www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

Rechtssicher | vollständig | dauerhaft

Juli 2024

Bild: iStock.com/mixmagic

Auch wenn DSB nicht direkt für die Umsetzung von Data Act & Co. verantwortlich sind, werden sie nicht darum herumkommen, sich mit diesen Themen zu beschäftigen

Zahlreiche EU-Rechtsakte parallel zur DSGVO

EU-Datenwirtschaftsrecht: Welche Rolle haben DSB?

Das Datenwirtschaftsrecht der EU befasst sich wenig überraschend mit der Verarbeitung von Daten. Es ist jedoch in seinen Zielen nicht deckungsgleich mit dem Datenschutzrecht. Datenschutzbeauftragten kommt bei der Umsetzung dennoch eine Schlüsselrolle zu.

Im Rahmen ihrer Datenstrategie hat die EU eine Reihe neuer Rechtsakte geschaffen, die sich mit dem Umgang mit Daten befassen, aber jeweils verschiedene Ziele und Zielgruppen adressieren.

Das EU-Datenwirtschaftsrecht – ein Überblick

Der **Digital Services Act (DSA)** und der **Digital Markets Act (DMA)** adressieren digitale Dienste und nehmen deren Anbieter in die Pflicht. Der **Data Act (DA)** und der **Data Governance Act (DGA)** haben vereinfacht gesagt die Bereitstellung von Daten für Dritte zum Gegenstand – das „Sharing" (wörtlich: Teilen) von Daten.

Ähnlich wie Art. 20 Datenschutz-Grundverordnung (DSGVO) haben diese Regelungen eher einen regulierungsrechtlichen („kartellrechtlichen") Charakter. Sie richten sich aber auch an den Datenschutz und gehen zum Schutz personenbezogener Daten über die DSGVO hinaus. Gleichwohl steht das „Sharing" grundsätzlich im Widerspruch zu diesem Schutz personenbezogener Daten.

Mehrere EU-Gesetze und -Richtlinien zielen darauf ab, die Cybersicherheit in der EU zu stärken. Sie unterstützen damit in gewissem Umfang den Datenschutz. Dazu zählen die **Network and Information Security Directive 2 (NIS-2-Richtlinie)** und ihr nationales Umsetzungsgesetz, der **Cyber Resilience Act (CRA),** der **Digital Operational Resilience Act (DORA)** sowie die **Critical Entities Resilience Directive (CER-Richtlinie).**

Eine Sonderstellung nimmt der **Artificial Intelligence Act (AI Act)** ein. Er reguliert die gesamte Wertschöpfungskette der Künstlichen Intelligenz (KI). Im Mittelpunkt steht die Regulierung der sogenannten KI-Systeme. Es handelt sich um ein „Risikobeherrschungsgesetz": Der AI Act lässt Risiken zu, schafft aber →

Editorial

Ricarda Veidt, Chefredakteurin

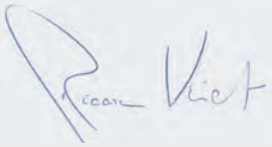
Orientierung im KI- & EU-Dschungel

Liebe Leserin, lieber Leser! Nun haben sich nicht nur einzelne Aufsichtsbehörden zum Thema „Künstliche Intelligenz" geäußert, sondern auch die Datenschutzkonferenz als Ganzes. In ihrer Orientierungshilfe, die Dr. Ehmann auf Seite 10 vorstellt, liefert sie einige Leitplanken und Empfehlungen für Verantwortliche, die KI-Anwendungen einsetzen möchten (https://datenschutzkonferenz-online.de/orientierungshilfen.html).

Viele Datenschutzbeauftragte wünschen sich mehr Orientierung auch in Bezug auf die vielen neuen EU-Rechtsakte wie etwa den AI Act. Im Titelbeitrag ordnet Dr. Eckhardt daher die mögliche Rolle von DSB zwischen DSGVO und EU-Datenwirtschaftsrecht ein. Klar ist: DSB werden nicht darum herumkommen, sich mit diesen Verordnungen und Richtlinien zu befassen. Wir werden aus diesem Grund die weitere Entwicklung verfolgen und regelmäßig berichten.

Und wenn es zur Abwechslung auch mal etwas handfester werden soll: Greifen Sie doch einfach zur Analogen Intelligenz, so wie unser Datenschutzbeauftragter im Daten-Schluss!

Herzliche Grüße
Ihre Ricarda Veidt



Anforderungen, um diese zu beherrschen. Der Schutz personenbezogener Daten steht dabei nicht im Vordergrund. So gesehen existieren der AI Act und die DSGVO nebeneinander. Allerdings sieht der AI Act ausdrücklich „Verzahnungen" mit der DSGVO vor.

WICHTIG

Die Rechtsakte haben etwas gemeinsam: Zwar regeln sie selbst nicht unmittelbar die Verarbeitung personenbezogener Daten. Doch um die Pflichten zu erfüllen, die sich aus den Rechtsakten ergeben, ist es erforderlich, auch personenbezogene Daten zu verarbeiten. Diese Aktivitäten müssen den Anforderungen der DSGVO entsprechen.

Wie ist das Verhältnis der DSGVO zu den EU-Rechtsakten?

Die EU-Rechtsakte unterscheiden insbesondere zwischen Daten (vgl. Art. 2 Nr. 1 DA), personenbezogenen Daten (vgl. Art. 2 Nr. 3 DA) und nicht-personenbezogenen Daten (vgl. Art. 2 Nr. 4 DA). Dabei ist jeweils definiert, was der Rechtsakt unter dem Begriff versteht. Für das Datenschutzrecht ist daher zunächst zu ermitteln, ob es überhaupt anwendbar ist, sprich ob es um die Verarbeitung personenbezogener Daten geht (zum Personenbezug siehe Eckhardt, Heft 11/2023, Seite 14 ff.).

Ist das der Fall, gilt es, im nächsten Schritt aus Sicht der DSGVO die datenschutzrechtliche Rolle der Personen zu klären, die der jeweilige Rechtsakt zum Handeln verpflichtet: Sind sie

- Verantwortliche (Art. 4 Nr. 7 erste Alternative DSGVO),
- Joint Controller (Art. 4 Nr. 7 zweite Alternative DSGVO) oder
- Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO)?

Daraus ergeben sich unabhängig von diesen neuen Rechtsakten die Anforderungen zum Datenschutz.

Was passiert, wenn es unterschiedliche Regelungen gibt?

Jeder dieser Rechtsakte regelt sein Verhältnis zur DSGVO eigenständig und unterschiedlich. Das reicht von einem „unbeschadet" über „unberührt" bis hin zu einem Vorrang im Konfliktfall. Art. 1 Abs. 7 AI Act lässt die Datenschutzrechtsakte der EU unberührt. Das Gesetz hebt deren Regelungen in den Erwägungsgründen 94 und 140 AI Act hervor. Auch Art. 2 Abs. 4 Buchst. g und Erwägungsgrund 10 Abs. 2 DSA regeln dies so. Dabei bleibt die Frage offen, wie es sich verhält, wenn die Anforderungen nach dem DSA strenger sind als nach der DSGVO.

Laut DMA müssen die Torwächter, also die Plattformbetreiber mit erheblichem Einfluss auf den Binnenmarkt, sicherstellen, dass die Maßnahmen zur Einhaltung des DMA mit dem EU-Datenschutzrecht „im Einklang" stehen (Art. 8 Abs. 1 Satz 3 DMA). Der DMA gilt aber „unbeschadet" dieser Vorschriften (Erwägungsgrund 12 DMA). Der DA gilt ebenfalls „unbeschadet" des EU-Datenschutzrechts, aber im Fall eines Widerspruchs soll der Schutz personenbezogener Daten und der Privatsphäre Vorrang haben (Art. 1 Abs. 5 DA). Auch der DGA regelt das Verhältnis des Gesetzes zum Datenschutzrecht in seinem Art. 1 Abs. 3.

Und was heißt das nun konkret? Hier beginnt eine stark von der EU-Rechtslage geprägte Auslegung. Sie orientiert sich an der bisherigen Rechtsprechung des Europäischen Gerichtshofs (EuGH). Dies betrifft die Frage, wann überhaupt ein Konflikt zwischen verschiedenen EU-Rechtsakten vorliegt. Diese Fragen sind noch nicht auf ausgetretenen Pfaden geklärt, sondern bedürfen vertiefter rechtlicher Analysen.

Welche Aufgaben können DSB übernehmen?

Die neuen EU-Rechtsakte richten sich nicht an die DSB. Das überrascht nicht. Auch die DSGVO nimmt nicht die DSB in die Pflicht, personenbezogene Daten zu schützen, sondern die Verantwortlichen (Art. 4 Nr. 7 DSGVO) und die Auftragsverarbeiter (Art. 4 Nr. 8 DSGVO).

Die Aufgaben von DSB sind in Art. 39 DSGVO definiert. Sie lassen sich vereinfacht auf Beratung, Unterstützung und Überwachung herunterbrechen. Bereits Art. 39 DSGVO stellt klar, dass es sich nicht um eine abschließende Aufzählung handelt. Verantwortliche können DSB also weitere Aufgaben übertragen. Dies ist in der Praxis auch regelmäßig der Fall. Die Grenze hierfür ergibt sich aus Art. 38 Abs. 6 DSGVO: Die anderen Aufgaben und die als DSB dürfen nicht zu einem Interessenkonflikt führen.

Grenze für weitere Aufgaben: Interessenkonflikte

Datenschutzbeauftragte tragen nicht die Verantwortung dafür, dass die Verantwortlichen und Auftragsverarbeiter den Datenschutz umsetzen und einhalten. Vielmehr unterstützen sie diese im Rahmen der Art. 39 und 35 Abs. 3 DSGVO lediglich dabei, den Datenschutz umzusetzen und einzuhalten. Dementsprechend haften DSB auch nicht dafür, wenn das Unternehmen, für das sie tätig sind, den Datenschutz nicht einhält. Sie haften nur, wenn sie ihre Pflichten nach Art. 37 bis 39 DSGVO verletzen.

Hieraus ergibt sich zunächst, dass DSB jedenfalls nicht originär für die Umsetzung und Einhaltung der Pflichten aus den neuen EU-Rechtsakten zuständig und verantwortlich sind, auch wenn diese die Datenverarbeitung adressieren und erfordern. Die DSGVO schließt allerdings nicht von Vornherein aus, dass DSB Funktionen übernehmen, die in diesen neuen EU-Rechtsakten vorgesehen sind, oder an deren Umsetzung mitwirken.

Auf den ersten Blick ist jedoch ein Interessenkonflikt möglich. Denn diese Rechtsakte enthalten nicht nur strengere Anforderungen als die DSGVO (z.B. Art. 26 und 28 DSA), sondern auch parallele Anforderungen. Hinzu kommt: Für die Umsetzung der Pflichten nach den neuen Rechtsakten gilt nicht die Weisungsfreiheit, die Art. 38 Abs. 3 Satz 1 DSGVO für DSB vorsieht.

Mit Ausnahme der NIS-2-Richtlinie handelt es sich bei den genannten Rechtsakten sämtlich um EU-Verordnungen. Die DSGVO hat daher nicht automatisch Vorrang. Jeder dieser Rechtsakte regelt sein Verhältnis zur DSGVO individuell. Die Frage, welche der Richtlinien bzw. Verordnungen Vorrang hat, kann eine Rechtsberatung erfordern, die auf Rechtsakten außerhalb der DSGVO beruht. Deshalb müssen DSB auch die Grenzen zulässiger Rechtsberatung nach dem Rechtsdienstleistungsgesetz beachten.

Beraten und unterstützen

Den DSB kann bei der Umsetzung dieser neuen Rechtsakte (dennoch) eine zentrale Rolle zukommen. Denn Unternehmen und Organisationen müssen insoweit das Datenschutzrecht anwenden und die Verpflichtungen beachten, die sich daraus ergeben. Hier kommt die Beratungs- und Unterstützungspflicht von DSB zum Tragen. Sie tun daher gut daran, wenn sie sich mit den Rechtsakten – zumindest aus der Perspektive der DSGVO – vertraut machen.

Anknüpfungspunkte identifizieren

Zunächst heißt es, die Anknüpfungspunkte dieser Rechtsakte zu identifizieren. Im Fall des AI Acts erfolgt dies z.B. anhand der Frage: Wo kommen KI-Systeme zum Einsatz? Dabei kann dem oder der DSB eine zentrale Rolle zukommen.

Die Rechtsakte, v.a. der AI Act, sehen auch Schnittpunkte und Verzahnungen mit der DSGVO vor (vgl. Art. 5, 26, 27 AI Act). Dies gilt v.a. im Hinblick darauf, ein Verzeichnis von Verarbeitungstätigkeiten zu führen, Transparenzpflichten zu erfüllen und Folgenabschätzungen durchzuführen.

Können DSB auch für die Umsetzung zuständig sein?

Die Frage steht im Raum, ob DSB auch dafür zuständig und verantwortlich sein können, die neuen Rechtsakte in Personalunion umzusetzen – jedenfalls dann, wenn sie über keinen personellen Unterbau verfügen. Dies muss eine Organisation im Einzelfall abwägen.

Dabei ist allerdings ein Punkt zu bedenken: In diesem Bereich gelten die Haftungsprivilegien, die Weisungsfreiheit und auch der Schutz vor Benachteiligung der DSGVO nicht bzw. nicht zwingend. Dies ist auch in anderen Konstellationen der Fall: DSB beraten bei der Frage, wie sich Vorgaben des Steuerrechts datenschutzkonform umsetzen lassen. Hingegen beraten sie nicht bezüglich der Steuergestaltung im Unternehmen.

PRAXIS-TIPP

Zusammengefasst kann den DSB eine Schlüsselrolle zukommen, wenn es darum geht, das EU-Datenwirtschaftsrecht im Einklang mit dem (Datenschutz-)Recht umzusetzen. DSB sind jedoch weder für die Umsetzung der neuen Rechtsakte noch für die Umsetzung der DSGVO zuständig oder verantwortlich. Sie begleiten vielmehr diesen Prozess, indem sie die Verantwortlichen beraten, kontrollieren und überwachen.

Dr. Jens Eckhardt ist Rechtsanwalt und Partner bei pitc legal Eckhardt Rechtsanwälte Partnerschaft mbB in Düsseldorf.

Bild: iStock.com/guvendemir

Digitale Lernsysteme zur Unterweisung der Mitarbeitenden im Datenschutz werden immer populärer. Beziehen Sie auf jeden Fall frühzeitig den Betriebsrat in die Erarbeitung des Schulungskonzepts ein.

Awareness-Training

Anforderungen an ein Datenschutz-Schulungskonzept

Zu den wesentlichen datenschutzrechtlichen Pflichten gehört die Schulung von Beschäftigten. Zum Nachweis der ordnungsgemäßen Umsetzung bietet sich ein Schulungskonzept an.

Auch wenn normalerweise der Arbeitgeber für Datenverarbeitungen in seinem Unternehmen verantwortlich ist (Art. 4 Nr. 7 Datenschutz-Grundverordnung – DSGVO), obliegt es seinen Beschäftigten, die Vorschriften aus den geltenden Datenschutzbestimmungen in der Praxis umzusetzen. Die Beschäftigten agieren dabei als „unterstellte Personen" (Art. 29 DSGVO) und dürfen personenbezogene Daten im Rahmen ihrer beruflichen Tätigkeit nur auf Weisung des Arbeitgebers verarbeiten.

Der Arbeitgeber ist wiederum gemäß Art. 32 Abs. 4 DSGVO dazu verpflichtet, sicherzustellen, dass ihm unterstellte Personen mit Zugang zu personenbezogenen Daten die Datenverarbeitungen nur auf Anweisung durchführen. Neben einer entsprechenden Verpflichtung, die datenschutzrechtlichen Vorgaben einzuhalten, sollten Arbeitgeber die Beschäftigten daher regelmäßig im Datenschutzrecht schulen.

PRAXIS-TIPP

Bereits zu Beginn des Arbeitsverhältnisses sind Beschäftigte auf die Einhaltung des Datengeheimnisses und die Umsetzung der Grundsätze für die Verarbeitung personenbezogener Daten aus Art. 5 Abs. 1 DSGVO zu verpflichten. Auch sollte der Bereich Datenschutz insbesondere bei Beschäftigten, die häufig mit personenbezogenen Daten in Berührung kommen, Teil des Onboarding-Prozesses sein.

Welche rechtlichen Regelungen gibt es?

Zum Detailgrad von Schulungsmaßnahmen oder deren Häufigkeit enthalten die DSGVO und die derzeitigen Regelungen zum Beschäftigtendatenschutz im Bundesdatenschutzgesetz (BDSG) keine konkreten Angaben. Ebenso ist dort nicht definiert, ob eine Awareness durch eine Präsenzschulung, im Rahmen eines Webinars oder durch ein eLearning erlangt werden soll.

Zusätzlich zu Art. 32 DSGVO – der Verpflichtung, angemessene technische und organisatorische Maßnahmen (TOM) zum Datenschutz zu treffen – gilt es in diesem Zusammenhang den Wortlaut von Art. 39 DSGVO zu beachten: Er beschreibt die Aufgaben von Datenschutzbeauftragten (DSB) und benennt u.a. die „Überwachung der Einhaltung dieser Verordnung, […] sowie der Strategien des Verantwortlichen oder des Auftragsverarbeiters für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen" (Art. 39 Abs. 1 Buchst. b DSGVO). Dadurch stellt der Artikel indirekt den Aufbau einer Schulungsstrategie als Pflicht des Verantwortlichen bzw. des Arbeitgebers klar.

Wie lässt sich ein Schulungskonzept im Unternehmen integrieren?

Arbeitgeber sollten daher – in Abstimmung mit dem oder der Datenschutzbeauftragten – ein Schulungskonzept festlegen. Dieses kann z.B. definieren, dass neue Beschäftigte bereits während des Onboardings im Datenschutz unterrichtet werden. Außerdem kann es beschreiben, auf welche Art und Weise und mit welchen Inhalten die Sensibilisierung durchzuführen ist und wie oft und wann sie wiederholt wird. Auch ist zu prüfen, für welche Gruppe von Beschäftigten eine einfache Grundsensibilisierung aufgrund des Tätigkeitsfelds nicht ausreicht.

Für Mitarbeitende, für die eine Verarbeitung von teils sensiblen personenbezogenen Daten alltäglich ist, sind zusätzliche Spezialschulungen sinnvoll. Diese bieten sich etwa für die folgenden Bereiche an:

- Personalabteilung: Fokusschulungen im Beschäftigtendatenschutz
- IT-Abteilung: Fokusschulungen für TOM, idealerweise durch einen IT-Sicherheitsexperten
- Marketing-Team: Fokusschulungen zu Webseiten, Social Media, Direktwerbemaßnahmen
- Vertrieb: Fokusschulungen zu Akquisen, Direktwerbung

Das Schulungskonzept lässt sich grundsätzlich in einer internen Arbeitsanweisung (Standard Operating Procedure, SOP) oder Richtlinie verankern oder durch Konzepte des Qualitätsmanagements oder eine entsprechende ISO-Zertifizierung sicherstellen.

PRAXIS-TIPP

Neben einem festen Schulungsplan sollten Sie als DSB immer aktuelle Entwicklungen im Auge behalten. Derzeit könnte künstliche Intelligenz (KI) ein Thema in Ihrem Unternehmen sein, das datenschutzrechtliche Fragen aufwirft und dem der Arbeitgeber daher mit Schulungen und Sensibilisierungsmaßnahmen begegnen sollte.

Neben geplanten, regelmäßigen Sensibilisierungsmaßnahmen sind rechtliche und praktische Entwicklungen einzubeziehen. Ein gutes Beispiel stellt der Trend zu Homeoffice und mobilem Arbeiten dar. Sofern den Beschäftigten derartige Möglichkeiten angeboten werden, sollte das Schulungskonzept um Sensibilisierungen zum Datenschutz abseits der Büroräumlichkeiten ergänzt werden. Auch technische Änderungen, neue Gesetze, bedeutende Urteile oder aufsichtsbehördliche Stellungnahmen können zu einem erneuten Schulungsbedarf und zur Aktualisierung der Schulungsinhalte führen. Daher sollten Arbeitgeber auch kurzfristig Maßnahmen ergreifen können, um die Einhaltung datenschutzrechtlicher Vorgaben durchgängig sicherzustellen.

Schulungskonzept	Ja	Nein
Erfolgt eine Grundsensibilisierung neuer Beschäftigter?	☐	☐
Bestehen Vorgaben zum zeitlichen Rhythmus von Grundsensibilisierungen?	☐	☐
Werden die Schulungsinhalte regelmäßig kontrolliert und aktualisiert?	☐	☐
Wird auf neue rechtliche und praktische Entwicklungen eingegangen?	☐	☐
Wird die aktive Teilnahme durch Prüffragen oder Aufgaben gefördert?	☐	☐
Werden Spezial-/Fokusschulungen angeboten?	☐	☐
Werden Tools externer Dienstleister eingesetzt? Bestehen Verträge zur Auftragsverarbeitung sowie ggf. Grundlagen für Datentransfers gemäß Art. 44 ff. DSGVO (bei Dienstleistern aus Drittländern)	☐	☐
Ist das Schulungskonzept dokumentiert?	☐	☐
Wird die Teilnahme aller Beschäftigten sichergestellt?	☐	☐
Wird die individuelle Teilnahme dokumentiert?	☐	☐
Wird ein Teilnahmenachweis für drei Jahre abgelegt?	☐	☐

Checkliste für ein Schulungskonzept zum Datenschutz. Die Checkliste finden Abonnentinnen und Abonnenten unter www.datenschutz-praxis.de/datenschutzbeauftragte/checkliste-datenschutzschulungskonzept.

Wie lassen sich Schulungen nachweisen und dokumentieren?

Um den Rechenschaftspflichten aus der DSGVO nachzukommen (Art. 24 Abs. 1 DSGVO, Art. 5 Abs. 2 DSGVO), sollten Arbeitgeber einen individuellen Nachweis der Teilnahme an den Schulungen führen können. Dieser Nachweis sollte nur die erforderlichen Daten zur Person enthalten, um dem Grundsatz der Datenminimierung nachzukommen (Art. 5 Abs. 1 Buchst. c DSGVO). In der Regel genügen Titel, Inhalt und Datum der Schulung sowie der Name des Beschäftigten und eventuell dessen Tätigkeitsbereich. Die Teilnahmenachweise sollten gemäß dem „Need-to-know-Prinzip“ für drei Jahre sicher abgelegt werden.

Außerdem muss der Arbeitgeber die Beschäftigten im Fall einer Verarbeitung ihrer personenbezogenen Daten durch die Dokumentation der Teilnahme datenschutzrechtlich gemäß Art. 13 DSGVO informieren. Er muss u.a. über den Zweck der Datenverarbeitung, die Dauer der Datenspeicherung und die Datenempfänger aufklären. Dementsprechend ist zu prüfen, inwiefern externe Dienstleister in die Prozesse eingebunden sind, wenn der Verantwortliche etwa ein Schulungstool einkauft. Hierbei könnten der Abschluss eines Auftragsverarbeitungsvertrags und eine Prüfung erforderlich sein, ob das Datenschutzniveau angemessen ist. Sofern ein Learning Management System (LMS) flächendeckend zum Einsatz kommt, wäre vorab ein diesbezügliches Zugriffs- und Berechtigungskonzept festzulegen.


Conrad S. Conrad ist Volljurist und Senior Berater Datenschutz bei der datenschutz nord GmbH in Hamburg.
Elena Folkerts, M.A. ist dort Senior Beraterin Datenschutz.

Um als DSB wirksam und kundenfreundlich zu beraten, brauchen Sie ein Verständnis für das Interesse des Gegenübers und nachvollziehbare Argumente. Beides liefert dieser Best-Practice-Beitrag

Bild: vom Autor auf einem eigenen KI-System generiert

Datenspeicherung

Die Protokollierung von IP-Adressen in Server-Logs

Ungekürzte Netzwerkadressen von Website-Besuchern in Protokolldateien zu speichern, ist diskussionswürdig, u.a. weil die Website-Anbieter auf diese Weise anlasslos personenbezogene Daten erfassen (Stichwort Vorratsdatenspeicherung). Welche Vorgehensweise können Sie als DSB stattdessen empfehlen?

Es begann im Jahr 2016, als der Europäische Gerichtshof (EuGH) entschied, dass selbst dynamische Netzwerkadressen als personenbezogene Daten anzusehen sind (Urteil vom 19.10.2016 – C-582/14). Der Bundesgerichtshof (BGH) bestätigte diese Rechtsauffassung im Jahr 2017 (Urteil vom 16.05.2017 – VI ZR 135/13). Netzwerkadressen werden auch als IP-Adressen bezeichnet. IP steht dabei für Internet Protocol.

Für Webseitenbetreiber ist es verführerisch, einfach die Netzwerkadresse jeder Person, die die Seite besucht, zu speichern. Immerhin lässt sich diese Adresse für die Gefahrenabwehr nutzen. Manche verwenden sie auch, um Nutzer voneinander zu unterscheiden und sie so besser kennenzulernen. Das wird auch als Web-Analyse bezeichnet.

Nachfolgend sind verschiedene **Motivationen** beschrieben, **die IP-Adressen von Webseitenbesuchern in Server-Logs zu speichern**. Anschließend wird das **Konzept des Anlasses** beschrieben und welchen **Nutzen** IP-Adressen in Server-Logs tatsächlich mit sich bringen sowie welche **Alternativen** bestehen. Es folgt eine **Einordnung** der Speicherung von IP-Adressen **aus dem Blickwinkel des berechtigten Interesses**. Nicht zuletzt schließen sich **Empfehlungen für Datenschutzbeauftragte** (DSB) und die Beratung ihrer Mandantinnen und Mandanten an.

Darum werden Netzwerkadressen in Server-Logs gespeichert

Es gibt eine Reihe von möglichen Gründen und Motivationen, die IP-Adressen von Webseiten in Server-Logs zu erfassen.

Vorgabe des Providers

Die wahrscheinlich häufigste Ursache, ungekürzte IP-Adressen in Server-Protokollen zu speichern, sind die Provider und Hoster der Webserver. Diese Anbieter haben schlichtweg ihr System oft so konfiguriert, dass die IP-Adressen der Website-Besucher automatisch in Server-Logs landen.

Kurz erklärt

Wozu dienen IP-Adressen?

Jede Zwei-Wege-Kommunikation setzt voraus, dass Absender und Empfänger wissen, wie sie einander erreichen, um Nachrichten auszutauschen.

Im Fall einer Webseite ist der Nutzer der Absender der Anfrage, eine Webseite ansehen zu wollen. Dieser Nutzer gibt in den eigenen Browser die Adresse der gewünschten Webseite ein oder ruft sie über eine Trefferliste aus einer Suchmaschine heraus auf. Dafür muss er die Adresse der Webseite kennen. Meistens kommen symbolische Namen zum Einsatz, wie z.B. www.datenschutz-praxis.de. Hinter diesen symbolischen Namen verbirgt sich immer eine IP-Adresse. Der symbolische Name hat einen praktischen Nutzen, weil er sich leichter merken lässt als eine längere Zahlenfolge.

Die Webseite empfängt dann die Anfrage des Nutzers oder der Nutzerin. Genauer gesagt ist der Empfänger der Server, auf dem die Webseite läuft. Damit der Server den Inhalt der Webseite an die anfragende Person zurücksenden kann, muss deren Adresse bekannt sein. Diese Adresse ist die Netzwerk- bzw. IP-Adresse des Nutzers bzw. die seines Rechners.

Deswegen wird bei jeder Anfrage über das Internetprotokoll automatisch die Adresse des Absenders an den Empfänger der Anfrage übermittelt. Der Empfänger kann dann seine Antwort an die Absenderadresse zurückschicken und somit die Anfrage des Absenders erfüllen.

Der Aufruf einer Webseite oder onlinefähigen App basiert also auf dem Austausch von Nachrichten zwischen Nutzenden und Anwendung wie Webseite oder App. Dieser Nachrichtenaustausch wiederum ist nur möglich, wenn die Netzwerkadressen der Kommunikationspartner bekannt sind.

Als Beispiel sei eine IP-Adresse (IPv4) genannt: 10.20.30.40. Es handelt sich um vier Blöcke mit je einer Zahl, die Werte zwischen 0 und 256 annehmen kann. Die theoretische Anzahl der Kombinationen beträgt also 256*256*256*256 = rund 4,3 Milliarden verschiedene Werte. Jede Netzwerkadresse muss eindeutig sein. Wenn sie zu einem gegebenen Zeitpunkt nicht eindeutig wäre, würden sich mehrere Nutzer beim Aufrufen von Webseiten gegenseitig beeinflussen.

Eine ungekürzte IP-Adresse bleibt in Originalform erhalten. Spricht man von gekürzten IP-Adressen, dann ist der letzte Zahlenblock ausgenullt, also 10.20.30.0 statt 10.20.30.40. Bis zu 256 IP-Adressen haben somit den gleichen Wert, wenn sie derart gekürzt in Server-Logs gespeichert werden.

Betrugserkennung und Gefahrenabwehr

In das Themenfeld Betrugserkennung und Gefahrenabwehr spielen auch Tatbestände wie Hassrede oder Urheberrechtsverletzungen hinein. Ihnen allen ist gemeinsam, dass sich ein Nutzer nachträglich aufspüren lässt, nachdem er eine rechtlich problematische Handlung vollzogen hat.

Über die IP-Adresse des Nutzers, so die Hoffnung, lässt sich später der Anschlussinhaber und somit der Täter ermitteln. Bei der Gefahrenabwehr hingegen sollen Nutzerinnen und Nutzer gezielt ausgesperrt werden.

Webanalyse

Die Analyse von Nutzerverhalten im Internet hat zum Ziel, Nutzerinnen und Nutzer möglichst wiederzuerkennen und somit von anderen Nutzern abzugrenzen.

Eine Möglichkeit, Nutzer wiederzuerkennen, ist deren digitaler Fingerabdruck, auch Browser Fingerprint oder Device Fingerprint genannt. Dieser Fingerabdruck ist oftmals eindeutig, wenn er die IP-Adresse enthält. Auch allein anhand der IP-Adresse lässt sich ein Nutzer gut isolieren, etwa indem man die Aufrufhistorie auf einer Webseite berücksichtigt: Wenn Nutzer X auf einer Webseite von Unterseite A nach Unterseite B springt, dann kann man auf Seite B mit an Sicherheit grenzender Wahrscheinlichkeit auf Nutzer X schließen.

Anlasslose und anlassbezogene Speicherung

Nicht alles, was nützlich ist, ist zulässig. So ist etwa ein Bankraub nicht erlaubt, auch wenn er für den Bankräuber sicherlich nützlich ist, um schnell an viel Geld zu gelangen. Analog verhält es sich mit der Verarbeitung personenbe- →

Checkliste Server-Logs

Diese Fragen können DSB stellen:

- Speichert der Website-Betreiber IP-Adressen anlasslos?
- Gab es bereits einen Nutzen aus der Speicherung in den Logs?
- Musste er bereits Angriffe abwehren?
- Welche Anlässe sind definiert?
- Wie lange speichert der Verantwortliche IP-Adressen pro Anlass?
- Speichert er zusätzliche Daten (Gerätekennungen, E-Mail-Adressen, …) ab?

Was ist ein Anlass?

Die zentrale Frage ist, ob bei der Speicherung von Verkehrs- und Standortdaten, denen auch IP-Adressen zuzurechnen sind, ein Anlass vorliegt oder nicht. Als Speicherung gilt in diesem Beitrag die persistente Ablage auf einem Datenträger. Üblicherweise ist dies eine Festplatte oder SSD. Es geht also nicht um die flüchtige Speicherung im Arbeitsspeicher, die nur von kurzer Dauer ist und kein Auslesen ermöglicht. Die Frage nach dem Anlass lässt sich aus technischer Sicht betrachten. Was als anlasslos gilt, ist schnell zu beantworten. Der Anlass fehlt dann, wenn IP-Adressen grundsätzlich immer in Server-Logs gespeichert werden. Dies betrifft die Speicherung voller Netzwerkadressen, die geeignet sind, Nutzer zu identifizieren. Eine Speicherung, die ausnahmslos immer stattfindet, unterscheidet nicht nach den vorliegenden Gegebenheiten und ist somit anlasslos.

zogener Daten. Das hat der EuGH in seinem Urteil vom 05.04.2022 (Az. C-140/20) festgestellt. Insbesondere in Rn 100f hat der EuGH verdeutlicht, dass „Verkehrs- und Standortdaten […] nicht allgemein und unterschiedslos auf Vorrat gespeichert werden" dürfen.

Was sind valide Anlässe?

Um IP-Adressen zulässigerweise zu speichern, ist also ein Anlass erforderlich. Ein Anlass liegt im Kontext dieses Beitrags dann vor, wenn ein Nutzer einer Webseite oder einer App eine relevante Aktion ausführt. Zu einer Aktion zählt etwa, die Webseite zu bedienen, einen Link anzuklicken oder einen Button zu drücken. Doch ist eine solche Aktion auch relevant, sprich: Könnte daraus ein Problem entstehen? Denkt man die Kausalkette vom Ende her, dann fällt es schwer, aus einem einzigen Klick auf einen Link ein Problem zu konstruieren. Gleiches gilt für das gewöhnliche Klick- und Bedienverhalten auf Webseiten. Ein **valider Anlass** sollte also dergestalt sein, **dass er in ein Problem münden könnte**.

Klickt ein Nutzer in kurzer Zeit nicht nur wenige Male, sondern sehr oft auf Buttons derselben Webseite, dann könnte man böse Absicht unterstellen. Zumindest erscheint es aus Sicht des Dienstanbieters nicht zielführend, wenn sich Nutzer so verhalten. Es kommt also auch auf das Schutzbedürfnis der verantwortlichen Stelle an.

In diesem Spannungsfeld zwischen Schutzbedürfnis der Nutzer und Nutzerinnen und dem der Verantwortlichen befindet sich die Frage nach der Speicherung von IP-Adressen. Relevante und valide Anlässe auf Webseiten oder in Apps können sein:

- Eine Person führt einen Bestellvorgang in einem Webshop aus.
- Ein Nutzer sendet ein Kontaktformular ab oder nutzt eine Kommentarfunktion.
- Ein Nutzer registriert sich für einen Newsletter.
- Ein Nutzer kopiert Massendaten in ein Kontaktformular.
- Der Dienst wird sehr oft automatisiert aufgerufen.
- Ein Nutzer gibt beim Log-in-Versuch mehrmals das falsche Passwort ein.

Es stellt sich die Frage, welche dieser Probleme sich rechtlich wie verfolgen lassen, sofern überhaupt ein rechtlicher Fall daraus entsteht. Insbesondere ist zu klären, wie Verantwortliche mit derartigen Problemen umgehen können.

Zulässige und unzulässige Speicherung von IP-Adressen

Der Nutzen einer Sache allein ist für die rechtliche Beurteilung nicht ausschlaggebend. Vielmehr kommt es auch darauf an, ob nicht mildere oder gar bessere Mittel zur Verfügung stehen und ob die Maßnahme überhaupt geeignet ist, um das Ziel zu erreichen.

Klar ist, dass insbesondere dynamische IP-Adressen zumindest bei bestimmten Anschlussarten häufig anderen Anschlussinhaber zugeordnet werden. Der nicht ganz dumme Kriminelle wird eine Denial-of-Service-Attacke auch nicht direkt von seinem privaten Internetanschluss aus durchführen. Vielmehr setzt er auf Proxy-Server oder öffentliche Netze. Oder er zweckentfremdet fremde Rechner dafür. Oft verwenden mehreren Personen oder gar mehrere Haushalte private Internetanschlüsse gemeinsam. Es kommt zudem vor, dass ein Dritter ein privates WLAN benutzt. Somit ist eine dynamische IP-Adresse nur begrenzt aussagekräftig.

Vertretbare Nutzung von IP-Adressen

Geht es um die Sperre einzelner IP-Adressen, um etwa **unerwünschte Kommentare zu verhindern**, kann es sinnvoll sein, die jeweilige IP-Adresse zu kennen und zu nutzen.

Denkt man an dynamische IP-Adressen, könnte das Aussperren unerwünschter Kommentargeber jedoch dazu führen, dass später ein anderer Anschlussinhaber keinen Kommentar mehr absenden kann. Es dürfte allerdings ausgeschlossen sein, dass zwei Personen dieselbe Webseite für dieselbe Funktion nutzen, die zudem in zeitlichem Abstand dieselbe IP-Adresse zugeordnet bekamen. Insofern wäre das Aussperren von

PRAXIS-TIPP

Mit einem validen Anlass ist es also möglich, die Speicherung voller IP-Adressen in Serverlogs zu rechtfertigen. Diese Adressen dürfen Verantwortliche dann nur zweckgemäß verwenden, also bezogen auf den jeweiligen Anlass.

unerwünschten Nutzern aufgrund von deren Netzwerkadressen in diesem Fall vertretbar.

Wenn ein Hacker einen Dienst über einen gekaperten Zombie-Rechner bombardiert, dann wäre es für den ahnungslosen Inhaber des gekaperten Rechners nicht besonders erfreulich, aufgrund der ihm unbekannten **Hackeraktivität** von einem Dienst ausgesperrt zu sein. Wie im vorherigen Fall überwiegt jedoch auch hier das Interesse des Dienstbetreibers.

Problematische Verwendung von IP-Adressen

Problembehaftet ist die **Speicherung von IP-Adressen ohne Anlass**, also auf Vorrat. Hier fehlt die Rechtfertigung für die Speicherung. Diese muss aber gemäß Art. 6 Abs. 1 der Datenschutz-Grundverordnung (DSGVO) vorliegen.

Zieht man die anlassbezogenen Rechtsgrundlagen wie den Vertrag ab, dann bleibt aus Art. 6 Abs. 1 DSGVO nur das berechtigte Interesse übrig. Die Abwehr schwerer Kriminalität, wie sie der EuGH thematisierte, dürfte aber für den kommerziellen oder privaten Betreiber einer Webseite grundsätzlich keine Rechtfertigungsgrundlage sein.

PRAXIS-TIPP

- *Ungekürzte IP-Adressen anlasslos zu speichern, erzeugt Probleme. Die Zusatzverantwortung führt nur in wenigen Fällen zu einem Nutzen. Diesen Nutzen hätte auch eine rein anlassbezogene Speicherung erreicht. Liegt kein Anlass vor, ist es sinnvoll, die Netzwerkadressen gekürzt zu speichern.*
- *Anlassbezogen ist die Speicherung von vollen IP-Adressen erlaubt. Verantwortliche dürfen die derart erhobenen Daten dann nur für den jeweiligen Anlass verwenden, sofern sich nicht Weiteres ergibt.*
- *Die Speicherdauer bei anlassbezogener Speicherung sollte maßvoll ausfallen.*
- *Datenschutzbeauftragte sollten Mandanten empfehlen, unterschiedslos geführte Server-Logs für deren Webseiten zu deaktivieren und auf den Provider einzuwirken. Sieht sich ein Provider überfordert, seine Konfiguration anzupassen, ist er im Zweifel zumindest in der Mitverantwortung.*

Das berechtigte Interesse ist nur dann gegeben, wenn ein Gleichgewicht der Interessen zwischen Verantwortlichem und betroffener Person vorliegt. Dieses Gleichgewicht kann nur dann gegeben sein, wenn

1. die Maßnahme nützlich sein kann, und
2. es keine milderen oder gar besseren Mittel gibt, und
3. der Eingriff in die Privatsphäre einer Person nicht übermäßig groß ausfällt.

Die Speicherung und nachträgliche Nutzung von IP-Adressen sind mitunter nicht nützlich, selbst wenn ein Anlass vorliegt, wie oben skizziert. Ohne Anlass ist dieser Nutzen noch geringer, und die Datenspeicherung geht noch stärker zulasten der betroffenen Personen.

Ist es notwendig, die IP-Adresse von Nutzerinnen und Nutzern in Server-Logs zu speichern? Ohne gegebenen Anlass ist diese Frage zu verneinen. Der Autor hat bei IT-Sicherheitsspezialisten und beim Bundesamt für Sicherheit in der Informationstechnik (BSI) nachgefragt, ob eine anlasslos gespeicherte IP-Adresse nachträglich, wenn sich ein Anlass ergeben hatte, notwendig für die Gefahrenabwehr oder Rechtsverfolgung sei. Das Ergebnis war, dass niemand ein einziges Beispiel nennen konnte. Liegt hingegen ein Anlass vor, dürfen Website-Betreiber volle IP-Adressen in Server-Logs speichern.

Speicherdauer

Die Speicherdauer hängt vom Anlass ab. Ohne differenzierte Betrachtung sind sieben Tage vertretbar, vielleicht auch 30 Tage. Alles, was über einen Zeitraum von zwei Jahren hinausgeht, erscheint kaum zu rechtfertigen.

Kommt es zwischen einem Dienstanbieter und einem Dienstnutzer zu einem Rechtsstreit, lassen sich die gespeicherten Daten je nach Fall einfrieren. Die Speicherdauer spielt dann also keine Rolle mehr. Dieses Einfrieren nennt man auch Freeze, oder in der Diskussion um die Vorratsdatenspeicherung Quick Freeze.

Dr. Klaus Meffert ist Diplom-Informatiker und seit 30 Jahren in der IT-Beratung und Software-Entwicklung tätig. Im Blog Dr. DSGVO schreibt Dr. Meffert regelmäßig zum digitalen Datenschutz und zu Offline-KI (dr-dsgvo.de).

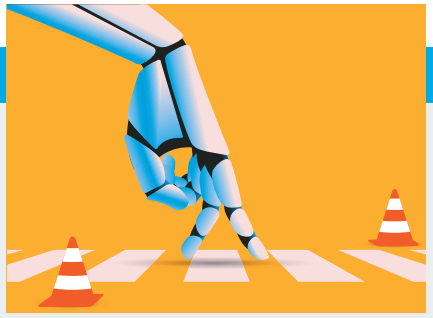
BEISPIEL

Den genannten Anlässen ist gemeinsam, dass daraus rechtliche Probleme entstehen können, insbesondere zulasten des Verantwortlichen. Exemplarisch seien einige dieser Probleme genannt:

- *Jemand hat Ware unter falschem Namen bestellt oder ein Newsletter-Abo mit falscher E-Mail-Adresse, sei es absichtlich oder aufgrund eines Tippfehlers.*
- *Über ein Kontaktformular wurden beleidigende Äußerungen verschickt.*
- *Ein Krimineller versucht, eine Webseite lahmzulegen, indem er sie mit Massenanfragen bombardiert.*
- *Ein Hacker versucht, sich unbefugten Zugang zu verschaffen.*

Datenschutzkonferenz (DSK)

KI-Orientierungshilfe



Einen Überblick über datenschutzrechtliche Kriterien, die beim Einsatz von KI-Anwendungen zu berücksichtigen sind, will eine Orientierungshilfe der DSK bieten. Sie richtet sich an Verantwortliche, die KI-Anwendungen einsetzen möchten. Andere Situationen, etwa die Entwicklung solcher Anwendungen, streift sie lediglich.

Die DSK hält Fallkonstellationen für denkbar, bei denen keinerlei personenbezogene Daten vorkommen, weder als Eingabe- noch als Ausgabedaten und auch nicht im Anmelde- und Verarbeitungsprozess. Solche Anwendungen unterlägen nicht dem Datenschutzrecht. Wegen dieser weitreichenden Folge seien sie allerdings besonders sorgfältig zu prüfen (Rn 4–6 der Orientierungshilfe).

Unzulässig: automatisierte Letztentscheidungen

Automatisierte Letztentscheidungen durch KI-Systeme seien untersagt. Hierzu führt die DSK aus: „Entscheidungen mit Rechtswirkung dürfen gemäß Art. 22 Abs. 1 DSGVO grundsätzlich nur von Menschen getroffen werden. Ausnahmen sind nur in bestimmten Fällen zugelassen, etwa bei einer Einwilligung der betroffenen Person. Erarbeitet eine KI-Anwendung Vorschläge, die für eine betroffene Person Rechtswirkung entfalten, muss das Verfahren so gestaltet werden, dass dem entscheidenden Menschen ein tatsächlicher Entscheidungsspielraum zukommt und nicht maßgeblich aufgrund des KI- Vorschlags entschieden wird." (siehe Rn 12).

Empfehlenswert: geschlossenes KI-System

Großen Wert legt der Text auf die Unterscheidung zwischen offenen und geschlossenen KI-Systemen (Rn 15–20). Ein – aus Sicht des Datenschutzes vorzugswürdiges – geschlossenes System liegt vereinfacht gesagt vor, wenn die Kontrolle über die Ein- und Ausgabedaten vollständig beim Anwender bleibt und der Systemanbieter die Daten nicht zum weiteren Training des Systems verwendet (Rn 17).

Ausführlich spricht die Orientierungshilfe organisatorische Fragen bei der Implementierung von KI-Systemen an (Rn 32–37). Eher allgemein äußert sie sich dagegen zur Datensicherheit bei KI-Anwendungen (Rn 44/45).

Im Wesentlichen verweist die Orientierungshilfe hier auf entsprechende Empfehlungen des Bundesamts für Sicherheit in der Informationstechnik (BSI).

Quelle: Datenschutzkonferenz (DSK), Orientierungshilfe „Künstliche Intelligenz und Datenschutz", Version 1.0 vom 06. Mai 2024. Der Text hat einen Umfang von 15 Seiten und ist abrufbar unter https://datenschutzkonferenz-online.de/orientierungshilfen.html.

Bild: iStock.com/Xeniya Udod Femagora

Datenschutzaufsicht Sachsen

Kennzeichenerfassung beim Parken

Die Kennzeichenerfassung beim Parken, etwa in Parkhäusern, hat nichts mit unerlaubter Videoüberwachung zu tun. Das hat die Datenschutzaufsicht Sachsen klargestellt. Voraussetzung ist dabei, dass geeignete Verfahren zum Einsatz kommen.

Standbilder, keine Bildsequenzen

Solche Verfahren arbeiten zwar mit Kamerasystemen. Die Systeme erzeugen jedoch keine Filmaufnahmen in Form von „Bildsequenzen", sondern nur einzelne Standbilder. Aus diesen Standbildern liest das System die Kennzeichen aus. Personen, etwa der Fahrer, kommen dabei buchstäblich gar nicht „ins Bild". Gespeichert werden folgende Daten:

- Standbild
- Kfz-Kennzeichen
- Datum und Uhrzeit der Einfahrt
- Datum und Uhrzeit der Ausfahrt

Das macht Parktickets entbehrlich. Die Ausfahrtsschranke hebt sich nur dann, wenn die Parkgebühren bezahlt worden sind.

Pseudonyme Daten unterliegen der DSGVO

Die genannten Daten sind als pseudonyme Daten (siehe Art. 4 Nr. 5 DSGVO) anzusehen, sind also personenbezogen (siehe Erwägungsgrund 26 Satz 2 zur DSGVO). Damit gelten für sie die Vorgaben der DSGVO. Rechtsgrundlage für ihre Verarbeitung ist regelmäßig ein „Parkvertrag" (Konstellation von Art. 6 Abs. 1 Buchst. b DSGVO). Er kann unter Verwendung Allgemeiner Geschäftsbedingungen auch dadurch zustande kommen, dass jemand zum Parken einfährt.

Information der Betroffenen

Eine ordnungsgemäße Datenschutz-Information der betroffenen Person beim Einfahren zum Parken ist geboten (Information gemäß Art. 13 DSGVO). Piktogramme sind dabei möglich.

Quelle: Datenschutzaufsicht Sachsen, Tätigkeitsbericht Datenschutz Sachsen 2023, S. 61–63. Der Bericht ist abrufbar unter www.datenschutz.sachsen.de/taetigkeitsberichte.html.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken und seit vielen Jahren als Autor, Referent sowie Moderator im Datenschutz aktiv.

Bild: iStock.com/Prostock-Studio

Vertraulichkeit nach dem Hinweisgeberschutzgesetz und Informationspflichten nach DSGVO erzeugen ein Spannungsfeld. Wie Sie die zwei Pole im Tagesgeschäft ins Gleichgewicht bringen, erläutert Dr. Lang aus seiner praktischen Erfahrung

Datenschutz-Compliance

Vertraulichkeit nach dem Hinweisgeberschutzgesetz

Das Vertraulichkeitsgebot schützt die Identität von Hinweisgebern und weiteren Personen. Dieser Schutz ist aber nicht absolut. Dieser Leitfaden gibt einen Überblick über die Regelungen sowie zum Zusammenspiel mit den datenschutzgesetzlichen Informations- und Auskunftsrechten.

Das Vertraulichkeitsgebot ist ein zentraler Pfeiler des Hinweisgeberschutzes. Es gibt zwei praxisrelevante Gruppen von Anwendungsfällen:

1. die Weitergabe von Informationen durch Meldestellen im Rahmen ihrer Aufgaben nach dem HinSchG und
2. den Umgang mit den datenschutzgesetzlichen Informations- und Auskunftsrechten betroffener Personen.

Erfasster Personenkreis

Das Vertraulichkeitsgebot ist in § 8 Hinweisgeberschutzgesetz (HinSchG) geregelt. Es soll die Identität von Personen schützen, die von einer Meldung im Rahmen des HinSchG betroffen sind. Erfasst sind damit

- Personen, die Hinweise geben,
- Personen, die Gegenstand einer Meldung sind, da ihnen ein Fehlverhalten vorgeworfen wird, und
- sonstige in einer Meldung genannte Personen, etwa beteiligte oder unbeteiligte Dritte wie Kollegen oder Vorgesetzte.

Das Vertraulichkeitsgebot bezieht sich nicht nur auf Identitätsangaben wie Vor- und Nachnamen, die eine unmittelbare Zuordnung ermöglichen. Es umfasst auch alle Informationen, aus denen sich die Identität der Personen ableiten lässt.

Das Gebot der Vertraulichkeit der Identität gilt unabhängig davon, ob die Meldestelle für die eingehende Meldung zuständig ist. Das folgt aus § 8 Abs. 2 HinSchG.

Beachten Sie die Anwendbarkeit!

Das Vertraulichkeitsgebot gemäß § 8 HinSchG gilt nur in Fällen, in denen das Gesetz tatsächlich anwendbar ist. Es kommt daher nicht zum Tragen,

- wenn Unternehmen oder Dienststellen nicht nach HinSchG verpflichtet sind, oder
- bei Sachverhalten, die nicht in den Anwendungsbereich des HinSchG fallen.

Ausnahmen vom Vertraulichkeitsgebot

Das Vertraulichkeitsgebot gilt nicht absolut. Es gibt zahlreiche Ausnahmen, die § 9 HinSchG näher regelt.

Hierbei unterscheidet das HinSchG

- zwischen den Personen, deren Identität grundsätzlich geschützt ist, und
- zwischen den Anlässen und Zwecken der Weitergabe sowie den Empfängern der Informationen.

Systematik der Ausnahmen

Die Ausnahmen vom Vertraulichkeitsgebot sind in Hinblick auf die betroffenen Personen wie folgt unterteilt:

- Die Regelungen zur Identität von Hinweisgebern und Informationen, aus denen deren Identität abgeleitet werden kann, finden sich in den Absätzen 1 bis 3.
- Die Regelungen zur Identität von Personen, die Gegenstand einer Meldung sind, und von sonstigen in der Meldung genannten Personen sowie zu Umständen, die Rückschlüsse auf diese Personen erlauben, enthält Absatz 4. →

Vertraulichkeitsgebot nur bei Anwendbarkeit des HinSchG

Anwendbarkeit des HinSchG

1. Verpflichtete (Normadressaten)
„Beschäftigungsgeber", also Unternehmen und Behörden
- mit mehr als 50 Beschäftigten sowie
- unabhängig von der Beschäftigtenzahl bestimmte Unternehmen der Finanz- und Versicherungswirtschaft, die § 12 Abs. 3 HinSchG auflistet.

2. Sachlicher Anwendungsbereich
Alle Informationen über
- strafbewehrte Verstöße,
- bußgeldbewehrte Verstöße, soweit die verletzte Vorschrift dem Schutz von Leben, Leib, Gesundheit oder dem Schutz der Rechte von Beschäftigten oder ihrer Vertretungsorgane dient (z.B. Arbeits- und Gesundheitsschutz),
- sonstige Verstöße gegen Bundes- und Landesvorschriften sowie unmittelbar geltende Rechtsakte der EU in den Rechtsgebieten, die in § 2 Abs. 1 Nr. 3 HinSchG genannt sind,
- weitere Verstöße, die in § 2 Abs. 1 Nr. 4 bis 10 und Abs. 2 HinSchG aufgelistet sind.

3. Persönlicher Anwendungsbereich
Alle Personen,
- die im Zusammenhang mit ihrer beruflichen Tätigkeit Informationen über Verstöße erlangt haben und diese melden oder offenlegen,
- die Gegenstand einer Meldung oder Offenlegung sind, indem ihnen ein Fehlverhalten vorgeworfen wird, oder die in anderer Form davon betroffen sind, etwa als Zeugen.

Die differenzierende Regelung der Ausnahmen vom Vertraulichkeitsgebot sei anhand von zwei Beispielen veranschaulicht.

Beispiel „Weitergabe von Daten in Strafverfahren"

Informationen über die Identität von Hinweisgebern oder über sonstige Umstände, die Rückschlüsse auf die Hinweisgeber erlauben, dürfen aufgrund einer gerichtlichen Entscheidung und in Strafverfahren auf Verlangen der Strafverfolgungsbehörde weitergegeben werden (§ 9 Abs. 2 Satz 1 Nr. 1 und 3 HinSchG). Dasselbe gilt für Informationen über die Identität von Personen, die Gegenstand eines Hinweises sind, und von sonstigen in der Meldung genannten Personen (§ 9 Abs. 4 Nr. 4 und 6 HinSchG). Im Gegensatz zu diesen Personen sind Hinweisgeber jedoch vorab über die Weitergabe und deren Gründe zu informieren, sofern die Strafverfolgungsbehörde bzw. das Gericht nicht der Auffassung sind, dass hierdurch die Ermittlungen oder das Gerichtsverfahren gefährdet würden (§ 9 Abs. 1 Satz 2 und 3 HinSchG).

Beispiel „Weitergabe für Folgemaßnahmen"

Auch zum Zweck von Folgemaßnahmen nach § 18 HinSchG wie interne Untersuchungen dürfen Informationen über die Identität von Hinweisgebern weitergegeben werden, wenn es erforderlich ist und die hinweisgebende Person zuvor eingewilligt hat (§ 9 Abs. 3 HinSchG). Informationen zur Identität von Personen, die Gegenstand eines Hinweises oder anderweitig in einer Meldung erwähnt sind, dürfen in diesen Fällen ohne deren Einwilligung weitergeben werden (§ 9 Abs. 4 Nr. 2 und 3 HinSchG).

Vertraulichkeitsgebot begrenzt Informations- und Auskunftsrechte

Damit das Vertraulichkeitsgebot nicht ins Leere läuft, sind die datenschutzgesetzlichen Informations- und Auskunftsrechte sowie die korrespondierenden Pflichten der Verantwortlichen teilweise eingeschränkt. Diese Ausnahmen sind nicht im HinSchG geregelt, sondern datenschutzgesetzlich. Für die Informationspflicht sind das Art. 14 Abs. 5 Buchst. c und Art. 23 Abs. 1 Buchst. i DSGVO in Verbindung mit § 29 Abs. 1 Satz 1 BDSG in Verbindung mit §§ 8 und 9 HinSchG.

Teilweise wird auch Art. 14 Abs. 5 Buchst. b DSGVO herangezogen, etwa vom Landesbeauftragen für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW). Danach besteht keine Informationspflicht, „wenn und solange dadurch die Aufklärung des Sachverhalts und … Untersuchungen ernsthaft beeinträchtigt würden, z.B. aufgrund von drohenden Verdunklungsmaßnahmen der beschuldigten Person." Die FAQ zum Hinweisgeberschutzgesetz vom LfDI BW sind nachzulesen unter https://ogy.de/FAQ-LfDI-BW.

In Bezug auf die Identität von Hinweisgebern verweist aber auch der LfDI BW auf § 29 Abs. 1 Satz 1 BDSG. Danach besteht keine Informationspflicht, soweit Informationen offenbart würden, die ihrem Wesen nach geheim gehalten werden müssen. Letzteres folgt wiederum aus dem Vertraulichkeitsgebot, das im HinSchG verankert ist. Für das datenschutzgesetzliche Auskunftsrecht kommt die Ausnahme

ACHTUNG!

Bei einer Einwilligung von Hinweisgebern in einem Beschäftigungsverhältnis sind die Vorgaben gemäß § 26 Abs. 2 des Bundesdatenschutzgesetzes (BDSG) zu beachten. Danach sind bei der Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit und die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Letzteres sollten Sie mit Blick auf die spezifischen Aspekte von Whistleblowing besonders sorgfältig prüfen.

gemäß Art. 23 Abs. 1 Buchst. i DSGVO in Verbindung mit § 29 Abs. 1 Satz 2 BDSG in Verbindung mit §§ 8 und 9 HinSchG zum Tragen.

Denken Sie an die Ausnahmen vom Vertraulichkeitsgebot

Die datenschutzgesetzlichen Einschränkungen der Informations- und Auskunftsrechte kommen jedoch nur dann zum Tragen, wenn das Vertraulichkeitsgebot nach HinSchG tatsächlich gilt. Das setzt nicht nur die Anwendbarkeit des HinSchG voraus. Es darf auch keine Ausnahme vom Vertraulichkeitsgebot gemäß § 9 HinSchG vorliegen, wie oben bereits beschrieben.

Es bestehen auch Gegenausnahmen. Daher lässt nicht jede Ausnahme vom Vertraulichkeitsgebot die Informations- oder Auskunftspflicht automatisch wieder aufleben. Das sei an dem bereits erwähnten Beispiel erläutert, dass Informationen über die Identität von Hinweisgebern ausnahmsweise in Strafverfahren auf Verlangen der Strafverfolgungsbehörden an die zuständige Stelle übermittelt werden dürfen. Über diese Weitergabe sind die Hinweisgeber nach dem HinSchG grundsätzlich zu informieren. Das gilt aber nicht, wenn die Strafverfolgungsbehörde der Meldestelle mitgeteilt hat, dass die Information die entsprechenden Ermittlungen gefährden würde (§ 9 Abs. 2 Satz 2 und 3 HinSchG).

Vorgehen in der Praxis

Sie sollten sämtliche Detailregelungen des Vertraulichkeitsgebots im Datenschutzmanagement und in dem zugrunde liegenden Datenschutzkonzept berücksichtigen und abbilden. Sie müssen die Vorgaben des HinSchG vollständig in die Datenschutzprozesse integrieren. Andernfalls besteht die Gefahr, im konkreten Einzelfall die datenschutzgesetzlichen Informations- und Auskunftsrechte oder das Vertraulichkeitsgebot nach dem HinSchG zu verletzen.

PRAXIS-TIPP

Die datenschutzgesetzliche Information von Hinweisgebern ist ebenso wie eine entsprechende Auskunft relativ einfach umzusetzen, da lediglich die allgemeinen Vorgaben gemäß Art. 13 und 15 DSGVO gelten, aber grundsätzlich keine Ausnahmetatbestände. Ein Beispiel einer datenschutzgesetzlichen Information für Hinweisgeber finden Sie in den Datenschutzhinweisen des LfDI BW unter https://ogy.de/Info-LfDI-BW, wo diese Information als ein spezifischer Teil von mehrstufigen Datenschutzhinweisen abgebildet ist.
Etwas schwieriger gestalten sich die Informations- und Auskunftspflichten gegenüber Personen, die Gegenstand einer Meldung oder anderweitig in der Meldung erwähnt sind. Die datenschutzgesetzliche Information und Auskunft wird in Whistleblowing-Fällen regelmäßig die Quelle bzw. Herkunft der Daten umfassen, also auch die Identität von Hinweisgebern (Art. 14 Abs. 2 Buchst. f, Art. 15 Abs. 1 Buchst. g DSGVO). Allerdings werden die datenschutzgesetzlichen Informations- und Auskunftsrechte sowie die korrespondierenden Pflichten des Verantwortlichen durch die Einschränkungen begrenzt, die die DSGVO und das BDSG vorsehen.

Um unvollständige Auskünfte nach Art. 15 DSGVO durch Unternehmen und Behörden zu vermeiden, sollten Sie Ihre Meldestelle in den allgemeinen Prozess der datenschutzgesetzlichen Auskunft einbeziehen. Das kann unter Berücksichtigung der bereits vorhandenen Prozessabläufe z.B. dadurch erfolgen, dass die interne Meldestelle über das Auskunftsbegehren informiert wird und sie es in Bezug auf ihren Zuständigkeitsbereich eigenständig beantwortet. Andernfalls besteht die Gefahr, gegen das Vertraulichkeitsgebot zu verstoßen.

Dokumentieren Sie genau

Schließlich sollten Sie in den Prozessen der datenschutzgesetzlichen Information und Auskunft vorsehen, dass bei jeder Information bzw. Nicht-Information und bei jeder Bearbeitung eines Auskunftsanspruchs konkret dokumentiert wird, warum die Identität des Hinweisgebers (nicht) offengelegt wurde. Das gilt gleichermaßen für die Prozesse der Weitergabe von Informationen durch die Meldestellen im Rahmen ihrer Aufgaben nach dem HinSchG. Denn ein Verstoß gegen die Pflicht zur Vertraulichkeit ist in jedem Fall nach § 40 Abs. 3 und 6 HinSchG bußgeldbewehrt.

Dr. Markus Lang ist Rechtsanwalt in Düsseldorf (Datenschutzrecht-Praxis) und berät Unternehmen zu allen Fragen des Datenschutz- und IT-Rechts.

Bild: iStock.com/metamorworks

Diese Tipps helfen dabei, ein vollständiges, verständliches und alltagstaugliches VVT zu erstellen bzw. als DSB dabei zu beraten. So können sich Arztpraxen auf ihre Hauptaufgabe konzentrieren: Patientinnen und Patienten zu behandeln.

DSGVO-konform im Praxisalltag

VVT und Ärzte – Tipps für die Umsetzung in der Praxis

Das Verzeichnis von Verarbeitungstätigkeiten (VVT) ist eine wichtige Grundlage, um die DSGVO umzusetzen. Dies gilt insbesondere für Ärztinnen und Ärzte, da sie häufig Gesundheitsdaten verarbeiten. Der Beitrag vermittelt Tipps, wie man in der Arztpraxis ein VVT erstellt.

Als Verantwortliche gemäß Art. 4 Nr. 7 Datenschutz-Grundverordnung (DSGVO) sind Arztpraxen nach Art. 30 Abs. 1 Satz 1 DSGVO verpflichtet, ein VVT zu führen. Diese Pflicht besteht erst ab 250 Beschäftigten. Doch es greifen Ausnahmen nach Art. 30 Abs. 5 DSGVO: Arztpraxen verarbeiten personenbezogene Daten nicht nur gelegentlich. Zudem verarbeiten sie besondere Kategorien personenbezogener Daten gemäß Art. 9 Abs. 1 DSGVO in Form von Gesundheitsdaten.

Auch abseits der gesetzlichen Pflicht empfiehlt sich ein VVT: Es schafft einen Überblick über alle Datenverarbeitungsprozesse der Praxis. Dies erleichtert es z.B., mit Datenschutzvorfällen umzugehen und Anfragen Betroffener zu beantworten.

PRAXIS-TIPP

Um ein VVT zu erstellen, gibt es – abgesehen von den Vorgaben aus Art. 30 Abs. 1 Satz 2 DSGVO – keine Regelungen zum strukturellen Aufbau. Hinzu kommt, dass der Begriff der „Verarbeitungstätigkeit" im Gesetz nicht definiert ist. In der Praxis finden sich daher verschiedene Herangehensweisen. Beraten Sie als Datenschutzbeauftragte/-r (DSB) eine Arztpraxis, empfehlen Sie die Aufteilung in verschiedene Abteilungen bzw. Bereiche. Anschließend dokumentiert die Praxis für jeden Bereich die Verarbeitungstätigkeiten. Dann ergänzt sie diese um die Pflichtangaben aus Art. 30 Abs. 1 Satz 2 DSGVO.

Aufbau in der Praxis

Auf der ersten Ebene unterteilt die Person, die das VVT erstellt, die Arztpraxis in verschiedene Bereiche, z.B. Personal, Marketing oder IT. Die Anzahl der Bereiche hängt dabei insbesondere davon ab, wie groß die Praxis ist und wie zahlreich und komplex die Verarbeitungstätigkeiten sind. Daneben empfiehlt es sich, einen Bereich festzulegen, in dem alle Tätigkeiten aufgeführt sind, die die Haupttätigkeit der Arztpraxis betreffen, also die Prävention, Diagnose und Therapie von Beschwerden und Krankheiten. Dieser Bereich heißt folgerichtig z.B. „Kern- oder Haupttätigkeit".

Anschließend erfasst die Person die Verarbeitungstätigkeiten. Dabei gilt: Je umfangreicher und komplexer die Datenverarbeitungen sind, desto kleinteiliger und detaillierter sind sie zu definieren. Sofern Verarbeitungstätigkeiten die Kerntätigkeit betreffen, sind diese im entsprechenden Bereich aufzulisten.

Es gibt jedoch auch typische Verarbeitungstätigkeiten in einer Arztpraxis, die die Kerntätigkeit nicht direkt betreffen. Diese sind auf die thematisch passenden Bereiche zu verteilen (z.B. die Online-Terminbuchung; siehe dazu auch Conrad/Folkerts, Terminbuchungstools für Arztpraxen, in der Ausgabe Datenschutz Praxis 06/24, S. 17–19).

Kategorien personenbezogener Daten

Arztpraxen verarbeiten insbesondere Gesundheitsdaten von Patientinnen und Patienten. Dabei handelt es sich nach Art. 4 Nr. 15 DSGVO um personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen, einschließlich der Gesundheitsdienstleistungen, und aus denen Informationen über deren Gesundheitszustand hervorgehen. Der Anwendungsbereich ist aus Schutzgesichtspunkten weit zu verstehen.

Verarbeitungstätigkeiten in Arztpraxen

Typische Verarbeitungstätigkeiten in einer Arztpraxis sind:

- **Anlage und Verwaltung von Patientenakten**
- **Terminvergabe und -Planung (ggf. auch durch ein Onlineformular)**
- **Abrechnung mit gesetzlichen Krankenversicherungen**
- **Abrechnung mit privaten Krankenversicherungen sowie bei individuellen Gesundheitsleistungen**
- **Überweisungen zu Fachärzten**
- **Erstellung ärztlicher Gutachten**
- **Laboruntersuchungen**
- **Ausstellung der elektronischen Arbeitsunfähigkeitsbescheinigung (eAU)**

Kategorien von Empfängern

Nach Art. 30 Abs. 1 Satz 2 Buchst. d DSGVO haben Arztpraxen zudem die Kategorien von Empfängern sowie die Empfänger in Drittländern oder internationalen Organisationen zu dokumentieren.

Mit Ausnahme von Datenübermittlungen in ein Drittland reicht es laut dem Gesetz aus, lediglich die Kategorien von Empfängern anzugeben. Dennoch empfiehlt es sich, möglichst die konkreten Empfänger aufzunehmen. Der Hintergrund: Verantwortliche sind bei Auskunftsansprüchen nach Art. 15 Abs. 1 Buchst. c DSGVO grundsätzlich verpflichtet, der betroffenen Person die konkreten Empfänger mitzuteilen (Europäischer Gerichtshof (EuGH), Urteil vom 12.01.2023 – C-154/21 Rn 46).

Sollten Patientinnen oder Patienten ihr Recht aus Art. 15 DSGVO geltend machen, erleichtert die Dokumentation der konkreten Empfänger, solche Anfragen zu beantworten.

Typische Kategorien von Empfängern einer Arztpraxis sind:

- Labore
- Kassenärztliche Vereinigung
- Krankenkassen
- privatärztliche Verrechnungsstellen
- Facharztpraxen, Physiotherapiepraxen, Krankenhäuser

Die Zusammenarbeit mit Laboren ist keine Auftragsverarbeitung. Dasselbe gilt für die Abrechnung über die Kassenärztliche Vereinigung. Bei der privatärztlichen Verrechnungsstelle ist zu unterscheiden: Erstellt diese lediglich die Rechnung, liegt eine Auftragsverarbeitung vor. Überträgt eine Arztpraxis hingegen eine Forderung, ist keine Auftragsverarbeitung gegeben. Denn die Stelle macht den Anspruch dann eigenständig geltend.

Löschfristen

Nach Art. 30 Abs. 1 Satz 2 Buchst. f DSGVO sind – soweit möglich – auch die Löschfristen für personenbezogene Daten anzugeben. Dabei reicht es aus, die konkrete Aufbewahrungsdauer und den Fristbeginn aufzunehmen.

Wenn Arztpraxen Gesundheitsdaten verarbeiten, haben sie besondere Aufbewahrungspflichten zu beachten. Diese sind z.B.:

- Patientenakte: zehn Jahre nach Abschluss der Behandlung (§ 630f Abs. 3 BGB)
- Röntgenaufnahmen im Fall einer Untersuchung: zehn Jahre (§ 85 Abs. 2 Nr. 2 Buchst. a StrlSchG) bzw. bei minderjährigen Personen bis Vollendung des 28. Lebensjahrs (§ 85 Abs. 2 Nr. 2 Buchst. b StrlSchG); Röntgenaufnahmen im Fall einer Behandlung: 30 Jahre (§ 85 Abs. 2 Nr. 1 StrlSchG)
- Daten im Zusammenhang mit der Anwendung von Blutprodukten und Arzneimitteln zur spezifischen Therapie von Gerinnungsstörungen bei Hämophilie: 15 bzw. 30 Jahre (§ 14 Abs. 3 TFG)

Diese Beispiele verdeutlichen, dass es eine eindeutige Bezeichnung der Datenkategorien erheblich erleichtert, die Daten später zu löschen. Würde in jeder Verarbeitungstätigkeit lediglich „Gesundheitsdaten" stehen, wäre die jeweils einschlägige Löschfrist nicht sofort ersichtlich.

Technische und organisatorische Maßnahmen

Das VVT enthält gemäß Art. 30 Abs. 1 Satz 2 Buchst. g DSGVO – soweit möglich – auch eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (TOM) nach Art. 32 Abs. 1 DSGVO. Einige Maßnahmen sind stets zu empfehlen, z.B. die IT-Systeme abzusichern oder Beschäftigte regelmäßig zu schulen. Daneben gibt es in Arztpraxen Besonderheiten, die die Durchführung spezifischer TOM erfordern.

So sollte eine Arztpraxis insbesondere vermeiden, dass andere Patienten oder Patientinnen spezifische Kenntnisse über die gesundheitliche Situation einer Person erlangen. Dies kann die Praxis z.B. sicherstellen durch:

- einen separaten Raum für die Anmeldung oder ausreichend Abstand von anderen Patientinnen und Patienten,
- indem das Praxispersonal keine Gesundheitsdaten preisgibt, wenn es jemanden aufruft,
- und indem die Arztpraxis Patientengespräche im Flur oder bei geöffneter Tür des Behandlungszimmers vermeidet.

ACHTUNG!

Obwohl Arztpraxen in vielen Tätigkeiten Gesundheitsdaten verarbeiten, sollten sie die Datenkategorien im VVT nicht in jeder Verarbeitungstätigkeit als „Gesundheitsdaten" bezeichnen. Sinnvoller sind dagegen individuell benannte Datenkategorien. Diese Herangehensweise ermöglicht es Arztpraxen, den Datenkategorien Aufbewahrungsfristen zuzuordnen. Dies erleichtert es später, die Daten zu löschen.

Daniel Lösch, LL.M. ist Rechtsanwalt mit mehrjähriger Erfahrung in den Bereichen Datenschutzrecht, Digitalisierung und Legal Tech.

Bild: iStock.com/Shutthiphong Chandaeng

Sicher eines der alltäglichsten Dateiformate ist das PDF. Inzwischen gibt es je nach Sicherheitsbedürfnis verschiedene Verfahren, PDF vor Komprimittierung zu schützen. Die Kunst ist, das richtige Verfahren zu wählen

Dateien rechtssicher austauschen

Schutz von PDF-Dokumenten: die digitale Signatur

Das Dateiformat PDF kommt für viele Belange des täglichen Lebens zum Einsatz – beruflich und privat. Doch Angreifer finden immer wieder Möglichkeiten, PDFs zu manipulieren und Identitäten zu stehlen. Dieser Artikel stellt Schutzmaßnahmen vor.

PDF-Dokumente (Portable Document Format) sind aus dem betrieblichen und privaten Alltag kaum wegzudenken. PDF ist weit verbreitet, und für fast jedes Betriebssystem gibt es PDF-Reader sowie Anwendungen, um andere Dateiformate (z.B. Microsoft Office) in PDFs umzuwandeln.

So können Kriminelle PDFs missbrauchen

Doch PDF ist kein sicheres Dateiformat. Mit geeigneten Werkzeugen können Kriminelle PDFs nachträglich manipulieren oder gefälschte PDFs erstellen, einschließlich Briefkopf und Firmenlogo. Sie haben dann leichtes Spiel, mit falschen PDFs Betrügereien zu begehen.

Aber auch PDF-Dateien abzufangen und zu verändern ist eine beliebte Betrugsmethode. So kommen Rechnungen als PDF oft per Mail. Gelingt es Kriminellen, eine Mail abzufangen, können sie die PDF-Rechnung im Anhang mit Software bearbeiten, z.B. die IBAN ändern und das Geld auf das eigene Konto überweisen lassen. Bis der Betrug auffällt, ist das Geld unwiderruflich ins Ausland transferiert.

Es ist also nötig, PDF-Dateien zu schützen, um Manipulationen oder falsche Absenderadressen zu erkennen. Die Werkzeuge dazu gibt es längst, allerdings sind sie noch nicht weit verbreitet. Digitale Signaturen können die Integrität eines PDFs sicherstellen. Sie ermöglichen auch nachzuweisen, dass das PDF tatsächlich von der richtigen Quelle stammt. Dies verhindert Manipulation und Identitätsdiebstahl.

So schützen digitale Signaturen

Die Technik digitaler Signaturen ist schon lange bekannt. Verschlüsselungssoftware erzeugt dazu ein Schlüsselpaar. Der eine Schlüssel (der private) bleibt geheim, der andere (der öffentliche Schlüssel) wird veröffentlicht. Bei der digitalen Signatur berechnet die Software zunächst eine kryptografisch abgesicherte, nicht fälschbare Prüfsumme („Hash“) des Dokuments und verschlüsselt diese anschließend mit dem privaten Schlüssel. Das Dokument geht dann zusammen mit dem verschlüsselten Hash auf die Reise.

Der Empfänger oder die Empfängerin erhält das Dokument und den verschlüsselten Hash und kann nun prüfen, ob das Dokument von der korrekten Quelle stammt oder ob jemand es unterwegs manipuliert hat. Dazu berechnet Software auf Empfangsseite den Hash des Dokuments. Diesen vergleicht sie dann mit dem mitgeschickten Hash, den sie mithilfe des öffentlichen Schlüssels der Quelle entschlüsselt. Stimmen die beiden Werte überein, stammt das Dokument von der erwarteten Person und wurde auf dem Weg zum Ziel nicht manipuliert.

Dieses Verfahren hat aber einen Haken. Es ist nicht garantiert, dass der öffentliche Schlüssel tatsächlich korrekt ist und nicht der von Kriminellen. Erforderlich ist deshalb eine externe, vertrauenswürdige Instanz, die bestätigt, dass der öffentliche Schlüssel echt ist.

Dies erfolgt ebenfalls über eine digitale Signatur. Mittlerweile gibt es gerade im Bereich der Signatur von PDF-Dokumenten zahlreiche Dienstleistungsunternehmen (Trust Services), die sich dieser Aufgabe widmen. Zudem bieten sie Werkzeuge an, um Dokumente zu signieren und die Signatur z.B. von PDF-Dokumenten mit wenigen Mausklicks zu kontrollieren.

Signaturverfahren sind unterschiedlich sicher

Die gerade beschriebene Signatur von Dokumenten ist nur eine Variante bei der Absicherung von PDFs. Es gibt drei Verfahren mit unterschiedlich starkem Schutz:

1. Einfache elektronische Signatur (EES)
2. Fortgeschrittene elektronische Signatur (FES)
3. Qualifizierte elektronische Signatur (QES)

1. Die einfache elektronische Signatur (EES)

Die einfache elektronische Signatur (EES) ist der Standard mit der geringsten Schutzwirkung. Die Anforderungen sind minimal. Es muss sich um digitale Daten handeln, die in irgendeiner Form unterzeichnet sind. Dazu reicht es, ein Bild der Unterschrift im PDF anzuzeigen oder bei einem Online-Dienst den eigenen Namen einzugeben. Die rechtliche Relevanz der EES ist eher bescheiden. Denn Kriminelle können eine eingescannte Unterschrift durch eine andere ersetzen oder sie in einem anderen Zusammenhang präsentieren. Vor Gericht dürfte ein EES-signiertes Dokument nur wenig Beweiskraft haben.

Zum Einsatz kommt EES bei Dokumenten oder Verträgen, die die Beteiligten auch mündlich oder „per Handschlag" in Kraft setzen, z.B. bei einem Angebot oder der Bestätigung einer Bestellung.

2. Die fortgeschrittene elektronische Signatur (FES)

Die fortgeschrittene elektronische Signatur (FES) verlangt, Absender oder Absenderin eindeutig zuzuordnen und zu identifizieren. Zudem ist nachzuweisen, dass niemand das Dokument verändert hat. Dies lässt sich durch eine digitale Signatur wie oben beschrieben erreichen.

Mittels FES lassen sich Verträge, Versicherungen oder Geheimhaltungsvereinbarungen absichern. Vor Gericht sollte ein FES-signiertes Dokument als ausreichendes Beweismittel dienen.

3. Die qualifizierte elektronische Signatur (QES)

Bei der qualifizierten elektronischen Signatur (QES) schließlich sind die Sicherheitsanforderungen noch strenger. QES ist die höchste Stufe der Signatur. Das Verfahren ist wie EES und FES durch die EU-Verordnung eIDAS geregelt. Dabei steht eIDAS für „electronic identification, authentication, and trust services" (elektronische Identifizierungs-, Authentisierungs- und Vertrauensdienste).

QES kommt zum Einsatz, wenn für einen Vertrag die Schriftform vorgeschrieben ist, z.B. elektronisch per PDF. QES ist im Rechtsverkehr gleichgesetzt mit einer handschriftlichen Unterschrift und gilt vor Gericht als Beweismittel.

QES arbeitet wie FES mit Verschlüsselung, um Quelle und Datenintegrität nachzuweisen. Der Schwerpunkt von QES liegt in der besonders hohen Vertrauenswürdigkeit der Signaturen. Dafür sorgen u.a. hohe Anforderungen an die Trust Services. Diese müssen sich regelmäßigen staatlich kontrollierten Zertifizierungen unterziehen.

Einsatzszenarien für Signaturverfahren

Es stellt sich die Frage, welches Signaturverfahren für welche Dokumente einzusetzen ist. Maßgeblich für die Entscheidung ist letztlich das Haftungsrisiko, das mit einem Missbrauch des Dokuments einhergeht. Die Person, die ein Dokument absendet, muss also prüfen, welcher Schaden bei einem Missbrauch für sie eintreten kann. Bei einem geringen Risiko wählt sie EES, bei einem höheren, aber durchaus noch kalkulierbaren Risiko FES, bei einem hohen Risiko QES. QES kommt auch grundsätzlich zum Einsatz, wenn die Schriftform erforderlich ist.

PRAXIS-TIPP

Grundsätzlich sollten Personen, die ein Dokument empfangen, darauf achten, dass die Signatur des Dokuments dem eigenen Risiko entspricht. Ist das nicht der Fall, können sie das Dokument so nicht akzeptieren. Die absendende Seite ist dann aufgefordert, ein adäquates Sicherheitsniveau für das Dokument zu gewährleisten. Ansonsten droht in den Fällen von Identitätsdiebstahl oder der Manipulation von PDF-Dokumenten ein hohes Haftungsrisiko.

Aber auch die Personen, die Dokumente empfangen, müssen sich fragen, welche Risiken sie tragen, wenn sie unsignierte PDFs, EES, FES oder QES nutzen. Bekommen sie etwa ein unsigniertes PDF mit einem größeren Rechnungsbetrag, müssen sie sich fragen, wie groß für sie das Risiko bei einem manipulierten PDF ist. Passt die Sicherheitsstufe des Dokuments nicht zum eigenen Risikoprofil, so sind zusätzliche Maßnahmen erforderlich, im Fall eines unsignierten PDFs zumindest ein Rückruf beim Absender oder der Absenderin.

Zusatzfunktionen von QES

QES umfasst gegenüber FES oder EES einige Zusatzfunktionen für Dokumente mit hohem Schutzbedarf:

- **Elektronische Siegel, die dann nicht mehr natürlichen Personen, sondern juristischen Personen wie etwa Firmen oder Behörden zugeordnet sind.**
- **Elektronische Zeitstempel belegen den Weg des Dokuments in seinem zeitlichen Verlauf beweiskräftig.**
- **Elektronische Einschreiben als rechtsgültiger Nachweis, dass ein Dokument dem Empfänger zugestellt worden ist.**
- **Ein qualifiziertes Zertifikat für Websites garantiert, dass die Einrichtung, die die Website betreibt, vertrauenswürdig ist.**

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

Bild: iStock.com/Olivier Le Moal

Unternehmen arbeiten verteilt (Remote Work) und verwenden zunehmend Cloud-Dienste anstelle interner Server und Anwendungen. Das IT-Team kann sie deshalb nicht mehr zentral absichern.

Keine Cybersicherheit ohne Datenschutz (Teil 1)

Zero Trust darf nicht „kein Datenschutz" bedeuten

Aufgrund hoher Schäden durch Cyberattacken investieren Unternehmen stark in Cybersicherheit. Mit neuen Konzepten wie Zero-Trust-Sicherheit wollen sie steigende Risiken in den Griff bekommen. Dabei dürfen sie aber die Grenzen des Datenschutzes nicht überschreiten.

Frühere Cybersicherheitskonzepte gingen davon aus, dass die Bedrohungen immer von außerhalb kommen. Inzwischen aber haben sich die Ansätze verändert.

Zero Trust bedeutet, in der Cybersicherheit umzudenken

Unternehmen müssen sich bewusst machen, dass oft die eigenen Beschäftigten die Sicherheitsvorfälle verursachen, ungewollt oder absichtlich. Man spricht von Innentätern und Insider-Attacken.

Deshalb sagen Sicherheitskonzepte wie „Zero Trust": Vertraue niemanden, überprüfe alles, ganz gleich, ob extern oder intern!

Zero Trust ist schwer umzusetzen

Auch wenn das Prinzip von Zero Trust einfach klingt, viele Unternehmen haben Schwierigkeiten mit diesem Sicherheitsansatz. So erwartet das Analystenhaus Gartner (https://ogy.de/ckhp), dass nur 10 % der großen Unternehmen bis 2026 über ein ausgereiftes und messbares Zero-Trust-Programm verfügen werden. Alle anderen Unternehmen setzen Zero Trust nur unvollständig um. Darunter kann der Datenschutz leiden.

Auch das BSI (Bundesamt für Sicherheit in der Informationstechnik) sieht eine ganzheitliche, wirksame Umsetzung von Zero-Trust-Prinzipien als langfristiges Vorhaben. Es erfordert hohen wie dauerhaften finanziellen sowie personellen Ressourcenaufwand. Vernetzen sich Organisationen, müssen die Beteiligten die Zero-Trust-Konzepte verbindlich abstimmen, so das BSI. Dies stelle heute, u.a. aufgrund fehlender Standardisierung, noch eine große Herausforderung dar.

Zero Trust hat Vor- und Nachteile für den Datenschutz

Ohne Zweifel bietet Zero Trust Möglichkeiten, die Risiken durch Cloud-Nutzung und verteiltes Arbeiten zu verringern. Entsprechend profitiert auch der Datenschutz. Ganz generell kann man sagen, dass der moderne Datenschutz nicht mehr ohne Cybersicherheit auskommt (wir berichteten in der Reihe „Datenschutz und Cybersicherheit").

Allerdings darf man es nicht versäumen, die neuen Sicherheitskonzepte auch aus Datenschutzsicht zu betrachten. So erklärt z.B. das BSI in seiner Information zu Zero Trust: „Zu den wichtigsten Aspekten von Zero Trust gehört: Protokollierung, Monitoring und Analyse sämtlicher Aktivitäten und falls nötig das sofortige Ergreifen von Gegenmaßnahmen."

Offensichtlich haben „Protokollierung, Monitoring und Analyse sämtlicher Aktivitäten" eine Folge für den Datenschutz. Schließlich sollen die IT-Systeme den Nutzenden erst nach Prüfung vertrauen. Es geht also bei Zero Trust insbesondere

ONLINE-TIPP

Mit einem Positionspapier (https://ogy.de/67uo) möchte das BSI die konzeptionellen Grundlagen von Zero Trust vermitteln, eine Diskussionsgrundlage schaffen und erste Ansätze skizzieren. Ergänzend betrachtet das Papier erste organisationsübergreifende Zero-Trust-Ansätze.
Um das Management über Zero Trust aufzuklären, bietet das BSI auch eine Kurzinformation an, das „Management Blitzlicht – Zero Trust" (https://ogy.de/bsi-zero-trust).

auch um Protokollierung, Monitoring und Analyse sämtlicher Aktivitäten der Nutzerinnen und Nutzer.

Besserer Datenschutz bei Zero Trust

Wenn man die Sicherheitssysteme im Sinne von Zero Trust alles überwachen, protokollieren und analysieren lässt, dann mutiert Zero Trust schnell zu „Zero Privacy" (kein Datenschutz bzw. keine Privatsphäre). Denn Sicherheitssoftware würde dann alle Nutzenden bei ihren Aktivitäten mit IT und Daten durchleuchten.

Datenschutzfreundliche Ansätze für Zero Trust arbeiten stattdessen so:

- Fordern Nutzende Zugriff auf Serverressourcen an, bleibt dabei die Privatsphäre geschützt. Die Serveradministration kann das Zugriffsverhalten der Nutzenden nicht ohne Weiteres einsehen oder an Dritte weitergeben.
- Dazu ordnet die IT-Sicherheitssoftware den gewünschten Zugriff einem Pseudonym zu. Selbst die Administration kann dieses nur auflösen, wenn es ein definiertes Vier-Augen-Prinzip einhält.
- Grundsätzlich werden also die personenbezogenen und personenbeziehbaren Informationen aus der Protokollierung, die das Administrationsteam einsehen kann, entfernt. Dies gilt besonders für eindeutige Geräte-IDs, die Personenbezug haben können, IP-Adressen oder Mail-Adressen, die häufig in den Zugangsdaten enthalten sind.
- Nur eine spezielle Rolle darf nach Vier-Augen-Prinzip die vollständige Protokollierung einsehen. Dies beschränkt sich auf die Protokollierung zum aufgefallenen Pseudonym.

Was Datenschutzbeauftragte jetzt tun sollten

Die meisten Unternehmen sind erst dabei, Zero-Trust-Konzepte einzuführen, wie die genannte Prognose von Gartner zeigt. Es ist also die richtige Zeit dafür, die genaue Zero-Trust-Implementierung zu hinterfragen und auf den Datenschutz zu pochen.

Im Mittelpunkt des Datenschutzes stehen alle personenbeziehbaren und personenbezogenen Daten. Diese hängen mit dem Identitätsmanagement als Teil von Zero Trust zusammen: Jede Nutzerin, jeder Nutzer muss ihre bzw. seine Identität nachweisen. Die Zero-Trust-Software bestimmt das Risiko (z.B. anhand des Aktivitätsmusters). Auf dieser Grundlage erteilt oder verwehrt sie die Berechtigungen.

Deshalb sollten die betrieblichen Datenschutzbeauftragten (DSB) die folgenden Funktionen von Zero Trust aus Datenschutzsicht abklopfen:

- Identitätsmanagement: technische Systeme, Richtlinien und Prozesse, die den Besitz, die Nutzung und den Schutz von Identitätsinformationen erstellen, definieren, steuern und synchronisieren, um einer Person digitale Identitäten zuzuordnen.
- Berechtigungsverwaltung: technische Systeme, Richtlinien und Prozesse, die eine digitale Identität an eine Person binden und dies aufrechterhalten. Dazu gehört, die Notwendigkeit eines Berechtigungsnachweises festzustellen, den Berechtigungsnachweis zu registrieren, zu erstellen bzw. auszustellen und ihn während seines gesamten Lebenszyklus zu bewahren.
- Zugriffsverwaltung: Verwaltung und Kontrolle der Mechanismen, die dazu dienen, Zugriff auf Ressourcen zu gewähren oder zu verweigern. Dazu zählt die Zusicherung, dass die Software Identitäten ordnungsgemäß validiert und prüft, ob sie zum Zugriff auf die Ressourcen berechtigt sind.

Dabei müssen DSB jeweils die Frage stellen: Wie sind die personenbezogenen und personenbeziehbaren Informationen in den Security-Funktionen geschützt, sodass sich Auswertungen für Zero Trust nur mit Vier-Augen-Prinzip und konkretem Anlass auf bestimmte Nutzende zurückführen lassen?

Oliver Schonschek ist freier Fachjournalist, News-Analyst und Tech Journalist. Er moderiert regelmäßig den Podcast von Datenschutz PRAXIS. Gleich reinhören unter www.datenschutz-praxis.de/podcasts/!

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:
Jochen Hortschansky
Kurt Skupin

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

Anzeigen:
Anton Sigllechner
Telefon: 0 82 33.23-72 68
Fax: 0 82 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 33.23-74 00
E-Mail: service@weka.de

Abonnementpreis:
12 Ausgaben Print + Online-Zugriff 279 € (zzgl. MwSt. und Versandkosten)
12 Ausgaben als PDF im Heftarchiv + Online-Zugriff 269 € (zzgl. MwSt.)

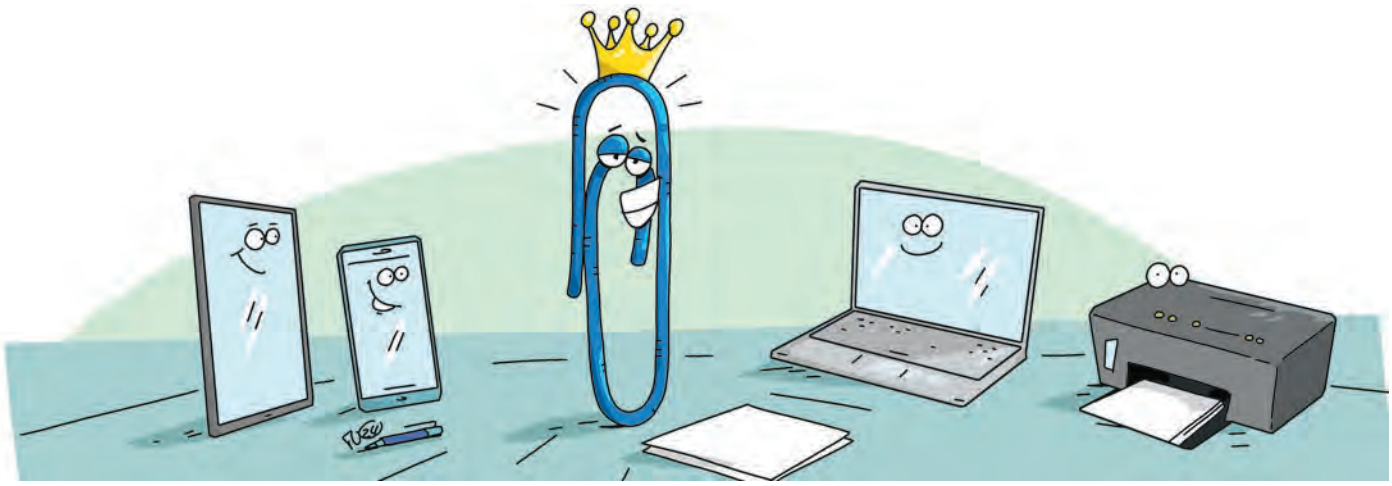
Druck:
Burscheid Medien GmbH
Leonhardstraße 23, 88471 Laupheim

Layout & Satz:
METAMEDIEN
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4126

ISSN:
1614-6867

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



Die Büroklammer!

AI (Analoge Intelligenz) in Perfektion

In der Welt der Technologie, wo Innovation und Komplexität Hand in Hand gehen, gibt es nicht nur für Datenschutzbeauftragte ein unscheinbares, aber vielseitiges Werkzeug, das in seiner Simplizität und Effizienz besticht: die Büroklammer. Ein Meisterwerk der analogen Intelligenz, das in der IT-Welt unverzichtbar ist.

Eine der häufigsten Anwendungen der Büroklammer: der Reset. Ob Notebooks oder Router – die Büroklammer ist klein und stabil genug, um die Reset-Taste zu erreichen. Ein einfacher Druck setzt ein Gerät zurück, bei dem die digitale Lösung einfach nicht funktioniert.

Ein weiterer klassischer Einsatzbereich ist das Öffnen von SIM-Kartenschächten in Smartphones und Tablets. Hier kommt die Büroklammer ins Spiel, die perfekt passt und den Mechanismus mühelos aktiviert.

Kabelbinder & Staubwedel …

Verdrillen Sie Büroklammern zu einer Kette, um lose Kabel zusammenzuhalten. Entfernen Sie Staub in schwer zugänglichen Bereichen von Tastaturen und Druckern. Genial als CD-/DVD-Laufwerksöffner: Wenn der Auswurfknopf versagt, lässt sich die Büroklammer in das kleine Loch neben dem Laufwerksschacht einführen, um die Scheibe manuell auszuwerfen.

… Schraubendreher & Blockadelöser

Kleiner Schraubendreher: Eine zurechtgebogene Büroklammer kann kleine Schrauben anziehen oder lösen. Nicht zu vergessen der Reset von Festplatten: Bei einigen älteren Festplattenmodellen lässt sich mit einer Büroklammer eine manuelle Fehlerbehebung durchführen. Und last but not least das Entfernen blockierter Objekte: Ob festsitzender Papierstau im Drucker oder klemmender Schlüssel – die Büroklammer bietet die schnelle Lösung.

Tipp vom Profi: Immer eine in der Tasche

Die Büroklammer, dieses kleine Stück gebogenen Metalls, ist das unentbehrliche analoge Werkzeuge in einer digitalen Welt. In ihrer Einfachheit liegt ihre Stärke und in ihrer Vielseitigkeit ihre Unverzichtbarkeit. AI – Analoge Intelligenz – feiert mit der Büroklammer echte Triumphe!

PS: Ich habe immer eine in der Tasche!

Eberhard Häcker ist seit vielen Jahren selbstständig und mit großer Leidenschaft sowie Kreativität externer Datenschutzbeauftragter.

In der nächsten Ausgabe

Auftragsdatenverarbeitung
Auskunftsanspruch gegen Verantwortliche

Best Practice
MS Copilot

Cybersicherheit
Datenschutz bei SASE