‚Advertising Identity' meint der BVDW die rein technische, pseudonymisierte Identität des Nutzers in Form der Gesamtheit (Graph) der Identifier (ID) und damit die Zusammenführung der in den unterschiedlichen Devices verwendeten ID-Formen."

Die Advertising Identity habe ausdrücklich nicht den Zweck, natürliche Personen zu identifizieren, so der BVDW.

Tracking-Schutz bei Firefox aktivieren

Der Browser Firefox bietet bereits einen verbesserten Tracking-Schutz. Nutzer finden ihn unter „Einstellungen ⇨ Sicherheit&Datenschutz". Dort lassen sich Schutzmechanismen aktivieren, die einige „Verfolger" blockieren. Das gilt z.B. für

- Skripte zur Aktivitätenverfolgung durch soziale Netzwerke,
- Cookies zur seitenübergreifenden Aktivitätenverfolgung,
- Inhalte zur Aktivitätenverfolgung in privaten Fenstern,
- heimliche Digitalwährungsberechner (Krypto-Miner) und
- Identifizierer (Fingerprinter).

Internetnutzer sensibilisieren

Bisherige Wege wie der Cookie-Manager reichen nicht mehr aus, um den Tracking-Schutz bei Browsern zu aktivieren. Je nach Browsertyp können und sollten Nutzer nun weitere Einstellungen gegen das Tracking vornehmen, um z.B. Device Fingerprinting zu verhindern. Nutzer mobiler Endgeräte müssen an das Tracking über andere Apps als den Browser denken und die oben im Kasten genannten Einstellungen beherzigen. Geben Sie entsprechende Hinweise in Ihrer nächsten Datenschutzunterweisung. Denn wenn die Third-Party-Cookies ihr Ende finden, stehen die alternativen Cookies schon lange bereit.

Oliver Schonschek, Dipl.-Phys., ist Technology Analyst mit Fokus auf IT-Sicherheit und Datenschutz.

Tipps für die Datenschutzschulung

Mobiles Tracking abschalten

PRAXIS-TIPP

Empfehlen Sie den Nutzern, bei mobilen Endgeräten die Kennungen auf dem jeweiligen Gerät in den Geräteeinstellungen zurücksetzen, um das mobile Tracking zu unterbrechen.

iOS-Benutzer können dies tun, indem sie dem Pfad „Einstellungen ⇨ Datenschutz ⇨ Werbung ⇨ Werbekennung zurücksetzen" folgen. Für Android lautet der Pfad „Google-Einstellungen ⇨ Anzeigen ⇨ Werbe-ID zurücksetzen". Dann ist es schwieriger, das Gerät mit früheren Aktivitäten zu verknüpfen. Doch die Verfolgung lässt sich mithilfe der neuen Werbekennung erneut starten.

Die Nutzer können aber auch die Verwendung von Kennungen für die Personalisierung der Werbung einschränken. Für iOS sind die Steuerelemente über „Einstellungen ⇨ Datenschutz ⇨ Werbung ⇨ Anzeigenverfolgung einschränken" verfügbar. Für Android geht das unter „Google Einstellungen ⇨ Anzeigen ⇨ Interessensbasierte Anzeigen deaktivieren".

Bild: iStock.com/MarioGuti

iOS und Android bieten die Möglichkeit, die Verfolgung einzuschränken

Bild: iStock.com/AntonioGuillem

Die zentrale Frage muss stets lauten: Welche Daten sind für meine Zwecke wirklich unbedingt erforderlich?

Onboarding-Prozesse

Neue Mitarbeiter – was ist aus Datenschutzsicht zu regeln?

Bewerbungs- und Einstellungsprozesse sind ohne personenbezogene Daten undenkbar. Doch Verantwortliche müssen darauf achten, wirklich nur mit solchen Informationen zu arbeiten, die unbedingt erforderlich sind.

In Ergänzung zu den allgemeinen Pflichten der Datenschutz-Grundverordnung (DSGVO) bei der Verarbeitung personenbezogener Daten regelt § 26 Bundesdatenschutzgesetz (BDSG) für Deutschland weitere Eckpunkte zum Beschäftigtendatenschutz. So umfasst der Beschäftigtenbegriff u.a. Bewerber der Unternehmen (§ 26 Abs. 8 Satz 2 BDSG).

Allgemeine Grundsätze

Als allgemeine Grundsätze gelten hier:

1. Rechtmäßigkeit prüfen (Erlaubnis): Eine Rechtsgrundlage muss die Verarbeitung von Bewerber- oder Beschäftigtendaten erlauben.
2. Zweckbindung einhalten: Das verlangt von Arbeitgebern sehr konkret, dass sie Beschäftigtendaten nur für festgelegte, eindeutige und legitime Zwecke (Art. 5 Abs. 1 Buchst. b DSGVO) erheben sowie verarbeiten dürfen. Ferner muss der Arbeitgeber diese Zwecke nachweisen können.
3. Daten minimieren: Es werden nur die Daten verarbeitet, die im Sinne der Datensparsamkeit und Datenvermeidung erforderlich sind.
4. Richtigkeit wahren: Es werden nur Daten zu den Beschäftigten verarbeitet, die sachlich korrekt und richtig sind.
5. Datenspeicherung begrenzen und Daten löschen: Der Arbeitgeber muss die Daten löschen, sobald er sie nicht mehr benötigt.
6. Integrität, Vertraulichkeit und sichere Verarbeitung wahren: Die Datenverarbeitung muss die Grundsätze der Datensicherheit berücksichtigen.
7. Transparenz ist Pflicht: Die Betroffenen müssen über die Verarbeitung ihrer Daten informiert sein und ihre Rechte wahrnehmen können.

Voraussetzungen aus dem BDSG

§ 26 Abs. 1 Satz 1 BDSG erlaubt es Unternehmen, personenbezogene Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses zu verarbeiten unter den folgenden Voraussetzungen: Die Verarbeitung muss erforderlich sein, um eine Entscheidung über die Begründung eines Beschäftigungsverhältnisses zu treffen, das Beschäftigungsverhältnis durchzuführen oder es zu beenden. →

BEISPIELE

Wie setzen Arbeitgeber die allgemeinen Grundsätze in der Praxis um?

- *Die Personalstelle eines Unternehmens kann Lebensläufe und Zeugnisse zum Zweck der Einstellung und der Personalverwaltung verarbeiten. Voraussetzung: Diese Unterlagen sind notwendig, um eine Entscheidung über die Begründung eines Beschäftigungsverhältnisses zu treffen, das Beschäftigungsverhältnis durchzuführen oder es zu beenden (§ 26 Abs. 1 Satz 1 BDSG).*
- *Lebensläufe und Zeugnisse von abgelehnten Bewerbern sollten nur dann und nur so lange in einem Bewerberpool gespeichert oder an andere Unternehmen weitergegeben werden, wie der Bewerber bzw. die Bewerberin dies im Rahmen einer ausdrücklichen Einwilligung gestattet.*
- *Belege und Angaben zu Bewerbern in Folge der Reisekostenerstattungen für Vorstellungstermine sollten zehn Jahre zum Zweck der Buchhaltung – und nur dafür! – aufbewahrt werden (§ 257 Abs. 4 HGB in Verbindung mit § 147 Abs. 3 AO).*

Weiterhin kann sie rechtmäßig sein, wenn sie erforderlich ist, damit die Interessenvertretung der Beschäftigten die Rechte und Pflichten, die sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung ergeben, ausüben oder erfüllen kann.

Dabei ist die Erforderlichkeit eng auszulegen. Das bedeutet, der Arbeitgeber muss einen legitimen Zweck verfolgen, den er ohne diese konkrete Datenverarbeitung nicht erreichen kann.

WICHTIG

Die Informationspflichten enden übrigens nicht mit dem Bewerbungsprozess. Sie gelten für alle Beschäftigten eines Unternehmens, selbst wenn ihr Beschäftigungsverhältnis bereits beendet wurde.

Recruiting-Prozess datenschutzkonform strukturieren

Was müssen Verantwortliche nun im Zuge der gesetzlichen Rahmenbedingungen beim Onboarding, also bei der Einstellung und Einführung eines neuen Mitarbeiters in seinen Einsatzbereich, beachten? Wie müssen sie ihren Recruiting-Prozess strukturieren?

Informationspflichten erfüllen

Verantwortliche dürfen Bewerbungsunterlagen und Daten zu den Bewerbern also zum Zweck der Entscheidung über die Begründung eines Beschäftigungsverhältnisses verarbeiten. Wichtig ist allerdings, die Bewerber und Bewerberinnen zu Beginn des Bewerbungsprozesses transparent darüber zu informieren, wie ihre personenbezogenen Daten verarbeitet werden.

Diese Informationen ergeben sich aus Art. 13 und Art. 14 DSGVO. Sie sollten u.a. Hinweise dazu enthalten, welche Daten verarbeitet werden, woher sie stammen, wer sie erhält, wie lange sie gespeichert werden und welche Datenschutzrechte Bewerber und Bewerberinnen haben.

Es spielt kaum eine Rolle, auf welchem Weg Bewerber diese Informationen erhalten. Das kann z.B. passieren über eine automatisierte Eingangsbestätigung, die die erforderlichen Informationen enthält, oder darüber, dass ein Online-Bewerberportal sie unmittelbar zur Verfügung stellt. Wichtig ist, dass Bewerber diese Informationen auf einem einfachen Weg bekommen. Die individuelle postalische Eingangsbestätigung ist der klassische Weg.

Social Monitoring

Manche Unternehmen nutzen im Recruiting-Prozess personenbezogene Daten aus dem Social Monitoring, d.h. aus sozialen Netzwerken. Die damit betrauten HR-Mitarbeiter müssen dabei sicherstellen, dass diese Daten möglichst mit einer ausdrücklichen Einwilligung des Bewerbers zur Verarbeitung in Bewerbungsprozessen versehen sind. Liegt keine Einwilligung vor, so wäre eine derartige Datenverarbeitung wohl nur auf der Rechtsgrundlage des berechtigten Interesses (Art. 6 Abs. 1 Buchst. f DSGVO) zulässig. Und die dabei durchzuführende Abwägung wird in privaten sozialen Netzwerken eher nicht zugunsten des Unternehmens ausfallen. Daher kann von der Verarbeitung von Bewerbungsdaten, die die Personalabteilung z.B. aus einem privaten Facebook-Profil erhoben hat, nur abgeraten werden.

Einstellungstests

Die Fragen eines Bewerbungsbogens sind stets so zu wählen, dass sie „als für die Begründung des konkreten Beschäftigungsverhältnisses erforderlich“ einzustufen sind.

Nutzen Unternehmen Einstellungstests im Rahmen eines Auswahlverfahrens, so sind sie nur erforderlich, wenn kein milderes Mittel zur Verfügung steht. Eignungstests – z.B. Arbeitsprobe, Leistungstest, Intelligenztest oder Assessments – müssen nachweisbar geeignet und erforderlich sein, um die Eignung des Bewerbers für die freie Position festzustellen. Allgemeine Intelligenz- oder Persönlichkeitstests, um die Gesamtpersönlichkeit des Beschäftigten einzuschätzen, sind daher vermutlich unzulässig.

Das Vorstellungsgespräch

Eines der wichtigsten Elemente im Recruiting-Prozess ist das persönliche Vorstellungsgespräch. Aber darf ich in diesem Gespräch denn noch alle Fragen stellen, die früher zur Entscheidungsfindung gedient haben? Spielt die DSGVO an dieser Stelle überhaupt eine Rolle?

Eine der teuersten Investitionen ist die Beschäftigung von neuen Mitarbeitern. Stellt ein Unternehmen z.B. eine junge Frau unbefristet als Sachbearbeiterin mit einem jährlichen Bruttoeinkommen von 40.000 € ein, so ist dies bis zu ihrem Renteneintritt bei einem normalen Beschäftigungsverlauf eine Investition von über 2 Millionen €. Plant ein Arbeitgeber Ausgaben in diesem Umfang, besteht bei ihm sicherlich ein berechtigtes Interesse an aussagekräftigen Informationen zu potenziellen Beschäftigten.

Daten aus beruflichen Netzwerken

Anders als bei privaten Sozialen Netzwerken sieht das Ergebnis der Abwägung vermutlich bei beruflichen Netzwerken wie XING oder LinkedIn aus, die Beschäftigte zur Selbstdarstellung nutzen. Hier darf in der Regel angenommen werden, dass das schutzwürdige Interesse des Bewerbers hinter dem Interesse des potenziellen Arbeitgebers an einer Datenerhebung ohne Mitwirkung des Beschäftigten zurücksteht. Zu beachten ist hier, dass die personenbezogenen Daten nicht direkt bei der betroffenen Person erhoben werden und zu prüfen ist, ob der/die Betroffene nach Art. 14 DSGVO informiert werden muss.

Nationalität, Gesundheitsdaten, Vorstrafen, Ermittlungsverfahren

Beispiele zu Fragen im Vorstellungsgespräch

Fragen zu bestimmten Stammdaten wie Namen, Anschrift, Telefonnummer und E-Mail-Adresse sind für den Arbeitgeber erforderlich, um mit dem Bewerber Kontakt aufnehmen zu können. Kritisch wird es, wenn der Bewerbungsprozess Geburtsort, Geburtsname, Alter und Nationalität abfragt. Solche Fragen können Indizien für eine Diskriminierung sein. Arbeitgeber sollten nur dann danach fragen, wenn die Informationen wirklich erforderlich sind.

Fragen nach einer Behinderung, Vorerkrankungen und dem Gesundheitszustand eines Bewerbers sind nur eingeschränkt zulässig. Der Arbeitgeber darf sich danach erkundigen, ob eine Krankheit oder eine Beeinträchtigung des Gesundheitszustands vorliegt, durch die der Bewerber nur eingeschränkt für die vorgesehene Tätigkeit geeignet ist. Ferner darf er fragen, welche Auswirkungen die Behinderung oder Erkrankung auf die angestrebte Tätigkeit haben, um mit geeigneten Maßnahmen zu unterstützen bzw. den Arbeitsplatz anzupassen.

Solche Fragen könnten Indizien für eine Diskriminierung sein. Nutzen Sie die Fragen nur, wenn sich die Erforderlichkeit konkret nachweisen lässt.

Nach Vorstrafen darf ein Arbeitgeber nur fragen, wenn sie für den Arbeitsplatz unbedingt relevant sind. So wären hier wohl Vorstrafen, die nach der Art ihrer Begehung oder den betroffenen Rechtsgütern objektiv eine besondere Nähe zur vorgesehenen Beschäftigung hätten, zu nennen. Hat sich z.B. ein Bankkaufmann bei einer Sparkasse beworben, darf das Vorstellungsgespräch nach Vorstrafen zu Vermögensdelikten fragen. Verkehrsdelikte sind dagegen nicht relevant.

Die Frage nach laufenden Straf- und Ermittlungsverfahren ist wohl zulässig, soweit ein solches Verfahren Zweifel an der persönlichen Eignung und Zuverlässigkeit des Bewerbers für den konkreten Arbeitsplatz begründen kann. Oder wenn das Verfahren die Verfügbarkeit des Bewerbers erheblich einschränken würde, weil ein zukünftiger Arbeitgeber mit umfangreichen Ermittlungen, Untersuchungshaft oder der Verurteilung zu einer Freiheitsstrafe rechnen müsste.

Bild: iStock.com/Charday Penn

Hier treffen dann möglicherweise das Interesse des Unternehmens an aussagekräftigen Informationen und das Persönlichkeitsrecht von Bewerberinnen und Bewerbern aufeinander. Grundsätzlich besteht für Arbeitgeber sicherlich das durch die Rechtsprechung entwickelte „Fragerecht des Arbeitgebers“ weiterhin und kann als zulässig eingestuft werden.

PRAXIS-TIPP

Es dürfen im Bewerbungsgespräch und im weiteren Bewerbungsprozess nur solche Informationen erhoben werden, die – je nach Stand des Bewerbungsverfahrens – für die Entscheidungsfindung tatsächlich benötigt werden. Und das sollte der potenzielle Arbeitgeber sorgfältig und nachweislich dokumentieren.

Bewerberunterlagen: Wer bekommt sie, wie lange aufbewahren?

Im Rahmen des Recruiting-Prozesses dürfen Unternehmen die Bewerbungsunterlagen nur den Personen zugänglich machen, die direkt damit befasst sind, die Stelle zu besetzen. Das ist zumeist der/die zuständige Sachbearbeiter(in) in der HR-Abteilung sowie der unmittelbare Vorgesetzte des möglichen Arbeitnehmers.

Ist eine Entscheidung getroffen, empfiehlt es sich, die nicht mehr benötigten Bewerbungsunterlagen nicht sofort zu löschen, sondern so lange vorzuhalten, dass das Unternehmen der Klage eines Bewerbers aufgrund des Allgemeinen Gleichbehandlungsgesetzes (AGG) entgegnen kann. Solange der Arbeitgeber mit einer solchen Klage rechnen muss, kann er die Bewerberdaten aufbewahren.

Die Frist zur Aufbewahrung der Bewerbungsunterlagen ergibt sich aus § 15 Abs. 4 AGG. Sie beträgt gemäß dem 25. Tätigkeitsbericht Nr. 5.7.3 des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) bei einer ablehnenden Bewerbung sechs Monate ab Zugang der Ablehnung an die Bewerberin oder den Bewerber. Dann sind die Bewerbungsunterlagen zurückzugeben oder ordnungsgemäß zu vernichten. →

Führungszeugnisse & Co.

Neben den Ergebnissen aus Einstellungstests können z.B. ärztliche Bescheinigungen oder ein Führungszeugnis eine wesentliche Rolle spielen, um die berufliche Eignung festzustellen. Die Daten aus diesen Unterlagen müssen jedoch eine wichtige Voraussetzung sein, um den Beruf ausüben zu können (z.B. Busfahrer, Erzieher). Im Rahmen der Datenminimierung dürfen Verantwortliche also ausschließlich Daten abfragen, die die geforderte Eignung auch tatsächlich nachweisen.

Verarbeitungsverzeichnis nicht vergessen

Welche Wege die personenbezogenen Daten der Beschäftigten einschließlich der Bewerber nehmen, wie sie verarbeitet und gespeichert werden, wer die Daten zur Kenntnis erhält und wie lange sie gespeichert werden: All das sollte im Verzeichnis von Verarbeitungstätigkeiten (Art. 30 DSGVO) zu finden sein.

Personalfragebogen

Im nächsten Schritt benötigt der Arbeitgeber weitere Informationen von seinem neuen Arbeitnehmer. Das passiert in der Regel in Form eines Personalfragebogens. Bei diesen Angaben handelt es sich um eine Datenverarbeitung zur Begründung des Beschäftigungsverhältnisses. Dabei ist zu beachten, dass die Rechtmäßigkeit der erhobenen Daten nur für solche Daten vorliegt, die für die Begründung des Arbeitsverhältnisses erforderlich sind. Der Arbeitgeber muss jeweils ein berechtigtes, billigenswertes und schutzwürdiges Interesse daran haben, dass der Beschäftigte die Fragen beantwortet.

Auf Vertraulichkeit verpflichten

Neben den Verpflichtungserklärungen für neue Beschäftigte zu den Themen Betriebs-, Telekommunikations- und Steuergeheimnis ist es für jedes Unternehmen empfehlenswert, neue Mitarbeiter nach Art. 29 DSGVO auf die Vertraulichkeit im Umgang mit personenbezogenen Daten zu verpflichten.

Dabei sollten die neuen Mitarbeiter und Mitarbeiterinnen darüber informiert werden, was sie in datenschutzrechtlicher Hinsicht bei ihrer täglichen Arbeit beachten müssen. Diese Vertraulichkeitsverpflichtung sollte der Arbeitgeber ausreichend dokumentieren.

ONLINE-TIPP

Geeignete Mustervorlagen für die Verpflichtung finden Sie auf der Seite des bayerischen Landesamts für Datenschutzaufsicht unter https://ogy.de/baylda-verpflichtung-beschaeftigte oder bei der Stiftung Datenschutz unter https://ogy.de/stiftungds-praxishilfen.

Abschließend sei nochmals betont, dass der Arbeitgeber alle genannten Aspekte im Rahmen der Verarbeitungen von Beschäftigtendaten sorgfältig und nachweislich dokumentieren muss. Nur so kommt er der Rechenschaftspflicht von Art. 5 Abs. 2 DSGVO nach!

Arnd Fackeldey ist Geschäftsführer der Digital Compliance Consulting GmbH. Als DSB und Auditor unterstützt er Unternehmen bei Design und Einführung von Datenschutzprozessen sowie Datenschutzbeauftragte und Betriebsräte bei Kontrollaufgaben.

Vorschlag für Checkliste

bei Eintritt von neuen Beschäftigten

Name, Vorname der/des Beschäftigten	
Funktion/Stelle laut Stellenplan	
Unmittelbarer Vorgesetzter	
Fachbereich/Abteilung	
Einstellungsdatum	
Personalnummer	
Beschäftigungsform	☐ Angestellte/r ☐ Leiharbeitnehmer/in ☐ Auszubildende/r ☐ Praktikant/in

ELEMENT	ERFORDERLICH	Erledigt am/durch
Unmittelbare/r Vorgesetzte/r	**Onboarding-Aufgabe (Vorbereitung)** ☐ Stellenbeschreibung vorbereiten/anpassen ☐ Einarbeitungsplan für die ersten drei Monate vorbereiten ☐ Information zur/m neuen Mitarbeiter/in an Kollegen vorbereiten ☐ Zugänge für folgende Systeme vorbereiten ☐ Zeiterfassungszugang anlegen lassen/Chipkarte ordern ☐ Netzwerkzugänge und Berechtigungen abstimmen und ordern ☐ Schlüssel und Zugangskarte mit Ausgabeformular vorbereiten ☐ weitere Berechtigungen und Ausgaben vorbereiten (Firmenfahrzeug, Notebook, Mobiltelefon, etc.) ☐ Betreuung für die ersten Tage personell festlegen ☐ Einarbeitungspaten benennen ☐ Einstellungsuntersuchung organisieren ☐ Ausgabe von Formularen und grundsätzlichen Dienstanweisungen	

ELEMENT	ERFORDERLICH	Erledigt am/durch
	Prozess ab Eintritt (erste Woche): ☐ Firmenrundgang/-besichtigung durchführen ☐ Kantinenbesichtigung und Einweisung in die Abläufe zur Pause ☐ Einweisung in das Zeiterfassungssystem und die Abläufe zur Beantragung von Urlaub ☐ Einweisung in die Arbeitsanweisungen zur Nutzung der EDV (Netzwerk, Cloud, Mail, etc.) und den Umgang mit Geschäftsgeheimnissen ☐ Einweisung in die Hausordnung und Sicherheitssysteme ☐ Schulung zur Datensicherheit und zum Datenschutz organisieren ☐ Vertraulichkeitsverpflichtung besprochen und unterzeichnet	
Sicherheitsbeauftragter	☐ Sicherheitsunterweisung durchführen ☐ Brandschutzvorgaben und Erste-Hilfe-Abläufe schulen	
IT-Abteilung	☐ Abstimmung mit dem Vorgesetzten über die Ausrüstung und den Zugriff auf Software ☐ Zugriffsrechte mit dem Vorgesetzten abstimmen ☐ Bei Home-Office: Datensicherheit gem. Richtlinie sicherstellen, Zugang ☐ Telefon und / oder Mobile gem. Richtlinie ☐ Büroausstattung ☐ Verbindung zum Eingangskontrollsystem herstellen	
Sekretariat/ Verwaltung	☐ Schlüssel- und Chipkarten bestellen ☐ Anpassung von Mail Sammeladressen und Telefonanlage ☐ Büromaterialien vorbereiten (Locher, Tacker, etc.)	
Marketingbereich	☐ Homepage anpassen ☐ Visitenkarten abstimmen/ordern	

Wichtiger Hinweis:
Nach der kompletten Abarbeitung ist die Checkliste an die HR-Abteilung zu überreichen. Diese Checkliste wird nach Überprüfung auf Vollständigkeit aus datenschutzrechtlichen Gründen vernichtet! Es dürfen keine (Teil-)Kopien von dieser Checkliste angefertigt werden!

Muster einer Checkliste für neu eingestellte Mitarbeiter. Die Checkliste finden Abonnenten kostenlos als anpassbare Word-Datei unter www.datenschutz-praxis.de/downloads.

Fokus Datensicherheit

Kompendium Videokonferenzsysteme

Videokonferenzen erleben gerade einen Boom. Von der Installation eines Systems bis zu seiner Deinstallation ergeben sich dabei zahlreiche Fragen zur Datensicherheit. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) gehört zu den ganz wenigen Institutionen, die sich diesen Fragen bereits seit Jahren widmen. Sein Kompendium Videokonferenzsysteme (KoViKo) ist deshalb trotz des Stands April 2020 kein Schnellschuss aus aktuellem Anlass, sondern eine umfassende Ausarbeitung zu diesem Thema.

Technische Grundlagen & Funktionen

Berücksichtigt sind alle Facetten der Datensicherheit, mit Ausnahme der Besonderheiten, die sich beim Umgang mit Verschlusssachen (im Volksmund: Geheimdokumenten) in Videokonferenzen ergeben. Ziel ist dabei nicht der Produktvergleich konkreter Konferenzsysteme. Dargestellt sind vielmehr die technischen Grundlagen, auf denen in der einen oder anderen Form alle Systeme aufbauen. Daran schließt sich eine Erklärung der üblichen Leistungsmerkmale und der häufigsten optionalen Funktionen an, jeweils verbunden mit einer sicherheitstechnischen Bewertung.

Wichtige Fragen für eine Bewertung

Auf dieser Basis ist es dem Leser möglich, selbst sehr schnell die Fragen zu formulieren, die relevant sind, um ein konkretes System zu bewerten. Hierfür einige Beispiele:

- Was ist eine Multipoint Control Unit und wann brauche ich sie? (Seite 23)
- Was bringt ein separater Raum im Gebäude, in dem ein Konferenzsystem fest installiert ist? (Seite 47)
- Lässt sich die von vielen Aufsichtsbehörden geforderte Ende-zu-Ende-Verschlüsselung bei Konferenzsystem überhaupt realisieren? (Seite 22 und Seiten 24/25)
- Was ist mit Manipulationen der Signalisierung gemeint und wie kann man sich dagegen schützen? (Seite 54)

Typische Nutzungsszenarien

Ausgesprochen hilfreich sind drei ausführlich dargestellte typische Nutzungsszenarien (Forschungszentrum, Start-up, Großunternehmen; Kapitel 8, Seiten 109 folgende). In einem eigenen Unterkapitel ordnet ihnen das Kompendium die notwendigen Sicherheitsanforderungen zu. Das erfolgt in Form einer Tabelle (siehe Kapitel 8.5, Seiten 120 folgende).
Wer über keine oder geringe Vorkenntnisse zum Thema verfügt, kann das Kompendium als eine Art Lehrbuch nutzen. Wer konkrete Einzelaspekte vertiefen will, findet die entsprechenden Kapitel in der Regel schon mithilfe der Inhaltsübersicht. Ein ausführliches Stichwortverzeichnis ist jedoch ebenfalls vorhanden.
Das Kompendium Videokonferenzsysteme (KoViKo – Version 1.0.1) weist den Stand April 2020 aus und umfasst 173 Seiten. Es ist abrufbar unter https://ogy.de/bsi-koviko.

Bild: iStock.com/elenabs

Geldbuße von 6.800 €

Deutlich verspätete Data-Breach-Meldung

Eine Reha-Klinik sandte den Entlassungsbericht eines Patienten per Post versehentlich an einen anderen Patienten. Der „falsche Adressat" informierte die Klinik an einem Freitag per Telefon über den Vorfall. Die Meldung nach Art. 33 Abs. 1 DSGVO an die hessische Datenschutzaufsicht durch die Klinik erfolgte erst sieben Tage später.

Als Begründung für die verspätete Meldung gab die Klinik zum einen an, dass ein Wochenende dazwischen lag. Zum anderen sei ein derartiger Fehler in der Klinik noch nicht vorgekommen. Daher hätten die Mitarbeiter nicht gleich gewusst, was in diesem Fall zu tun ist.

Diese Argumente hielt die hessische Datenschutzaufsicht für unzureichend. Sie verhängte wegen der verspäteten Meldung eine Geldbuße von 6.800 €. In der Begründung hierfür heißt es u.a.: „Der Klinik war hier insbesondere anzulasten, dass sie ihre Mitarbeiter trotz der Geltung der DS-GVO seit dem 25.05.2018 immer noch nicht ausreichend über ihre Pflichten unterrichtet hatte."

Verfahren frühzeitig festlegen!

Als Lehre aus dem Vorfall mahnt die Datenschutzaufsicht, eine Verfahrensanweisung für den Ernstfall schriftlich zu fixieren. Sie sollte insbesondere festlegen,

- welche Personen und Fachbereiche wann und wie in entsprechenden Fällen einzubinden sind (z.B. die IT-Abteilung),
- wie die Vertretung geregelt ist, wenn einzelne Personen abwesend sind (Urlaub, Krankheit etc.), und
- wie die Beschäftigten die Meldeprozesse im Detail durchführen sollen.

Quelle: 48. Tätigkeitsbericht des Hessischen Beauftragten für Datenschutz und Informationsfreiheit für 2019, Seiten 136/137. Der Bericht ist abrufbar unter https://ogy.de/tb-hessen-2019.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken (Bayern). Neben Corona beschäftigen ihn gerade historische Verbindungswege.

Bild: iStock.com/metamorworks

Allzu oft landen z.B. Diagnosen beim falschen Empfänger. Gerade bei Gesundheitsdaten ist dann nicht nur eine Meldung an die Aufsicht, sondern auch an die betroffene Person nötig.

Wer ist wann wie zu informieren?

Benachrichtigungspflichten bei Datenpannen richtig umsetzen

Eine Umfrage des Senders NDR unter den Datenschutz-Aufsichtsbehörden zeigt: Sensible Patientendaten landen in großer Zahl bei falschen Empfängern. Wer richtig mit solchen Datenpannen umgeht und dafür sorgt, sie zukünftig zu vermeiden, minimiert das Risiko von Bußgeldern.

Der Landesbeauftragte für den Datenschutz und die Informationsfreiheit Baden-Württemberg hat für seinen Tätigkeitsbericht 2019 Meldungen von Datenpannen ausgewertet (abrufbar unter https://ogy.de/tb-bw-2020). Eine Vielzahl dieser Meldungen betraf Arztpraxen. Arztbriefe, Rezepte, Diagnosen oder Röntgenbilder landen also durch verschiedentlichen Fehlversand bei falschen Empfängern.

- Geradezu ein Klassiker landet auf Platz 1 der Pannen: der Postfehlversand.
- Der E-Mail-Fehlversand erreicht Platz 3.
- Der Versand von E-Mails mit offenem Verteiler – also ohne die „bcc-Funktion" zu verwenden – nimmt Platz 5 ein.
- Und der Fehlversand von Telefaxen landet auf Platz 7.

Welche Datenpannen Platz 4 und 6 belegen, ist dem Bericht nicht zu entnehmen.

Besonders kritisch ist Platz 2. Dabei geht es um Datenpannen aufgrund von Cyberangriffen auf Arztpraxen. Das lässt auf einen mangelnden technisch-organisatorischen Datenschutz schließen.

Was ist eine Datenpanne?

Die Datenschutz-Grundverordnung (DSGVO) spricht in Art. 33 nicht von Datenpannen, sondern von der „Verletzung des Schutzes personenbezogener Daten". Das ist nach Art. 4 Nr. 12 DSGVO eine „Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung bzw. zum unbefugten Zugang zu personenbezogenen Daten führt", die der Verantwortliche in irgendeiner Art und Weise verarbeitet hat.

Verantwortliche müssen beachten, dass auch eine vorübergehende Nicht-Verfügbarkeit aufgrund von Sicherheitsvorfällen eine Form von Datenschutzverletzungen darstellt. Denn in solchen Fällen sind die

Kategorie	Erläuterung
Verletzung der Vertraulichkeit	ist die unbefugte oder unbeabsichtigte Offenlegung bzw. Einsichtnahme in personenbezogene Daten. Die Datenpannen-Klassiker in Arztpraxen wie Fehlversendungen oder offene E-Mail-Verteiler fallen alle in diese Kategorie.
Verletzung der Integrität	ist die unbefugte oder unbeabsichtigte Änderung personenbezogener Daten. Dazu gehört z.B. die versehentliche Änderung von Adressdaten.
Verletzung der Verfügbarkeit	ist der unbefugte oder unbeabsichtigte Verlust des Zugangs zu personenbezogenen Daten oder auch die unbeabsichtigte/unrechtmäßige Vernichtung von Daten. Hierzu zählen z.B. die versehentliche Löschung von Daten oder der Verlust des Schlüssels bei verschlüsselten Daten. Darüber hinaus kann ein Verlust der Verfügbarkeit auch entstehen, wenn der normale Betriebsablauf erheblich gestört wird, z.B. bei einem Stromausfall oder bei einem Angriff in Form der gezielten Überlastung von Servern (Denial-of-Service-Angriff).

In diese drei Gruppen lassen sich Verletzungen des Schutzes personenbezogener Daten unterteilen

Anforderungen von Art. 32 DSGVO (angemessenes Schutzniveau) nicht erfüllt.

Wann und wie erfolgt die Meldung an die Aufsichtsbehörde?

Verantwortliche müssen Datenpannen innerhalb von 72 Stunden ab „Bekanntwerden" an die zuständige Aufsichtsbehörde melden (Art. 33 DSGVO). Bekanntwerden bedeutet in diesem Zusammenhang, dass der Verantwortliche eine bestimmte Gewissheit in Bezug auf einen Sicherheitsvorfall hat, der auch den Schutz personenbezogener Daten beeinträchtigt hat. Der Verantwortliche darf aber zunächst eine kurze interne Prüfung durchführen, ob eine Verletzung vorliegt oder nicht.

Für die Meldung halten die Aufsichtsbehörden auf ihren jeweiligen Internetseiten Hinweise und Formulare bereit.

Was muss drinstehen?

Die Meldung von Datenpannen an die Aufsichtsbehörde muss bestimmte Informationen enthalten:

- Beschreibung der Verletzung des Schutzes personenbezogener Daten (z.B. Fehlversand von Post durch falsche Adressierung), die Kategorien betroffener Personen und die ungefähre Anzahl, betroffene Datenkategorien (z.B. Bankverbindungen)
- Namen und Kontaktdaten des Datenschutzbeauftragten bzw. einer sonstigen Anlaufstelle
- Beschreibung der wahrscheinlichen Folgen der Schutzverletzung
- Beschreibung der ergriffenen bzw. vorgeschlagenen Maßnahmen, um die Datenpanne zu beheben und mögliche nachteiliger Auswirkungen zu beheben. Hier können Verantwortliche z.B. ihre Mitarbeiter erneut zum Faxversand schulen oder wirksame Verschlüsselungen einführen.

Nicht alle Datenpannen lassen sich innerhalb von 72 Stunden in einer Meldung zusammenfassen. Verantwortliche müssen eventuell weitere Untersuchungen durchführen, um alle Fakten zusammenzutragen. Art. 33 Abs. 4 DSGVO gestattet ausdrücklich eine schrittweise Meldung an die Aufsichtsbehörden.

Wann bestehen zusätzliche Informationspflichten?

Zusätzlich zur Meldung an die Aufsichtsbehörde müssen Verantwortliche auch die betroffenen Personen unverzüglich – d.h. ohne schuldhaftes Zögern – von der Datenpanne benachrichtigen. Voraussetzung ist, dass als Folge der Datenpanne voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten der betroffenen Personen besteht. Das regelt Art. 34 DSGVO. Aus Art. 34 Abs. 3 DSGVO ergeben sich die Ausnahmefälle, in denen betroffene Personen nicht von der Datenpanne zu informieren sind.

Wann besteht ein hohes Risiko für die betroffenen Personen?

Im Gegensatz zur Datenschutz-Folgenabschätzung (DFSA), die mögliche Risiken und mögliche Schäden betrachtet, ergibt sich das „hohe Risiko" bei der Datenpanne aus ihren Folgen:

- Art der Datenschutzverletzung: Sind Daten offengelegt worden oder „nur" unwiederbringlich verloren gegangen?
- Art der betroffenen personenbezogenen Daten: je sensibler die Daten (z.B. Gesundheitsdaten), desto höher das Risiko für die betroffenen Personen
- Identifizierbarkeit der Betroffenen
- Schwere der Folgen für die betroffenen Personen: Kann die Datenpanne zu Identitätsdiebstahl bzw. -betrug führen? Kann sie Verletzungen, Demütigungen oder Rufschädigungen verursachen? Sind die Daten in die Hände von Kriminellen gelangt, die finanzielle Schäden bei den betroffenen Personen verursachen können?

Wann und wie Betroffene informieren?

Wann muss der Verantwortliche (bei hohem Risiko) die betroffenen Personen informieren? Ganz einfach: So schnell wie möglich! Wichtigstes Ziel muss es sein, die betroffenen Personen gezielt über Vorkehrungen zu informieren, die sie selbst zu ihrem eigenen Schutz treffen können (Erwägungsgrund 86 DSGVO).

Für die Informationspflichten muss der Verantwortliche u.U. mehrere Kommunikationskanäle nutzen, um alle Betroffenen optimal zu erreichen. Das kann per Post, E-Mail oder deutlich platzierte Hinweise auf der Unternehmenswebsite geschehen. Weiterhin sind herausgehobene Anzeigen in Printmedien möglich. Nicht ausreichen dürfte eine Pressemitteilung oder der Hinweis in einem Unternehmensblog.

PRAXISTIPP

Faustformel: Verantwortliche sollten sich fragen, ob betroffene Personen selbst etwas tun können, um ihr Risiko zu verringern. Können sie z.B. ihr Passwort wechseln oder die Kreditkarte sperren? Lautet die Antwort Ja, so sind sie von der Datenpanne zu benachrichtigen. Im Übrigen gehen die Aufsichtsbehörden davon aus, dass Datenpannen bei besonderen Kategorien personenbezogener Daten, v.a. bei Gesundheitsdaten, immer eine Benachrichtigung der betroffenen Personen erfordern.

Zwei Verstöße in einem!

Fehler lassen sich nicht immer vermeiden. Sind sie jedoch geschehen, reduziert der DSGVO-konforme Umgang mit Datenpannen das Risiko, dass die Aufsichtsbehörde zusätzlich eine Geldbuße verhängt.

Verantwortliche sollten beachten, dass Nichtmeldungen von Datenpannen bzw. Nicht-Information der Betroffenen ein Hinweis auf fehlende oder unzureichende Sicherheitsmaßnahmen sind. Das können die Aufsichtsbehörden als zwei Verstöße gegen die DSGVO werten – mit den entsprechenden Sanktionsmöglichkeiten!

Rechtsanwältin Andrea Gailus ist in eigener Anwaltskanzlei tätig und befasst sich neben dem Zivilrecht schwerpunktmäßig mit IT- und Datenschutzrecht.

Bild: iStock.com/dragana991

Wer für seine Beschäftigten einen Videokonferenz-Dienst nutzt, sollte schon im Vorfeld darauf achten, dass der Datenschutz stimmt – oder die Lücken zumindest jetzt nachträglich schließen

Noch keine Geldbußen, aber ...

Videokonferenz-Dienste – darauf achten die Aufsichtsbehörden

Verschiedene deutsche Datenschutzaufsichtsbehörden haben sich jüngst zum Einsatz von Videokonferenzen geäußert. Welche Punkte sind danach für Verantwortliche besonders wichtig?

Aufgrund der aktuellen Einschränkungen durch COVID-19 haben zahlreiche Unternehmen und Behörden Videokonferenz-Dienste eingeführt. So können sie die interne und externe Kommunikation weiterführen. Es ist davon auszugehen, dass zumindest einige Verantwortliche die Prüfung, ob sich diese Dienste auch datenschutzkonform einsetzen lassen, vernachlässigt haben.

Die Datenschutzaufsichtsbehörden haben dies zum Anlass genommen, Hinweise zu den Anforderungen an den Einsatz von Videokonferenz-Diensten zu veröffentlichen. Sie fordern Verantwortliche dazu auf, „kurzfristig eingesetzte, aber nicht datenschutzgerechte Lösungen sobald wie möglich durch datenschutzgerechte zu ersetzen". So die Berliner Beauftragte für Datenschutz und Informationsfreiheit.

Woran orientieren?

Die Kernaussage aller Aufsichtsbehörden lautet – wenig überraschend –, dass Verantwortliche auch in Ausnahmesituationen wie der COVID-19-Pandemie personenbezogene Daten nur verarbeiten dürfen, wenn sie die Datenschutz-Grundverordnung (DSGVO) einhalten.

Die DSGVO enthält jedoch keine spezifischen Regelungen zu Videokonferenz-Diensten oder ähnlichen Systemen. Also orientieren sich die Aufsichtsbehörden an den allgemeinen Datenschutzgrundsätzen und ergänzen sie um anwendungsspezifische Hinweise.

Was sind die wichtigsten Punkte?

Auch wenn die Stellungnahmen nicht deckungsgleich sind, kristallisieren sich folgende Punkte heraus, auf die die Datenschutzaufsichtsbehörden derzeit in besonderem Maße achten:

- Hat der Verantwortliche geprüft, ob es Alternativen zu Videokonferenzen gibt (z.B. Telefonkonferenzen oder E-Mails)?
- Bevorzugt er „On-Premises"-Lösungen? Also einen Dienst, den er nicht auf der Hardware des Anbieters betreibt, sondern auf der eigenen bzw. auf angemieteter Hardware in einem fremden Rechenzentrum?
- Hat er die datenschutzrechtlichen Rollen und Verantwortlichkeiten zwischen Unternehmen und Anbieter geprüft (separat Verantwortlicher, gemeinsam Verantwortlicher, Auftragsverarbeiter)? Hat er die erforderlichen Verträge abgeschlossen?
- Erfolgen Drittstaattransfers nur mit entsprechender Rechtsgrundlage (z.B. EU-U.S. Privacy Shield oder Standarddatenschutzklauseln)?
- Findet keine Auswertung von Metadaten oder Inhaltsdaten der Kommunikation zu eigenen Zwecken des Anbieters und keine Weitergabe an Dritte statt?
- Ist standardmäßig die Aufzeichnung von Sprache und Video deaktiviert (insbesondere wegen strafrechtlicher Risiken)?
- Hat der Verantwortliche seine Datenschutzerklärung angepasst?
- Sind die Kommunikationskanäle durch Transportverschlüsselung (TLS) und bei sensiblen Daten durch zusätzliche Inhaltsverschlüsselung (Ende-zu-Ende-Verschlüsselung) geschützt?

Sind die Hinweise vollständig?

Nein, die Stellungnahmen der Datenschutzaufsichtsbehörden erheben keinen

To do	Erledigt
Im Vorhinein überlegen, ob es Alternativen zur Videokonferenz gibt. Tut es auch eine Telefonkonferenz oder ein Austausch per E-Mail?	☐
Überblick zu Anbietern von Videokonferenz-Diensten verschaffen. Die niederländische Datenschutzaufsicht hat eine Übersicht zu verschiedenen Videokonferenz-Anbietern erstellt. Eine deutsche Übersetzung findet sich auf der Website des BfDI (siehe „Weiterführende Informationen“).	☐
Entscheidung für bestimmten Anbieter anhand genannter Kriterien treffen und dokumentieren (ggf. Betriebsrat involvieren).	☐
Prüfen, ob eine Datenschutz-Folgenabschätzung nötig ist.	☐
Verträge abschließen (z.B. Vertrag zur Auftragsverarbeitung und Standarddatenschutzklauseln).	☐
Interne Dokumente erstellen oder anpassen (z.B. Datenschutzerklärung und Verarbeitungsübersicht).	☐
Den ausgewählten Videokonferenz-Dienst kontrollieren und, wenn sich Funktionalitäten ändern, erneut prüfen.	☐

Die Checkliste hilft beratenden Datenschutzbeauftragten und Verantwortlichen dabei, den Entscheidungs- und Implementierungsprozess zu Videokonferenz-Diensten zu strukturieren. Abonnenten finden die Liste als Download unter www.datenschutz-praxis.de.

Anspruch auf Vollständigkeit. Stattdessen fokussieren sie sich auf die aus ihrer Sicht wichtigsten Anforderungen für einen datenschutzkonformen Einsatz.

Nicht zu vergessen sind weitere erforderliche Maßnahmen. Verantwortliche müssen etwa prüfen, ob eine Datenschutz-Folgenabschätzung nötig ist, sie müssen die Videokonferenzen in das Verzeichnis von Verarbeitungstätigkeiten aufnehmen und den Betriebsrat einbeziehen (sofern vorhanden).

Warum sollte ich das beachten?

Bindend oder nicht bindend?

Die Stellungnahmen der Datenschutzaufsichtsbehörden sind nicht unmittelbar bindend für Unternehmen. Deutsche Gerichte und andere Aufsichtsbehörden werden jedoch die dort formulierten Anforderungen bei der Auslegung und Anwendung der DSGVO oder des Bundesdatenschutzgesetzes berücksichtigen.

Risiken im Fall von Verstößen?

Datenschutzaufsichtsbehörden können Geldbußen von bis zu 20 Millionen Euro oder 4 % des Jahresumsatzes nach Art. 83 DSGVO verhängen. Während in der Vergangenheit Bußgelder deutscher Aufsichtsbehörden eher milde ausfielen, ließ sich im vergangenen Jahr eine signifikante Verschärfung beobachten.

Darüber hinaus können betroffene Personen wie z.B. Mitarbeiter bei Verstößen Schadenersatz nach Art. 82 DSGVO geltend machen. Dagegen ist es in der Rechtsprechung noch umstritten, ob Wettbewerber entsprechende Verstöße gegen die DSGVO abmahnen dürfen.

Schließlich ist zu beachten, dass für Unternehmen auch indirekte Kosten durch einen eventuellen Reputationsschaden oder durch den verursachten Managementaufwand anfallen können.

Durchsetzungsdichte und -härte?

Bislang gering. Der Umstand, dass sich innerhalb weniger Wochen mehrere Datenschutzaufsichtsbehörden unabhängig voneinander zum Einsatz von Videokonferenz-Diensten im Unternehmen geäußert haben, deutet jedoch darauf hin, dass dieses Thema besonders in den Fokus gerückt ist. Es ist daher zu erwarten, dass die Aufsichtsbehörden ihre Durchsetzungsmaßnahmen in Zukunft intensivieren.

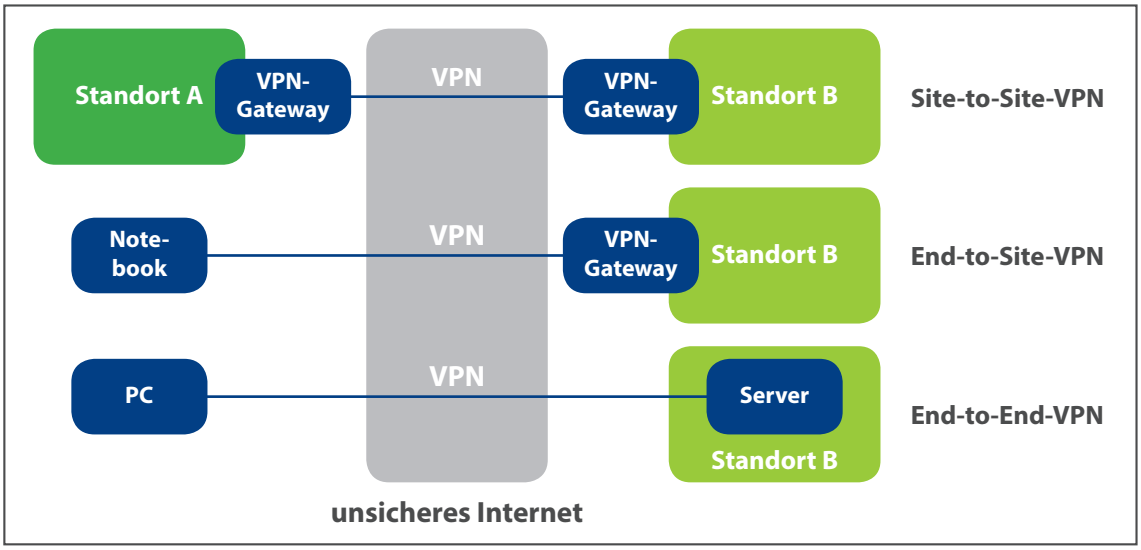
Gibt es Beispiele von bekannt gewordenen Verstößen?

Bislang sind keine Verstöße von Unternehmen bekannt, die zu aufsichtsbehördlichen Maßnahmen geführt haben. Das könnte sich jedoch bald ändern.

Constantin Herfurth arbeitet als Associate bei der Rechtsanwaltskanzlei Eversheds Sutherland. Seine Beratungstätigkeit umfasst das Datenschutz- und IT-Recht.

Quellen und weiterführende Informationen

- **Zur Durchführung von Videokonferenzen: https://ogy.de/BlnBDI-Videokonferenzsysteme**
- **Checkliste für die Durchführung von Videokonferenzen: https://ogy.de/BlnBDI-CL-Videokonferenzsysteme**
- **Nutzung von Messenger- und Videokonferenzdiensten in Zeiten der Corona-Pandemie: https://ogy.de/BfDI-Videokonferenzdienste**
- **Leitfragen zur Beurteilung von Angeboten: https://ogy.de/BfDI-Beurteilung-Angebote**
- **Auswahlhilfe Messenger-Systeme mit Audio-/Videounterstützung: https://ogy.de/BfDI-Auswahlhilfe**
- **Datenschutzfreundliche technische Möglichkeiten der Kommunikation: https://ogy.de/LfDI-BW-Kommunikation**
- **Datenschutz: Plötzlich Videokonferenzen – und nun?: https://ogy.de/ULD-Videokonferenz**
- **Kompendium Videokonferenzsysteme des BSI: https://ogy.de/bsi-koviko; siehe dazu auch die News auf Seite 11**



Die drei verschiedenen VPN-Architekturen

Nicht nur für Homeoffice wichtig

Virtuelle Private Netzwerke (VPN) – ein Überblick

Im Datenschutzalltag taucht im Zusammenhang mit Unternehmensnetzwerken häufig der Begriff „VPN" auf. Was ist das eigentlich genau? Und worauf müssen Verantwortliche achten?

Die Art und Weise, wie Unternehmen und Institutionen heutzutage arbeiten, benötigt einen fast permanenten Zugriff auf die IT-Infrastruktur des Unternehmens. Seien es E-Mails, Kollaborations-Tools oder Dateien: Allen ist gemein, dass sie im Unternehmensnetzwerk gut abgesichert hinter Firewalls und Intrusion-Detection-Systemen vor unbefugtem Zugriff geschützt sind.

Immer mehr Zugriffe von außen notwendig

Sobald aber Mitarbeiter ins Homeoffice gehen, das Unternehmen eine neue Niederlassung an einem anderen Ort gründet oder der Vertriebsmitarbeiter auf Auslandsreise Zugriff auf die interne Datenbank benötigt, stellt sich die Frage, wie sich dies am sichersten umsetzen lässt.

„Früher" ließ sich eine andere Niederlassung in vertretbarer räumlicher Nähe noch über eine dezidierte Verkabelung anbinden. Doch schon damals waren die Kosten hoch und die Bandbreite mäßig. Jetzt ist dieser Ansatz spätestens beim Zugriff beispielsweise aus einem Zug schon rein technisch nicht mehr machbar.

Durchs Internet ins Unternehmensnetz

Es ist also eine Technik erforderlich, die einer abgegrenzten Benutzergruppe Zugang in ein privates Netz gewährt. Kommt dafür nun nicht mehr eine extra verlegte Kabelleitung, sondern das Internet zum Einsatz, das überall auf der Welt kostengünstig und – mehr oder weniger – schnell verfügbar ist, dann spricht man von einem virtuellen Zugang.

Der Zugang über das Internet auf das eigene Netzwerk in einer Art und Weise, dass die IT einer abgegrenzten Benutzergruppe wie z.B. den eigenen Mitarbeitern so zur Verfügung steht, als wäre man mit einer Kabelleitung direkt angeschlossen, heißt folgerichtig Virtuelles Privates Netzwerk, abgekürzt VPN.

VPN-Architekturen

Es gibt im Prinzip drei verschiedene VPN-Architekturen. Sie spiegeln die Art und Weise wieder, wie sich die Anbindung ans Unternehmensnetz verwenden lässt.

Site-to-Site-VPN

Ein Site-to-Site-VPN verbindet zwei (oder mehr) lokale Netzwerke von Unternehmen, meist verteilt auf mehrere Standorte. Im Prinzip kann man sich vorstellen, dass alle Rechner von verschiedenen Standorten auf alle Server und Drucker so zugreifen können, als stünden sie innerhalb eines Gebäudes mit Netzwerkverkabelung. Begriffe wie Gateway-to-Gateway-VPN, Intranet-VPN oder Extranet-VPN sind spezielle Ausprägungen dieser Architektur.

End-to-Site-VPN

Das End-to-Site-VPN ist der typische Anwendungsfall aus dem Homeoffice. Der Zugriff auf das Unternehmensnetz erfolgt von einem Endgerät über das freie Internet (z.B. DSL oder LTE) an ein sogenanntes Gateway des Unternehmens. Dieses Gateway ermöglicht den Zugang zum gesamten Unternehmensnetz. Das Endgerät ist das „End", das Gateway ist meist eine Hardwarelösung, und das gesamte Unternehmensnetzwerk ist die „Site".

End-to-End-VPN

Das End-to-End-VPN ist die Variante, die am seltensten eingesetzt wird. Sie verbin-

det zwei Rechner (daher das „End“) über eine virtuelle Verbindung miteinander. Ein Anwendungsfall: Ein IT-Dienstleister hat Konfigurationszugang zu einem Server im betreuten Unternehmen über einen speziellen Rechner bei sich.

Kommunikation über Protokolle

Tauschen IT-Systeme über Bits und Bytes miteinander Daten aus, gibt es viele verschiedene Vereinbarungen, was diese Informationen zu bedeuten haben – man nennt dies auch ein Protokoll. Am bekanntesten dürfte dabei TCP/IP sein. Aber auch HTTP und TLS fallen in diese Gruppe.

VPN zieht ein virtuelles Kabel, über das diese Protokolle kommunizieren. Man spricht in diesem Zusammenhang auch von „Tunneln“. Denn ein Protokoll schafft einen Kommunikationsweg für viele andere Protokolle. Bei VPN gibt es folgende Varianten:

- PPTP sowie L2TP: Diese Protokolle kommen aus der Zeit der Einwahlverbindungen über Modems und sind heute nicht mehr gebräuchlich.
- IPSec: Dieses Protokoll ist derzeit der De-facto-Standard bei VPN-Technologien. Die virtuelle Leitung wird über das Internet-Protokoll (IP) realisiert. Es ist eine starke Verschlüsselung mit Perfect Forward Secrecy vorhanden, und IPsec wurde bei der Konzeption von IPv6 berücksichtigt. Über IPsec lässt sich auch hardwarenähere Datenkommunikation (z.B. Ethernet) tunneln.
- SSLVPN: Dieses Protokoll verwendet das vom Onlinebanking bekannte Protokoll TLS (früher SSL genannt). Damit lässt sich sowohl der Zugang zu einem gesamten Unternehmensnetz realisieren als auch der Zugang nur zu bestimmten webbasierten Anwendungen, bei denen dann neben dem Browser keine weitere Software nötig ist.

Verschlüsselung ist Pflicht

Ein VPN verbindet mittels eines „virtuellen Kabels“ verschiedene IT-Systeme. Technisch sieht das so aus, dass über das Internet Datenpakete versendet werden. Jeder, der an einem Internetknotenpunkt Zugriff auf diese Datenpakete hätte (z.B. Geheimdienste), könnte den Inhalt der Übertragung mitlesen oder verändern.

Innerhalb eines lokalen Netzwerks im Unternehmen ist es so, dass nicht sämtliche Kommunikation verschlüsselt erfolgt. Daher muss beim „virtuellen Kabel“ VPN eine Verschlüsselung zum Einsatz kommen, die die Vertraulichkeit und Integrität der Datenpakete sicherstellt.

PRAXIS-TIPP

Die heute fast immer eingesetzten Protokolle IPSec und SSLVPN haben eine starke Verschlüsselung integriert und voreingestellt. Es ist aber möglich, sie zu deaktivieren. Das muss nicht mutwillig passieren, sondern geschieht meist aus Versehen. Beispielsweise kommt es zu einem Konfigurationsfehler. Oder die IT vergisst, eine Verschlüsselung, die sie zeitweise zur Fehlersuche unterbrochen hat, wieder zu aktivieren. Es ist also sinnvoll, regelmäßig zu überprüfen, ob die Verschlüsselung wirklich läuft.

Authentifizierung

Beim Aufbau einer VPN-Verbindung muss sichergestellt sein, dass der anfragende Rechner auch wirklich zum berechtigten Personenkreis – etwa „Mitarbeiter im Homeoffice“ – gehört. Hier spricht man dann von einer Authentifizierung. Folgende Varianten stehen dabei zur Verfügung:

Benutzername und Passwort

Diese Form der Authentifizierung ist zwar wirksam, um Unbefugten den Zugang zu verwehren. Allerdings nur so lange, wie diese Unbefugten nicht im Besitz des Passworts sind. Das kann passieren über Brute-Force-Angriffe auf das VPN-Gateway, bei zu schwachen Passwörtern oder wenn Angreifer über Social Engineering auf den Mitarbeiter kommen.

Da mit einem einzigen erfolgreichen Angriff das komplette Unternehmensnetz offen steht, sollten Verantwortliche diese Form nur in Ausnahmefällen verwenden.

Einmal-Passwörter

Bei dieser Variante generiert ein (Hardware-)Token neben einem Benutzernamen und einem Passwort zusätzlich ein Einmal-Passwort. Brute-Force-Attacken auf Einmal-Passwörter laufen nach Sperrung des Zugangs ins Leere. Diese Variante ist empfehlenswert und erfüllt die Anforderung einer Zwei-Faktor-Authentifizierung.

Kryptografische Zertifikate

Eine VPN-Verbindung braucht ein kryptografisches Zertifikat, das mit einem Passwort geschützt z.B. auf einer Chipkarte oder in einer Datei des Rechners liegt. Diese Variante, die ebenfalls unter den Begriff „Zwei-Faktor-Authentifizierung“ fällt, ist die empfehlenswerteste. Sie bringt allerdings einen gewissen Aufwand bei der Verwaltung dieser Zertifikate mit sich.

Endgeräte absichern

Da über ein einziges Endgerät, das über VPN ans Unternehmensnetzwerk angebunden ist, der Zugriff auf das komplette Unternehmensnetz möglich ist – es sei denn, die VPN-Verbindung ist auf gewisse Teilnetze oder Server begrenzt –, müssen die Endgeräte z.B. im Homeoffice gut abgesichert sein. Eine Festplattenvollverschlüsselung, Schutz vor Schadcode und der Verzicht auf Privatnutzung stellen dabei die Mindestvoraussetzung dar.

VPN und DSGVO

Mit dem Einsatz von VPN-Technologien dürfte wohl fast jedes Unternehmen schon in Berührung gekommen sein. Ein Datenschutzthema wird es durch Art. 32 Datenschutz-Grundverordnung (DSGVO). Denn Verantwortliche müssen den wirksamen Einsatz dieser Technologie sicherstellen. Beispiele hierfür sind neben der richtigen Konfiguration und Authentifizierung auch das regelmäßige Einspielen von Sicherheitsupdates auf den VPN-Servern.

Andreas Sachs ist Vizepräsident des Bayerischen Landesamts für Datenschutzaufsicht. Er leitet das Referat, das sich mit dem technischen Datenschutz beschäftigt.

Bild: iStock.com/matejmo

Bei der Verschlüsselung gibt es nicht die eine Lösung. Welche Methode zum Einsatz kommt, hängt u.a. von den Daten ab, um die es geht.

Sicherheit der Verarbeitung

Verschlüsselung: Wann ist welche Methode sinnvoll?

Verschlüsselung gilt als wichtiges Mittel im Kampf gegen Hacker und Datenspione. Der Beitrag stellt die beiden Methoden Transport- und Inhaltsverschlüsselung gegenüber und gibt Ihnen Überlegungen zu einer risikobasierten Auswahl an die Hand.

Als Ergänzung zum Beitrag zu Virtual Private Networks (VPN) auf den vorhergehenden Seiten seien zwei unterschiedliche Ansätze vorgestellt, Daten zu verschlüsseln und so vor dem Zugriff Unbefugter zu schützen.

Transportverschlüsselung

Als Transportverschlüsselung bezeichnet man das Senden von unverschlüsselten Daten über einen verschlüsselten Kanal, auch als Tunnel bezeichnet. Dieser Tunnel baut sich vor dem Senden der Daten auf, die Daten werden in den Tunnel geleitet, und am anderen Ende des Tunnels erscheinen die Daten wieder in lesbarer Form, also im Klartext.

Ein weit verbreitetes Protokoll für verschlüsselte Tunnel ist TLS. TLS kommt häufig bei der Übertragung von Webseiten zum Einsatz und verhindert, dass Fremde etwa beim Online-Banking Daten mitlesen oder sogar manipulieren können.

Inhaltsverschlüsselung

Im Gegensatz dazu steht die Inhaltsverschlüsselung. Hier werden zunächst die Daten verschlüsselt, um anschließend über einen unverschlüsselten Kanal gesendet zu werden. Der Empfänger entschlüsselt die Daten und kann sie dann lesen. Auch hier können Fremde die Daten nicht lesen oder manipulieren.

Protokolle für die Inhaltsverschlüsselung sind beispielsweise PGP und S/MIME. Sie sind besonders im Bereich von E-Mails weit verbreitet. Aber auch wer eine verschlüsselte ZIP-Datei erstellt, verschlüsselt den Inhalt der zugrunde liegenden Daten.

Wo liegen die Unterschiede?

Auf den ersten Blick sieht es so aus, als gebe es zwischen Transport- und Inhaltsverschlüsselung keine großen Unterschiede. Das ist jedoch ein Irrtum. Am Beispiel einer E-Mail lässt sich das leicht sehen.

Transportverschlüsselung: keine echte Ende-zu-Ende-Verschlüsselung

Bei der Transportverschlüsselung baut der Mail-Client einen verschlüsselten Tunnel zu einem Mailserver auf und versendet die Mail. Auf dem Weg vom Client zum Server ist die Mail verschlüsselt. Anschließend wird sie entschlüsselt und liegt auf dem Server im Klartext vor. Nutzt der Server eine Transportverschlüsselung zu einem weiteren Server, baut er einen Tunnel zu diesem Server auf etc.

Eine echte Ende-zu-Ende-Verschlüsselung, also ein durchgehender Tunnel zwischen Sender und Empfänger, lässt sich mit einer Transportverschlüsselung also nur in Ausnahmefällen realisieren.

Inhaltsverschlüsselung: Metadaten werden unverschlüsselt transportiert

Bei der Inhaltsverschlüsselung wird die zu versendende Nachricht, also der „Body" der Mail nebst Anhängen, verschlüsselt und anschließend über einen unverschlüsselten Kanal verschickt. Die Metadaten der Mail, also Sender- und Empfängeradresse sowie der Betreff der Mail, verbleiben im Klartext. So können Dritte sie lesen oder verändern. Die Inhaltsverschlüsselung garantiert allerdings, dass der verschlüsselte Anteil der Mail bis hin zum Empfänger verschlüsselt bleibt. Denn nur dieser kann die Mail entschlüsseln.

Die Lösung: eine Kombination

Beide Verschlüsselungsmethoden haben also ihre Nachteile: Die meist fehlende Ende-zu-Ende-Verschlüsselung bei der Transportverschlüsselung, der unver-

schlüsselte Transport von Metadaten bei der Inhaltsverschlüsselung. Die Kombination beider Verfahren vermeidet die jeweiligen Nachteile, ist aber aufwendig. Dabei hängt es vom Anwendungsszenario ab, ob die Vor- und Nachteile tatsächlich Auswirkungen auf die Sicherheit haben.

Das sei anhand des Online-Bankings verdeutlicht: Ein Kunde verbindet sich mit seinem Browser über eine TLS-Verbindung mit dem Webserver einer Bank. Über diese Verbindung meldet er sich bei der Bank an und führt Transaktionen aus.

Der Webserver der Bank ist über eine TLS-Strecke mit einem Applikationsserver verbunden, der die Banking-Anwendung zur Verfügung stellt. Der Anwendungsserver kommuniziert über verschiedene TLS-Verbindungen mit anderen Servern, die Dienste für das Online-Banking bereitstellen wie etwa Konto-Abfragen. Schließlich wird über eine TLS-Verbindung das sogenannte Core-Banking-System kontaktiert, das die Transaktionen des Benutzers rechtsverbindlich durchführt.

In diesem Beispiel ist eine Transportverschlüsselung prinzipiell ausreichend. Denn es gibt zwar keine Ende-zu-Ende-Verschlüsselung, die beteiligten Banksysteme stehen aber alle im selben Rechenzentrum und sind vertrauenswürdig. Trotzdem kann es sinnvoll sein, für einzelne Daten wie etwa die Kontrollwerte von Passwörtern eine zusätzliche Inhaltsverschlüsselung einzuführen.

Risikobasiert entscheiden

Welche Verfahren zum Einsatz kommen, ist letztlich eine Entscheidung, die risikoorientiert erfolgt:

- Enthalten unverschlüsselt übertragene Metadaten personenbezogene Daten, ist das ein Argument gegen die reine Inhaltsverschlüsselung.
- Auf der anderen Seite stellt die Transportverschlüsselung ein Risiko dar, wenn die Server der diversen TLS-Übertragungsstrecken nicht alle vertrauenswürdig sind. Vertrauenswürdig sind Übertragungsstrecken, wenn sie etwa von der eigenen Institution oder von einem Provider, der nach ISO 27001 zertifiziert ist, betrieben werden.

Um die Risiken abzuschätzen, ist es sinnvoll, die Daten nach Risiken (Schutzklassen) zu klassifizieren. Eine Bank könnte die Daten einteilen nach „öffentliche Informationen" (Stufe C1), „interne Informationen für die Mitarbeiter" (C2), „Kunden- und Transaktionsdaten" (C3) sowie „Authentifizierungs- und PIN-Kontrolldaten" (C4):

- Die öffentlichen Informationen unterliegen keinen Beschränkungen.
- Interne Daten sind unverschlüsselt, aber nur im Intranet verfügbar.
- Kunden- und Transaktionsdaten können unverschlüsselt in Datenbanken liegen, müssen aber bei jedem Transport verschlüsselt werden.
- Daten der höchsten Vertraulichkeitsstufe müssen grundsätzlich per Inhaltsverschlüsselung verschlüsselt sein.

Im Beispiel der Bank gibt es keine Metadaten, die bei einer reinen Inhaltsverschlüsselung von C4-Daten im Klartext transportiert werden. Sind solche Metadaten vorhanden, muss die Anforderung für die höchste Schutzklasse lauten: Transport- UND Inhaltsverschlüsselung.

PRAXIS-TIPP

Beim Thema Transport- und Inhaltsverschlüsselung gibt es keinen Königsweg. Beide Verfahren haben ihre Vor- und Nachteile, und die Verfahren zu kombinieren, ist oft aufwendig. Deshalb ist es sinnvoll, risikobasiert auszuwählen. Damit lassen sich die eigenen Anforderungen an Datenschutz und Informationssicherheit realisieren, ohne mehr Aufwand als nötig zu betreiben.

Dr.-Ing. Markus a Campo arbeitet als unabhängiger Berater, Auditor und Gutachter im Bereich der Informationssicherheit.

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, Wolfgang Materna

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

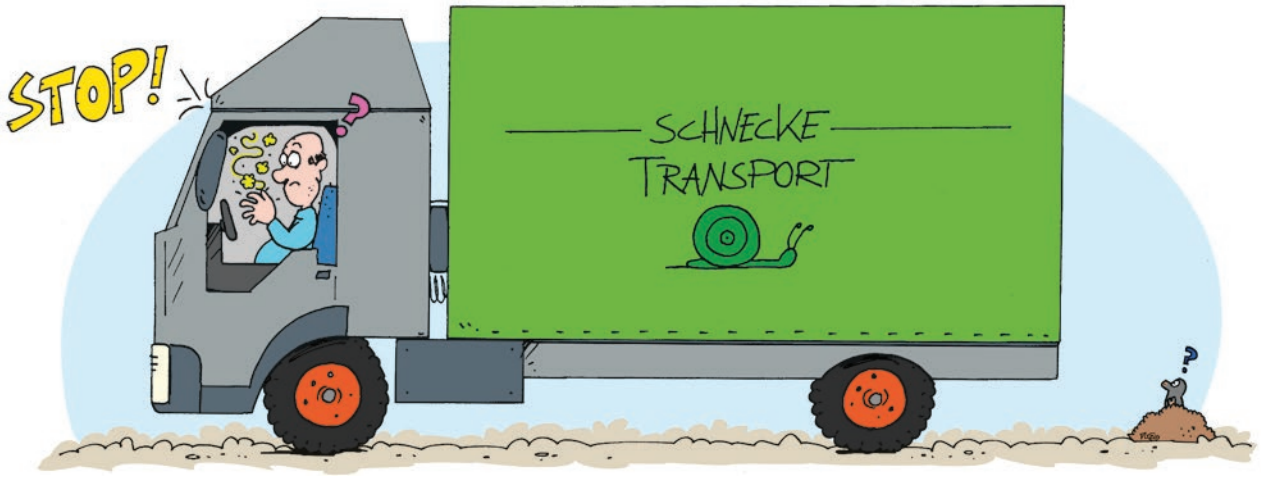
Layout & Satz:
metamedien
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4078

ISSN-Nr.:
1614-6867

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

Haftung:
Die WEKA MEDIA GmbH & Co. KG ist bemüht, ihre Produkte jeweils nach neuesten Erkenntnissen zu erstellen. Die inhaltliche Richtigkeit und Fehlerfreiheit wird ausdrücklich nicht zugesichert.
Bei Nichtlieferung durch höhere Gewalt, Streik oder Aussperrung besteht kein Anspruch auf Ersatz. Erfüllungsort und Gerichtsstand ist Kissing. Zum Abdruck angenommene Beiträge und Abbildungen gehen im Rahmen der gesetzlichen Bestimmungen in das Veröffentlichungs- und Verbreitungsrecht des Verlags über. Für unaufgefordert eingesandte Beiträge übernehmen Verlag und Redaktion keine Gewähr. Namentlich ausgewiesene Beiträge liegen in der Verantwortlichkeit des Autors. Datenschutz PRAXIS und alle in ihr enthaltenen Beiträge und Abbildungen sind urheberrechtlich geschützt. Jeglicher Nachdruck, auch auszugsweise, ist nur mit ausdrücklicher Genehmigung des Verlags und mit Quellenangabe gestattet.



Verhaltens- und Leistungskontrolle

Alkolock – das andere Homeoffice

Manchmal haben die Hygienemaßnahmen, die im Zuge der Corona-Pandemie notwendig sind, überraschende Folgen. So geschehen in einem Fuhrpark, den die Desinfektionsmittel fast lahmgelegt hätten.

Alkohol am Steuer ist ein häufiges Verkehrsdelikt. Leider sind zu viele Fahrer von Kleintransportern, Lieferwagen und größeren Lkw alkoholisiert unterwegs. Ab 2022 sollen daher EU-weit neue Fahrzeugklassen, ab 2024 dann alle Neuwagen mit Alkolock ausgestattet sein.

So funktioniert Alkolock

Die meisten der Geräte funktionieren durch direktes Pusten. Dafür braucht man jedes Mal ein neues Mundstück. Daher wird auch mit Luftmessgeräten für die Umgebung des Fahrers getestet. Sie sind jedoch nicht so genau wie die „Röhrchen".

Gemeinsam haben die Geräte eines: Das Fahrzeug lässt sich nicht starten, wenn der Alkoholgehalt in der Luft zu hoch ist. Das wird übrigens zunehmend auch ein Thema für Datenschutzbeauftragte werden. Stichwort: besondere Kategorien personenbezogener Daten von Beschäftigten und Kontrolle von Verhalten und Leistung.

Bereits heute im Einsatz

Mitunter ist in so manchem Fuhrpark Messtechnik dieser Art schon heute im Einsatz. Mit gutem Ergebnis, denn die Zahl alkoholbedingter Unfälle ist dort tatsächlich deutlich zurückgegangen.

Alkohol ist auch im Desinfektionsmittel!

Zusätzlich gibt es in Fuhrparks Tests, um die besten Messmethoden herauszufinden. Und das hätte in Zeiten von Corona für einen Fuhrparkleiter beinahe den Stillstand bedeutet. Denn die Fahrer hatten die Order bekommen, die Hände gut mit Desinfektionsmittel einzureiben. Das haben sie auch eifrig getan. Der Alkoholgehalt, der von der Händedesinfektion verdunstete, war offenbar so intensiv, dass der Alkolock automatisch eingriff und sich einzelne Fahrzeuge daher nicht starten ließen.

Einer der Fahrer freute sich schon: „Wenn schon kein Homeoffice, dann wenigstens Alkolock!" Doch daraus wurde nichts – die Wegfahrsperre ließ sich, da sich das Ganze in der Testphase befand, deaktivieren.

Eberhard Häcker ist seit vielen Jahren externer Datenschutzbeauftragter. Da er in zahlreichen verschiedenen Branchen berät, ist sein Erfahrungsschatz riesig.

IN DER NÄCHSTEN AUSGABE

„Datenschutz-Helfer" KI-Chips

Anwendungen, die mit KI-Verfahren arbeiten, sind eine Datenschutz-Herausforderung. KI-Chips könnten das ändern.

Analoge Schließsysteme

Analoge Schließsysteme, sprich die guten alten Schlüssel, sind in vielerlei Hinsicht ein Thema für den DSB.

Corona-App & Privacy by Design

Wie funktioniert praxisnaher und wirksamer technischer Datenschutz? Anhand der Tracing-App lässt sich das gut zeigen.