www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT | Mai 2022

Bild: iStock.com/useng

Alle Optionen offenhalten? Das ist bei der Datenverarbeitung aus Datenschutzsicht keine gute Idee.

Verarbeitungszwecke festlegen

Wie konkret muss die Zweckbestimmung ausfallen?

Wer nicht weiß, warum er eigentlich bestimmte personenbezogene Daten verarbeitet, hat ein massives Problem. Und das nicht nur mit der Datenschutzaufsicht, sondern oft auch mit den eigenen Prozessen. Also gilt es, sich im Vorfeld einer Verarbeitung den Zweck bewusst zu machen.

Verantwortliche müssen personenbezogene Daten ganz allgemein nach dem Zweckbindungsgrundsatz der Datenschutz-Grundverordnung (DSGVO) verarbeiten. An den Verarbeitungszweck knüpft die DSGVO weitere Rechtsfolgen, z.B. die Löschung von Daten, wenn der festgelegte Zweck erreicht ist. Die Umsetzung der Zweckbindung und die konkrete Bestimmung des Verarbeitungszwecks wirft in der Praxis jedoch so einige Fragen auf.

Zweckbestimmung ist Voraussetzung für Verarbeitung

Art. 5 Abs. 1 Buchst. b DSGVO bestimmt, dass Verantwortliche und Auftragsverarbeiter personenbezogene Daten für festgelegte, eindeutige und legitime Zwecke erheben dürfen. Das bedeutet konkreter:

- Zum einen ist eine Rechtsgrundlage für die Verarbeitung nötig, z.B. die Erfüllung eines Vertrags oder die Einwilligung der betroffenen Person.
- Zum anderen heißt das, dass Verantwortliche den Zweck der Verarbeitung von personenbezogenen Daten zwingend VOR der ersten Verarbeitung festlegen müssen.
- Der Zweck muss darüber hinaus eindeutig sein. Eindeutig bedeutet in diesem Fall: Es muss sich klar und ohne jeden Zweifel feststellen lassen, für welchen Zweck bestimmte Daten verarbeitet werden sollen.

Verstoß gegen Zweckbindung

Die DSGVO sieht bei Verstößen gegen die Grundsätze der Verarbeitung, wozu auch die Zweckbindung gehört, vor, dass die Datenschutzaufsichtsbehörden Geldbußen verhängen können. Sie können →

Editorial

Ricarda Veidt,
Chefredakteurin

Ein Experiment

Liebe Leserin, lieber Leser! Sicher treffen auch Sie immer wieder auf Menschen, die meinen, sie hätten doch nichts zu verbergen und der ganze Datenschutz-Quatsch sei völlig übertrieben. Sehr wirksam finde ich in solchen Situationen die Frage, die einer meiner geschätzten Kollegen gern stellt: „Und warum hast Du in Deiner Wohnung dann Vorhänge vor dem Fenster?"

Vielleicht kommt daraufhin der Versuch, zu erklären, dass es doch etwas ganz anderes sei, ob einem jemand ins Schlafzimmer schauen könne oder ob er lediglich mitbekäme, was man an Harmlosigkeiten bei Google suche oder auf Instagram & Co. poste. Dass die vermeintlichen Harmlosigkeiten z.T. äußerst tiefe Einblicke erlauben, zeigt das Projekt „Made to Measure – eine digitale Spurensuche" eindrucksvoll (abrufbar unter https://madetomeasure.online/de/).

Nominiert für den diesjährigen Datenschutz-Medienpreis des BvD, konstruiert das Datenexperiment den Doppelgänger einer Person aus Online-Daten und zeigt, wie durchsichtig uns allein schon Google macht. Sehr sehenswert!

Herzlichst
Ihre Ricarda Veidt

bis zu 20 Mio. Euro oder 4 % des weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs des Unternehmens betragen. Für Verantwortliche ist es auch aus diesem Grund wichtig, die Verarbeitungszwecke sorgfältig festzulegen.

BEISPIEL

Ein Beispiel für ein erhebliches Bußgeld bei Überschreiten der Zweckbindung (fehlendes Löschen nach Zweckerreichung) ist das Verfahren der Berliner Beauftragten für Datenschutz und Informationsfreiheit gegen die Immobiliengesellschaft Deutsche Wohnen SE. Das Bußgeld betrug 14,5 Mio. Euro, da die Immobiliengesellschaft persönliche Daten von Mietern jahrelang ohne Verarbeitungszweck gespeichert hatte. Allerdings steht dieses Bußgeld unter Vorbehalt. Derzeit ist das Verfahren beim Kammergericht Berlin ausgesetzt, da es dem Europäischen Gerichtshof einige Fragen zur Klärung vorgelegt hat. Zum Bußgeld gegen die Deutsche Wohnen siehe Dr. Ehmann in Heft 06/2021, https://ogy.de/dp-geldbussen-nach-dsgvo.

Folgen einer Zweckbindung

Einen Verarbeitungszweck festzulegen, wirkt sich in verschiedenen Bereichen aus, die die DSGVO regelt. Dazu gehören:

- die Information betroffener Personen nach Art. 13 und 14 DSGVO: Verantwortliche müssen die betroffenen Personen über die Zwecke der Datenerhebung unterrichten.
- Rechte betroffener Personen nach Art. 15 DSGVO: Betroffene haben ein Recht auf Auskunft über die Zwecke der Datenverarbeitung gegenüber dem Verantwortlichen.
- das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO: Das Verzeichnis von Verarbeitungstätigkeiten muss den Zweck der jeweiligen Verarbeitungstätigkeit enthalten.
- Rechte betroffener Personen nach Art. 17 DSGVO: Ist der Zweck erreicht oder entfällt er, d.h. benötigt der Verantwortliche die personenbezogenen Daten zu diesem konkreten Zweck nicht mehr, hat die betroffene Person einen Anspruch darauf, dass der Verantwortliche diese Daten löscht.

Erweiterung oder Änderung des ursprünglichen Zwecks

Zunächst gilt nach dem Grundsatz der Datenminimierung in Art. 5 DSGVO: Keine Verarbeitung auf Vorrat!

Den Verarbeitungszweck, den ein Verantwortlicher vor der ersten Erhebung der personenbezogenen Daten festgelegt hat, zu verändern oder zu erweitern, ist nur in eng begrenzten Ausnahmefällen möglich. Ein solcher Fall kann eintreten, wenn ursprünglicher und neuer bzw. geänderter Zweck miteinander vereinbar sind. Dafür muss zwischen den Zwecken ein innerer Zusammenhang bestehen (vgl. Art. 6 Abs. 4 DSGVO und Erwägungsgrund Nr. 50).

Die DSGVO gibt Kriterien vor, anhand derer Datenschutzbeauftragte und Verantwortliche eine Vereinbarkeit der Zwecke prüfen können. Folgende Kriterien sind dabei zu berücksichtigen:

- eine Verbindung zwischen den Zwecken
- der Gesamtzusammenhang, in dem die Daten erhoben wurden

- die Art der personenbezogenen Daten
- mögliche Konsequenzen für die betroffene Person aufgrund der Zweckänderung/-erweiterung
- angemessene Sicherheitsmaßnahmen wie z.B. Verschlüsselung oder Pseudonymisierung der Daten

Sind ursprünglicher und neuer Verarbeitungszweck nicht miteinander vereinbar, müssen Verantwortliche die Datenverarbeitung für den neuen Zweck komplett neu prüfen. Das bedeutet, es muss eine Rechtsgrundlage für diese weitere Verarbeitung vorliegen, und die Informationspflichten gegenüber betroffenen Personen müssen erneut erfüllt werden.

Ein typisches Beispiel aus der Praxis: Daten wurden erhoben, um einen Kaufvertrag zu erfüllen. Jetzt sollen sie zum Einsatz kommen, um den Kundinnen und Kunden Werbung zuzusenden.

Auswirkungen auf die Praxis

Aus diesen grundsätzlichen Regelungen der DSGVO ergibt sich, dass Verantwortliche den Verarbeitungszweck jeweils so konkret wie möglich angeben sollten. Das erleichtert es, mit den „Rechtsfolgen" wie der Löschung umzugehen. Und Verantwortliche wissen genau, wann sich beispielsweise ein Zweck ändert oder erweitert, und können mit den entsprechenden Maßnahmen darauf reagieren.

Ohne dass sie die Zwecke konkret festlegen, laufen Verantwortliche stets Gefahr, dass die Datenschutzaufsichtsbehörde gegen sie vorgeht. Denn sie wissen überhaupt nicht, wann z.B. ein Verarbeitungszweck erreicht ist und sie damit die betreffenden Daten löschen müssen. Die Faustformel lautet also: Zwecke der Verarbeitung möglichst konkret bestimmen!

Nutzen Sie die nachfolgenden Beispiele für verschiedene Verarbeitungssituationen, um sich zu orientieren und Verantwortliche zu beraten. Die Tabelle bietet einen guten Überblick. Sie umfasst jedoch natürlich nicht alle infrage kommenden Konstellationen. Sie kann dann aber Anhaltspunkte dafür geben, was in ähnlich gelagerten Fällen sinnvoll ist.

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

Beispiele für konkrete Zweckbestimmungen

Datenkategorie oder Verarbeitungsart	Zweck Do	Zweck Don't
Adresse	Versand bestellter Ware	Vertragserfüllung
	Weitergabe an Logistikdienstleister, um die bestellte Ware zu transportieren	Weitergabe an Dritte
	Zusendung von Werbung	Weitergabe an Dritte/Werbung
Name, Adresse, sonstige Kontaktdaten (Angabe durch betroffene Person freiwillig in Kontaktformular auf Website)	zur Bearbeitung Ihrer Kontaktanfrage/ Ihres Anliegens	keine Zweckbestimmung
E-Mail-Adresse	Vertragsbestätigung im Online-Handel	Vertragserfüllung
	Sendungsverfolgung bzgl. Transport der bestellten Ware/ Weitergabe an Logistikdienstleister	Weitergabe an Dritte
	Versand eines Newsletters zum Unternehmen	
	Zusendung von Werbung/Neuigkeiten über das eigene Unternehmen/neue Produkte	Werbung
Telefon-Nr.	zur Abstimmung eines konkreten Liefertermins bei Warenanlieferung durch eine Spedition	um Sie zu kontaktieren
	zur Nachfrage bei kundenspezifischen Spezialanfertigungen	um Sie zu kontaktieren
Geburtsdatum	zur Einhaltung von Jugendschutzbestimmungen (z.B. Versand von Alkohol)	Vertragserfüllung
	zur Überprüfung der Kreditwürdigkeit/zum Einholen von Bonitätsprüfungen bei der Auskunftei xy (konkret benennen)	Vertragserfüllung/ Sicherstellen der Zahlung
Bankverbindung	bei Beschäftigten: zur Überweisung des Arbeitsentgelts	Personalakte/Personalunterlagen
	bei Kaufverträgen: zur Überweisung des Entgelts (z.B. bei Vorkasse-Regelungen)	Vertragserfüllung

Beispiele für konkrete Zweckbestimmungen		
Datenkategorie oder Verarbeitungsart	**Zweck Do**	**Zweck Don't**
Steuer-ID	bei Beschäftigten: Einbehalt und Abrechnung der Einkommenssteuer mit den Finanzbehörden	Personalakte/Personalunterlagen
Sozialversicherungsnummer	bei Beschäftigten: Einbehalt und Abrechnung des Arbeitnehmeranteils zur gesetzlichen Rentenversicherung	Personalakte/Personalunterlagen
Krankenversicherung	zur Überweisung von Arbeitgeber- und Arbeitnehmeranteil zur Krankenversicherung	Personalakte/Personalunterlagen
Gesundheitsdaten (durch Arzt, Krankenhaus)	bei gesetzlich Krankenversicherten: zur Abrechnung mit der gesetzlichen Krankenkasse	Abrechnungszwecke
	bei privat Krankenversicherten: zur Weitergabe an Abrechnungsdienstleister	Abrechnungszwecke
	für die ärztliche Dokumentation	Arztvertrag
Gesundheitsdaten („krank" mit Arbeitsunfähigkeitsbescheinigung durch Arbeitgeber)	zur Berechnung der Dauer der gesetzlich vorgeschriebenen Entgeltfortzahlung nach Entgeltfortzahlungsgesetz/ für das Angebot der Durchführung von Maßnahmen des Betrieblichen Eingliederungsmanagements (BEM)	Personalakte/Gesundheitsvorsorge
Gesundheitsdaten (durch Arbeitgeber)	zur Durchführung gesetzlich vorgeschriebener arbeitsmedizinischer Vorsorgeuntersuchungen	Arbeitsschutz
Server-Log-Files (Uhrzeit des Aufrufs einer Website, URL der aufrufenden Webseite, das Betriebssystem der aufrufenden Website, Typ und Version des verwendeten Browsers, IP-Adresse des aufrufenden Computers	Aufrufbarkeit der Website Korrekte Darstellung der aufgerufenen Website Sicherstellung der Systemsicherheit der aufgerufenen Website	Funktion der Website
Technisch erforderliche Cookies	reibungsloses Funktionieren einer Website	Betrieb der Internetpräsenz
Cookies (Marketing)	zum Anzeigen ausgewählter Werbung über das eigene Unternehmen/konkret benannter Dritter	Werbung
Cookies (Analyse)	zur Reichweitenmessung einer Website und zur Optimierung einer Website	Verbesserung unseres Angebots
IP-Adresse/Online-Kennung/Gerätekennung (bei Webanalyse)	Analyse des Nutzerverhaltens auf der Website zur Verbesserung des Webangebots	Nutzeranalyse
IP-Adresse/Online-Kennung/Gerätekennung (bei Einwilligungen/Cookies)	zur Protokollierung der Einwilligung	Dokumentation
IP-Adresse (über Cookies/WebBeacons bei Verwendung von reCaptcha o.Ä. auf Website)	zur Feststellung, ob Eingaben auf einer Website von einer echten Person oder einem Bot erfolgen	Schutz der Website
Videoüberwachung (Aufnahmen werden nicht gespeichert)	zur Verhinderung von Straftaten (Zweck gilt dann nur für die Kamera, da keine Speicherung stattfindet)	Sicherheit
Videoüberwachung (mit Speicherung)	zur Aufklärung von Straftaten	Sicherheit
Aufzeichnung von Telefongesprächen	zur Ausbildung und Schulung unserer Mitarbeiterinnen und Mitarbeiter (im Führen von Telefonaten oder im Umgang mit Kunden)	Personalweiterbildung
Angabe des Arbeitgebers (z.B. bei Wohnungsmietern)	um im Falle einer Nichtzahlung den Arbeitgeber zwecks Pfändung des Lohns zu kontaktieren	zur Sicherstellung der Mietzahlung
Vorlage des Personalausweises (z.B. bei Banken)	zur Überprüfung der Identität	Sicherheit

Überblick: Dos & Don'ts bei der Zweckbestimmung

Bild: iStock.com/Geber86

Mitarbeitersensibilisierung ganz subjektiv

Ein Musterschreiben: „Datenschutz gestaltet das Unternehmen – und das ist gut so!“

Schulungen in Präsenz und online, Newsletter, Fachbeiträge, Communities … was machen Datenschutzbeauftragte nicht alles, um Mitarbeiter zu sensibilisieren. Probieren Sie doch einmal etwas Neues und teilen Sie subjektiv geprägt Ihre Einschätzungen und Erfahrungen mit. Um Ihnen eine Vorstellung zu geben, wie so etwas aussehen könnte, finden Sie hier und online als Word-Datei unter www.datenschutz-praxis.de den Musterbrief eines Datenschutzbeauftragten an die Mitarbeiterinnen und Mitarbeiter. Achtung, keine Paragrafen nennen und so wenig rechtliche Ausführungen wie möglich machen!

„Liebe Mitarbeiterinnen und Mitarbeiter,

heute erhalten Sie von mir eine Information, um Ihnen aus meiner Sicht zu zeigen, warum ich Datenschutz wichtig finde. Und ich hoffe stark, dass ich Sie ein bisschen davon überzeugen kann.

Wir Datenschützer im Unternehmen müssen dicke Bretter bohren und bekommen viel Gegenwind! Warum? Wir kümmern uns darum, dass jeder im Betrieb die datenschutzrechtlichen Anforderungen kennt und umsetzt. Doch leider wird der Datenschutz oft als bürokratisch, Showstopper oder einfach als überflüssig empfunden. Das kommt teilweise dadurch zustande, dass Medien bestimmte Themen ausschlachten oder sie zu Unrecht dem Datenschutz zugeschrieben werden, um von anderen Unzulänglichkeiten abzulenken. Besonders Politikerinnen und Politiker machen das gern. Denken wir etwa an die Posse um die Klingelschilder, die angeblich nach Einführung der Datenschutz-Grundverordnung (DSGVO) nicht mehr möglich waren. Völliger Blödsinn!

Ein Plädoyer pro Datenschutz

Nachfolgend möchte ich Ihnen aus meiner Erfahrung aufzeigen, wie die Anforderungen von Bundesdatenschutzgesetz (BDSG) und DSGVO das Unternehmen gestalten. Ein Plädoyer pro Datenschutz, lassen Sie sich darauf ein!

Worum geht es nochmal kurz?

Die DSGVO hat das Ziel, die Grundrechte und Grundfreiheiten natürlicher Personen und deren Daten zu schützen. Also auch von Ihnen, liebe Leser und Leserinnen. In Ihren vielfältigen Rollen als Bürger, Kundin, Arbeitnehmer, Bewerberin, Interessent, Mieterin etc. sind Sie nämlich die sogenannten „betroffenen Personen“. Was für ein vielsagender, einfacher Begriff!

Das Tolle an der DSGVO ist, dass sie als Verordnung europaweit einheitlich gilt. Dass sie überhaupt zustande kam, ist ein reines Wunder bei der ganzen Lobbyarbeit, die gegen sie gerichtet war. Mittlerweile kopiert selbst China sie, man kann es kaum glauben!

Die DSGVO ist für Sie wichtig, da Sie in einer zunehmend vernetzten, digitalen Welt unzählige Spuren hinterlassen, die, je mehr man sie zusammenfügt, Sie komplett analysieren können. Vielleicht kommt mancher Anbieter sogar durch Analysen auf Eigenschaften, die Sie →

sich vielleicht selbst gar nicht eingestehen würden. Sie glauben gar nicht, worauf die Algorithmen kommen können.

Überlegen Sie nur einmal, was Ihr Einkaufsverhalten, Ihr Zahlungsverkehr, Ihr Medienkonsum bei Netflix & Co., Ihr Karteneinsatz etc. alles über Sie aussagen könnten?! Und was, wenn man das auch noch alles zusammenführt?! Gut, dass es die Grundsätze der Zweckbindung und der Rechtmäßigkeit gibt und man das nicht vermischen darf! Gott sei Dank gibt es auch kein Sozialpunktesystem wie in China, das brave Bürger ermittelt und bevorzugt behandelt. Jedenfalls möchte ich selbst kein Bürger des Monats werden – Sie hoffentlich auch nicht?!

Die Datenschutzbeauftragten – Anwälte der Betroffenen

Die Datenschutzbeauftragten (DSB) in Unternehmen und Behörden haben die Aufgabe, das Unternehmen bzw. die Behörde als sogenannte (Daten-)Verantwortliche zu beraten, die Einhaltung der Vorschriften zu überwachen und Ansprechpartner für die Datenschutzaufsicht, also die Landesdatenschutzbeauftragten, zu sein. Wir sind für den Schutz Ihrer Persönlichkeitsrechte und aller sonstigen betroffenen Personen da.

Apropos „betroffene Personen“: Das sind übrigens auch Sie als Mitarbeiter oder Mitarbeiterin. Wie heißt es so schön in der DSGVO: „Die Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen“. Besser kann man es nicht ausdrücken! Damit ist der Datenschutzbeauftragte auch eine Art unabhängiger Anwalt der betroffenen Personen, und nicht immer passt das zu den Interessen, die das Unternehmen verfolgt.

Nicht in allen Fällen ist die Revision oder die Compliance-Abteilung des Mitarbeiters Freund, da sie viel über Sie erfahren und analysieren möchten. Aber machen Sie sich keine Gedanken, ich sorge dafür, dass der Arbeitgeber die manchmal konträren Interessenlagen sorgfältig abwägt. So kommen wir meistens zu gut vertretbaren Kompromissen.

Ein wichtiger Indikator: die Reaktionen der betroffenen Personen

Alle Studien zeigen: Kundinnen und Mitarbeiter erwarten, dass ein Unternehmen korrekt und sicher mit ihren Daten umgeht. Ist das Verhältnis zu ihnen gestört,

- reagieren sie in Form von Datenschutz-Beschwerden,
- unterstellen, dass das Unternehmen unberechtigt auf ihre Daten zugegriffen hat,
- wollen Auskunft über ihre Daten und
- verlangen, dass das Unternehmen restlos alle Daten löscht.

Diese Rechte stehen ihnen tatsächlich zu. Dafür wenden sie sich in den meisten Fällen direkt an den Datenschutzbeauftragen. Da kommt bei kundenorientierten Unternehmen einiges zusammen.

Kritische Kunden überlegen: „Will ich Werbung?“ „Sollen mein Surfverhalten oder meine Chats analysiert werden?“, „Was gibt es für Warnvermerke über mich und warum bekomme ich kein Produkt bei dem Unternehmen, bin ich auf einer schwarzen Liste?“

Über die letzten Jahre hat die Anzahl der Kunden, die hier sensibel reagieren, sehr stark zugenommen. Datenschutzbeauftragte merken bei jeder größeren Vertriebsaktion, ob sie vernünftig geplant ist und bei den Kunden gut ankommt oder nicht.

Läuft es für Sie als Mitarbeiterin oder Mitarbeiter rund, sind Sie zuverlässig, haben Sie keine Abmahnungen oder Ermahnungen, ein leeres polizeiliches Führungszeugnis, gute Beurteilungen, bei Prüfhandlungen, Überwachungsmaßnahmen oder beim Hinweisgebersystem sind Sie nicht aufgefallen, im Privatleben ist alles in Ordnung und Sie müssen keine Angst haben, dass Ihre Partnerin oder Ihr Partner gegen Sie vorgeht, dann überlegen Sie vielleicht – noch – nicht, ob Ihre Daten rechtmäßig erhoben, zweckgebunden verwendet und rechtzeitig gelöscht werden. Doch was, wenn nicht alles so gut läuft?

Meine Hauptaufgabe: die Beratung – da gibt es ein paar Datenschutzgrundsätze, die viel bewirken!

Ein zentraler Punkt bei meiner Beratung sind die Datenschutzgrundsätze. Das hört sich zunächst trocken an. Doch diese Grundsätze haben eine wirklich große Gestaltungswirkung:

- rechtmäßige Datenverarbeitung
- Transparenz
- Zweckbindung
- Datenminimierung
- Datenrichtigkeit
- Recht auf Vergessenwerden etc.

Meine erste Frage: Warum?

Im ganzen Unternehmen verarbeiten die Kolleginnen und Kollegen automatisiert Daten. Daher ist eine meiner ersten Fragen, warum und zu welchem Zweck sie jeweils die Daten verarbeiten. Das ist meines Erachtens übrigens auch ohne Datenschutzbezug eine berechtigte Frage … Doch manche Kolleginnen und Kollegen reagieren sehr erstaunt darauf!

Bekomme ich auf diese Frage keine sinnvolle Erläuterung, ist die Datenverarbeitung schlicht und einfach rechtswidrig! Es muss einen betrieblichen oder gesetzlichen Grund für die Datenverarbeitung geben. Zur Not weg damit: Löschen Sie die Daten!

Projekte von Beginn an datenschutzkonform aufsetzen

Berate ich durch diese „Brille“ Anwendungsverantwortliche im Unternehmen, können Sie sich vorstellen, dass viele Anwendungen oder Systeme anders umgesetzt werden, als sie vorher geplant waren. Oft fallen nicht notwendige Daten oder Auswertungen weg, wir schränken den Zugriff auf Daten ein oder implementieren Löschfristen, die den gesetzlichen oder betrieblichen Erfordernissen entsprechen. Fast alle Projekte berate ich durchgehend oder an der ein oder ande-

ren Stelle, sodass bereits das Konzept den Datenschutz berücksichtigt.

Manche Anwendungen sind besonders sensibel!

Besonders sensibel heißt, dass z.B.

- Leistungskontrollen möglich sind,
- Gesundheitsdaten,
- biometrische Daten oder
- Daten von Minderjährigen verarbeitet werden,
- künstliche Intelligenz,
- Videoüberwachung oder
- Ortungsdienste zum Einsatz kommen.

Hier sieht die DSGVO eine sogenannte Datenschutz-Folgenabschätzung (DSFA) vor. Bevor ein Verantwortlicher diese sensiblen Anwendungen oder Prozesse einführt, muss er überlegen, welche Risiken für die betroffenen Personen vorhanden sein könnten und welche Maßnahmen er trifft, um sie zu minimieren.

Da kann es durchaus sein, dass Anwendungen nicht eingeführt werden können. Das gilt etwa, wenn Personen auf Basis künstlicher Intelligenz ausschließlich automatisiert bewertet werden sollen. Das ist aber nicht die Regel: Oft lassen sich die technischen und organisatorischen Maßnahmen, z.B. das Berechtigungs- oder Löschkonzept oder Regelwerke, die den Umgang beschreiben, so gestalten, dass der Einsatz datenschutzkonform wird. Ein Datenschutz-Qualitäts-Check im Unternehmen sozusagen!

Was keiner braucht: Datenschutzverletzungen

Die falschen Empfänger haben eine E-Mail erhalten, ein Kollege hat einen offenen Mailverteiler verwendet, Angreifer haben Daten gehackt oder es kamen anderweitig personenbezogene Daten abhanden – übrigens auch bei eingesetzten Dienstleistern: In solchen Fällen muss der Datenschutzbeauftragte von der Datenschutzverletzung wissen.

Die DSGVO zwingt die Unternehmen, sich damit zu beschäftigen und diese Vorfälle nicht unter den Tisch zu kehren. Ist die Datenschutzverletzung zu heikel und mit Risiken verbunden, muss man sie auch extern an den Landesdatenschutzbeauftragten melden und je nach Risiko sogar die Betroffenen informieren. Gelangen beispielsweise heikle Kundenunterlagen mit Bonitätsnachweisen o.Ä. an falsche Empfänger, ist eine Meldung an den Landesdatenschutzbeauftragten fällig.

Dieser durchaus gewollte Druck auf die Unternehmen zwingt oft dazu, Schwachstellen oder fehlende Kontrollen in Prozessen aufzudecken und zu beheben – was letztendlich dafür sorgt, dass wir als Unternehmen mit dem wertvollen Gut, den Daten, sorgsam umgehen.

Welchen Dienstleister nehme ich mit an Bord – alles in die Wolke?

Outsourcing ist ein Trend für alle Unternehmen. Dienstleister sind spezialisierter und oft kostengünstiger. In letzter Zeit kommt ein neuer Trend dazu: Cloud Computing. Hier werden Computer-Ressourcen und oft auch Software dazu eingekauft. Das kann man nicht so ohne Weiteres tun. Maßstab aus Datenschutzsicht ist: Schütze das, was du auslagerst, so, wie du es bei dir selbst tun würdest, und kontrolliere das auch regelmäßig!

Da stellt sich oft die Frage, ob sich das unter diesem Gesichtspunkt wirklich lohnt. Auf jeden Fall müssen Verantwortliche die Dienstleister datenschutzrechtlich prüfen und mögliche Risiken bewerten, bevor sie sie einsetzen. Seit dem Jahr 2020 kommt eine erhöhte Sensibilität dazu, in welche Länder ausgelagert wird. Das liegt an einem Urteil des Europäischen Gerichtshofs, das sich auf Datentransfers in die USA bezieht und dort kein ausreichendes Datenschutzniveau sieht. Das gilt auch für weitere Länder, die problematisch sein könnten.

Lösungs- statt problemorientiert

Wir Datenschützer schauen, was man machen kann: Lassen sich mit dem Cloud-Dienstleister europäische Rechenzentren vereinbaren? Lässt sich der Dienstleister darauf ein, Behördenzugriffe transparent zu machen und sie anzufechten? Sorgt er für eine starke Verschlüsselung? Darauf hinzuwirken, ist unser Job! Und glauben Sie uns, die Datenschützer in Europa haben die großen Cloud-Anbieter ziemlich bearbeitet, und sie bewegen sich in die richtige Richtung. Denn sie möchten in der Regel doch nicht auf das Europageschäft verzichten.

Sind wir froh, dass wir ihn haben!

Ohne hier noch Ausführungen anzufügen, dass sich Datenschutz auch als Demokratieschutz in unserer Gesellschaft verstehen lässt, wirkt er im Unternehmen umfassend zum Schutz aller betroffenen Personen. Damit ist er für uns selbst elementar wichtig.

Ich finde es auch gut, dass die DSGVO 2018 mögliche Bußgelder sehr stark hochgesetzt hat und zudem Schadensersatzforderungen möglich sind. Die höchste Strafe 2021 war mit 746 Mio. gegen Amazon gerichtet. Damit ist die DSGVO kein zahnloser Tiger. Im Datenschutz funktioniert es auch nicht anders als bei anderen Gesetzen: Sind die Bußgelder nicht abschreckend, hält sich niemand dran.

Sie als Mitarbeiter oder Mitarbeiterin haben alle Umgang mit personenbezogenen Daten, und auf Sie kommt es an, dass es nicht zu Verstößen kommt. Als Datenschutzbeauftragter helfe ich Ihnen dabei! Wir sollten den Datenschutz nicht belächeln oder als reine Bürokratie verstehen, sondern froh sein, dass es ihn gibt. Denn er wirkt enorm und gestaltet viel interessenausgleichend mit!

Ihr/e Datenschutzbeauftragte/r

PS: Und wenn Sie nach diesem Artikel eine Frage haben, rufen Sie mich an oder schreiben Sie eine E-Mail. Ich freue mich auf Sie und helfe gern weiter!“

Uwe Hochstein ist stellvertretender Datenschutzbeauftragter der Landesbank Baden-Württemberg und geht im Datenschutz gern neue Wege.

Bild: iStock.com/putilich

Haben Sie einmal das theoretische Grundgerüst, gilt: „Training on the job" ist die beste Möglichkeit, bei Datenschutz-Audits sattelfest zu werden

Wichtige Aufgabe für DSB

Das Datenschutz-Audit in der Praxis – Gegenstand, Inhalte, Anforderungen

Ein Datenschutz-Audit ist ein systematischer und dokumentierter Prozess, um zu prüfen, ob eine Organisation die gesetzlichen Bestimmungen im Bereich des Datenschutzes einhält. Zu einem Audit gehört, Schwächen zu identifizieren und Maßnahmen, um sie zu beseitigen. Ziel ist es, Erkenntnisse über die datenschutzrechtliche Konformität zu erlangen. Lesen Sie, wie Sie dazu am besten vorgehen.

Genehmigte Verhaltensregeln und Zertifizierung

Die typischen Datenschutz-Audits, die ein DSB in der Praxis durchführt, sind zu unterscheiden von den rechtlichen Instrumenten „genehmigte Verhaltensregeln" (Art. 40 DSGVO) und „Zertifizierung" (Art. 42 DSGVO). Beiden gehen zwar ebenfalls „Audits" voraus. Sie haben sich aber bisher in der Praxis noch nicht oder nicht flächendeckend etabliert. Daher besitzen sie für die breite Masse an Unternehmen aktuell nur eine untergeordnete Bedeutung.

Der rechtliche Ausgangspunkt für Datenschutz-Audits findet sich in den Rechenschafts- und den Nachweispflichten (Accountability) des Verantwortlichen (Art. 5 Abs. 2 Datenschutz-Grundverordnung (DSGVO)). Insbesondere um Haftungs-/Bußgeldrisiken zu vermeiden, hat der Verantwortliche ein Interesse daran, zu prüfen, ob er die Anforderungen von DSGVO & Co. erfüllt.

Und Nachweispflichten gibt es in der Grundverordnung einige: Dazu gehören etwa die Datenschutz-Grundsätze (Art. 5 DSGVO), der Nachweis von Einwilligungserklärungen (Art. 7 und 8 DSGVO) oder Datensicherheitsmaßnahmen (Art. 32 DSGVO).

Internes oder externes Datenschutz-Audit?

Die erste Frage, die sich im Zusammenhang mit einem Datenschutz-Audit stellt, ist, wie das Audit im Unternehmen durchgeführt werden soll: intern oder von extern?

- Intern meint, dass Personen, die zum Betrieb gehören, das Audit durchführen. Das betrifft meist die Datenschutzbeauftragten (DSB).
- Extern meint hingegen, dass ein externes Unternehmen ohne Bezug und Zugehörigkeit zum Verantwortlichen, wie etwa ein externes Prüf- und Beratungsunternehmen, das Audit durchführt.

Bei den zahlreichen datenschutzrechtlichen Nachweispflichten kommt folglich Ihnen als DSB (gleich ob intern oder extern) eine wichtige Rolle zu. Schließlich müssen DSB die Einhaltung datenschutzrechtlicher Vorschriften überwachen (Art. 39 Abs. 1 Buchst. b DSGVO). Gerade in kleinen und mittleren Unternehmen (KMU) wird regelmäßig die oder der DSB entsprechende Audits durchführen.

Wer ist an einem Audit beteiligt?

An einem Datenschutz-Audit in der beschriebenen Ausgangskonstellation sind typischerweise die folgenden Parteien beteiligt:

WICHTIG

Datenschutz-Audits sind unabhängig von der Unternehmensgröße und daher auch für KMU von Bedeutung. Denn es geht generell darum, die Einhaltung rechtlicher Anforderungen zu prüfen – ähnlich wie bei einer Kfz-Werkstatt, die ihre Bilanz von einem Steuerberater auf etwaige Fehler und Unstimmigkeiten überprüfen lässt. Auf Basis des Feedbacks, das der Auditor gibt, kann das Unternehmen das Verbesserungspotenzial nutzen und seine internen Abläufe (um-)strukturieren.

- das auditierte Unternehmen (der sogenannte Auditee)
- Mitarbeitende des Unternehmens, z.B. um organisatorisch zu unterstützen
- der oder die DSB als Auditor und – falls vorhanden –
- der Datenschutzkoordinator sowie, je nach Schwerpunkt des Audits,
- ggf. weitere interne oder externe Stellen wie IT-Administratoren oder IT-Sicherheitsbeauftragte

Welche fachlichen Anforderungen müssen Auditoren erfüllen?

Konkrete rechtliche Anforderungen an die Fachkompetenz von Datenschutz-Auditoren sucht man vergebens. Da in den meisten Fällen der DSB das Audit durchführt, sind auf jeden Fall die Anforderungen von Art. 37 Abs. 5 in Verbindung mit Art. 39 DSGVO einzuhalten. Der Grad der fachlichen Kompetenzen richtet sich daher im Wesentlichen nach dem Auditgegenstand sowie der Komplexität der Bewertungen (rechtlich/technisch/prozessual).

Konkretere Voraussetzungen finden sich im Zusammenhang mit der Zertifizierung gemäß Art. 42 und 43 DSGVO. Geht es etwa um die Akkreditierung von Zertifizierungsstellen, so formuliert die Datenschutzkonferenz genauere Vorgaben für die Personalkompetenzen dieser Stellen (siehe https://ogy.de/anforderungen-akkreditierung). Neben allgemeinen Ausführungen (z.B. „Kenntnisse im Datenschutzrecht“) finden sich hier Aussagen zu den fachlichen Voraussetzungen, die sich in die Bereiche „technisch“ und „rechtlich“ unterteilen. Je nach Größe und Komplexität des Unternehmens und des Auditgegenstands kann es sich für Unternehmen anbieten, sich an diesen (hohen) Anforderungen zu orientieren, um eine gute Qualität des Audits sicherzustellen.

Auditscope und Auditvarianten – Worauf soll sich das Audit beziehen?

Um ein Datenschutz-Audit vorzubereiten, ist es essenziell, zunächst den Auditscope zu bestimmen, also festzustellen, was genau Gegenstand des Audits sein soll. Es gibt vier gängige Auditvarianten, die den Scope – zumindest grob – festlegen. Über diese Unterteilung lässt sich das zu auditierende Unternehmen systematisch strukturieren und für das Auditprogramm →

PRAXIS-TIPP

Datenschutz-Audits können ereignisbezogen oder zeitbezogen (z.B. alle 12 Monate) erfolgen. Der DSB als Auditor entscheidet bei allen Varianten und Mischformen, welche Schwerpunkte er individuell setzt und/oder wie tief er prüft, z.B. ob er beteiligte Externe wie Auftragsverarbeiter einbezieht.

Auditvariante	Gegenstand des Audits
Bestandsaufnahme-Audit des DSB und allgemeine/generelle Folgeaudits	Diese generelle Variante bezieht die gesamte Datenverarbeitung des jeweiligen Verantwortlichen in die Auditierung ein, meist jedoch auf einem höheren Abstraktionslevel. Diese Auditvariante führt idealerweise der DSB in KMU zu Beginn seiner Tätigkeit und sodann in regelmäßigen Abständen (z.B. 1 x pro Jahr) durch, um seiner Überwachungspflicht gemäß Art. 39 DSGVO hinreichend nachzukommen.
Sektorspezifisches Audit	Hierbei handelt es sich um eine Unterform des allgemeinen Datenschutz-Audits, aber mit Schwerpunkt auf eine bestimmte Abteilung/Bereiche des Verantwortlichen (z.B. „HR“ oder „Sales/Marketing“). Das Audit prüft die Einhaltung aller (!) datenschutzrechtlichen Pflichten, von der Zulässigkeit der Datenverarbeitung (Art. 6 DSGVO) bis hin zur Sicherheit (Art. 32 DSGVO).
Themenspezifisches Audit	Bei dieser Auditvariante stehen besondere Themen auf der Prüfagenda, z.B. Prüfung der Umsetzung der datenschutzrechtlichen Informationspflichten gemäß Art. 12 bis 14 DSGVO oder Datenschutz-Folgenabschätzung gemäß Art. 35/36 DSGVO. Der Prüffokus liegt hier sehr konzentriert und tiefgehend auf der Umsetzung ganz bestimmter datenschutzrechtlicher Pflichten in allen einschlägigen Bereichen des Unternehmens.
Verarbeitungsprozess-spezifisches Audit	Diese Auditvariante bezieht sich auf die Prüfung ganz bestimmter Verarbeitungen (z.B. „Prüfung des Bewerbermanagements unter Einbezug der Software xyz“) und hat die gesamten datenschutzrechtlichen Pflichten des Unternehmens (DSGVO und weitere, auch nationale Gesetze) hinsichtlich dieser Verarbeitung zum Gegenstand.

Übersicht über Auditvarianten und Auditgegenstände

PRAXIS-TIPP

Je nachdem, wie viele datenschutzrechtliche Vorschriften im Einzelfall einschlägig und daher zu überprüfen sind, gestaltet sich auch das Datenschutz-Audit komplexer. Ein Audit in einer medizinischen Klinik mit zahlreichen Spezialgesetzen benötigt erheblich mehr Vorbereitung als eine Prüfung in einem Industrieunternehmen.

erschließen. Zudem hilft sie, die Prüfbereiche voneinander abzugrenzen.

Am Schluss stehen die sogenannten Re-Audits. Das sind fortführende Audits zu den genannten Auditvarianten. Die nochmalige Auditierung überprüft, ob alle „Findings", also alle gefundenen Schwachstellen, rechtskonform geschlossen wurden (sogenannte „fortlaufende Soll-Ist-Analyse").

Auditkriterien – Woran orientiert man sich beim Datenschutz-Audit?

Nach den Auditvarianten richten sich zumindest teilweise auch die Auditkriterien. Die Frage lautet: „Was wird auf welcher Grundlage geprüft"? In den allermeisten Fällen sind die (abstrakten) Auditkriterien in KMU die einschlägigen datenschutzrechtlichen Vorschriften aus DSGVO, BDSG und weiteren Fachgesetzen.

Daneben gibt es offizielle Managementsysteme, die ihrerseits eigene Auditkriterien aufstellen. Dazu gehört z.B. der British Standard für Datenschutzmanagementsysteme (BS 10012:2017). Aufgrund des enormen Ressourcen-Aufwands sind derartige Managementsysteme und ihre Auditierung/Zertifizierung meist jedoch nur für große, finanzstarke Unternehmen interessant.

Was sind die Hauptkontrollbereiche eines Unternehmens?

Damit, Auditkriterien und Auditvariante festzulegen, ist es nicht getan. Sie bilden quasi den äußeren Rahmen des Audits. Der innere Kern orientiert sich an den Kernbereichen des Unternehmens und ihrer Bedeutung für die interne Umsetzung datenschutzrechtlicher Pflichten. Diese Kontroll-Kernbereiche sind „Recht", „Organisation & Prozesse" sowie „IT" (siehe Tabelle).

BEISPIEL

Um zu veranschaulichen, wie die Auditvarianten und die Kontrollbereiche in der Auditor-Praxis zusammenwirken, ein Beispiel: Sie als DSB haben sich entschieden, die Umsetzung der Informationspflichten zu prüfen. Sie führen also ein themenspezifisches Audit durch. Die Auditkriterien geben in diesem Fall Art. 12 bis Art. 14 DSGVO vor. Anhand der Hauptkontrollbereiche können Sie nun systematisch vorgehen:

- Im Kontrollbereich „Recht" prüfen Sie, ob die Datenschutzinformation rechtlich/inhaltlich korrekt ist und z.B. alle Zwecke und Rechtsgrundlagen genannt sind.
- Im Kontrollbereich „Organisation & Prozesse" prüfen Sie, wer für die Datenschutzinformation (z.B. abteilungsbezogen) verantwortlich/zuständig ist und ob die betroffene Person sie tatsächlich stets zum Zeitpunkt der Erhebung erhält.
- Im Kontrollbereich „IT" prüfen Sie dann, ob das Unternehmen die datensicherheitsrechtlichen Anforderungen (z.B. Art. 25 – Privacy by Design) in Zusammenhang mit der Bereitstellung der Datenschutzinformation einhält. Hat die betroffene Person etwa die Möglichkeit, die Datenschutzinformation in ihrem Kunden-Login (ständig) abzurufen und sie visuell wahrzunehmen?

Wie läuft ein Audit in der Praxis ab?

Ist der Prüffokus klar und definiert, stellt sich die Frage, wie der Auditprozess abläuft. Er gliedert sich in die folgenden Phasen:

Bereich	Kontroll-Fokus
Recht	Dieser Kontrollbereich fokussiert die einschlägigen rein rechtlichen Anforderungen des Datenschutzrechts an das Unternehmen und/oder an einen bestimmten Bereich, z.B. die Vorgabe, den Betroffenen gemäß Art. 13 DSGVO zum Zeitpunkt der Datenerhebung bestimmte Informationen mitzuteilen.
Organisation & Prozesse	Der Kontrollbereich „Organisation & Prozesse" konzentriert sich auf die grundlegenden (Datenschutz-)Prozesse eines Unternehmens, mithin darauf, wie die rechtlichen Vorgaben innerbetrieblich abgebildet werden, wie deren Einhaltung überprüft wird und welche Verantwortungsbereiche existieren. Beispiel: Es reicht nicht aus, eine rechtlich vollständig korrekte Datenschutzinformation gemäß Art. 13 DSGVO in der Schublade zu haben (s. Kontrollbereich „Recht"). Sie muss auch – durch betriebliche Prozesse und Organisation – an die Betroffenen distribuiert werden, etwa durch Übermittlung oder elektronische Bereitstellung. Ob diese Distribution ordnungsgemäß abläuft, ist Gegenstand dieses Kontrollbereichs.
IT	Dieser Kontrollbereich bezieht sich auf alle Anforderungen, die an IT-Anwendungen gestellt werden, mithin auf die datensicherheitsrechtlichen Anforderungen (z.B. Art. 25, 32 DSGVO) und ihre Umsetzung oder Unterstützung.

Kern-Kontrollbereiche eines Datenschutz-Audits

I. Planung und Vorbereitung

In der ersten Phase legen Sie u.a. die Auditvariante und -kriterien fest, erstellen den Auditbogen inklusive Checklisten, terminieren das Audit in Absprache mit den Abteilungsverantwortlichen und der Geschäftsführung und führen ggf. eine Vorbesprechung durch. Je nach Audit und Scope ist diese Phase mit einem großen Aufwand verbunden.

II. Auditdurchführung

Bei der Durchführung kommt es maßgeblich darauf an, an Informationen zu kommen. Die wichtigste Informationsquelle ist das Interview mit den beteiligten Ansprechpartnerinnen und -partnern (z.B. Abteilungsleitung Marketing). Nicht zu vernachlässigen sind überdies Dokumente, Arbeitsanweisungen und Prozessbeschreibungen sowie die eigene Wahrnehmung, etwa im Rahmen von Begehungen der Räumlichkeiten. Beherzigen Sie die folgenden Punkte:

- Verlassen Sie sich nicht (zwingend) auf Aussagen der interviewten Personen („Ja, mit diesem Dienstleister haben wir einen Vertrag zur Auftragsverarbeitung geschlossen"). Prüfen Sie wenn möglich die Aussagen nach.
- Haken Sie bei zu ungenauen Angaben wie „Das macht alles der Dienstleister xyz" oder „Bei uns unterzeichnet jeder Mitarbeiter immer eine Vertraulichkeitsverpflichtung" unbedingt nach.
- Schaffen Sie eine Atmosphäre des Vertrauens – Sie sind nicht die Datenschutzaufsichtsbehörde, kommunizieren Sie das!
- Lassen Sie sich nicht zu wertenden Aussagen hinreißen wie „Das sieht gut aus." oder „Das ist rechtskonform." Solche Aussagen stehen ausschließlich im Auditbericht.

III. Abschlussgespräch und Auditbericht

Das Abschlussgespräch findet üblicherweise mit der Geschäftsleitung und ggf. mit den auditierten Abteilungen statt (variabel). Kommunizieren Sie in diesem Gespräch höchstens summarische Ersteindrücke, z.B. offensichtliche Rechtsverstöße. Denn Sie werten die Informationen erst im Nachgang sorgfältig aus und bewerten sie rechtlich. Zum Abschlussgespräch gehört zudem, den weiteren Ablauf zu besprechen, etwa bis wann der Auditbericht fertiggestellt ist. Die Informationserfassung für den Auditbericht und die Ableitung von Maßnahmen könnten wie folgt aussehen:

- Erhaltene Information: „Unsere Personalsachbearbeiterin schickt nach Eingang der Bewerbung händisch eine E-Mail an die Bewerber und hängt die Datenschutzinformation gemäß Art. 13/14 DSGVO an".
- Hinweis des Auditors: „Händische Übermittlung bietet Risiken, Prozessumgestaltung empfohlen, Maßnahme: Einrichtung Automatic-Reply-Antwort mit Datenschutzinformation."

IV. Maßnahmenplan

Auf Basis der rechtlich bewerteten Informationen erstellen Sie einen Maßnahmenplan. Er stellt im Soll-Ist-Vergleich dar, welche Maßnahmen der Verantwortliche ergreifen muss, um Datenschutz-Compliance zu erreichen (Beispiel: „Erstellung/Revision des Prozesses Umgang mit Schutzverletzungen, einschließlich Sensibilisierungsmaßnahmen intensivieren").

Listen Sie die Maßnahmen risikoorientiert und priorisiert auf. Die Granularität der Maßnahmen ist abhängig von der Auditvariante und vom Scope des Audits (Beispiel: „Implementierung eines Einwilligungsmanagements" oder „Revision Einwilligungserklärung xyz bzgl. Informiertheit"). Im Anschluss daran erfolgt die Umsetzung der Maßnahmen in Abstimmung mit Ihnen als DSB.

Übung macht den Meister

Wichtig für den Erfolg von Datenschutz-Audits sind neben einer guten Planung und Vorbereitung v.a. die Softskills „Scharfsinn und analytische Auffassungsgabe", gepaart mit einer guten Menschenkenntnis. Je mehr Erfahrung Sie mit Audits haben, desto einfacher gehen sie von der Hand und desto besser sind sie.

Ein Audit muss v.a. in KMU relativ „einfach" gehalten sein. Eine hundertseitige Checkliste bringt keinem etwas, wenn weder der Auditor noch die Verantwortliche damit umzugehen wissen. Und für Auditoren und die, die es noch werden wollen, sei abschließend die Empfehlung gegeben: „Sei hart in der Sache, aber sanft im Ton".

Dr. Kevin Marschall ist Geschäftsführer der GDPC GbR, einer auf Datenschutz und Informationssicherheit spezialisierten Unternehmensberatung mit Sitz in Kassel.

Aufbau eines Auditberichts

- **Deckblatt inkl. Angaben zum Prüfer, beteiligte Personen, Datum, Versionsnummer, Auditvariante, Auditkriterien**
- **Management-Summary zum Audit (max. 1–2 Seiten), Inhalte:**
  - **Soll-Ist-Vergleich und ggf. Scorewert zur visuellen Verdeutlichung des Compliance-Stands**
  - **Hauptrisiken (größte Findings) und Folgemaßnahmen (priorisiert)**
- **Hauptteil mit Fragen und Antworten aus den Interviews und Prüfungen, ggf. Unterteilung in rechtlichen und technischen Teil hilfreich**
- **Übergebene Dokumente während des Audits inkl. Ergebnis der Kurzbewertung durch DSB**
- **Beurteilung des Reifegrads des Unternehmens/des Prozesses/der Software etc. (Scorewert)**
- **Maßnahmenplan**

Gesetze verraten viel

Spionage durch China, Russland, USA

Weitreichende Pflichten von Privaten

Privatunternehmen sind vielfach verpflichtet, Nachrichtendienste zu unterstützen, indem sie ihnen technische Zugriffsmöglichkeiten eröffnen. Teils müssen sie sogar Daten für die Zwecke der Nachrichtendienste sammeln und sie ihnen zur Verfügung stellen.

In China, Russland und den USA gibt es für beide Aspekte ausdrückliche gesetzliche Regelungen. Die Analyse dieser öffentlich zugänglichen Normen bringt viel mehr als Spekulationen darüber, wie sich die Nachrichtendienste dieser Länder in der Praxis verhalten.

Gesetzliche Fakten statt Spekulationen

Das ist eine der Schlussfolgerungen in einem Impulspapier, das die Wissenschaftliche Arbeitsgruppe des Nationalen Cyber-Sicherheitsrats erstellt hat. Es stellt für China, Russland und die USA jeweils knapp dar,

- welche Nachrichtendienste dort existieren,
- welche gesetzlichen Aufgaben ihnen zugewiesen sind und
- über welche gesetzlichen Befugnisse sie verfügen.

Besonders hervorgehoben ist jeweils der Aspekt „Indienstnahme von Unternehmen und Staatsangehörigen". Einer solchen Indienstnahme sehen sich vielfach auch ausländische Töchter von deutschen Organisationen ausgesetzt. Dadurch verfügen die Nachrichtendienste in Deutschland selbst oder jedenfalls in der Kommunikation mit deutschen Stellen über „Trojanische Pferde", denen ihre nachrichtendienstliche Funktion nicht anzusehen ist (Seiten 4/5 des Papiers).

Russland: klare Aufgaben des FSB

Alle Ausführungen in dem Papier sind sachlich-nüchtern gehalten und durch öffentlich zugängliche Normen belegt. Gerade deshalb dürften sie z.B. im Hinblick auf Russland erhebliche Nervosität in manchen Unternehmen und Organisationen auslösen. So hat der Inlandsnachrichtendienst FSB die offizielle gesetzliche Aufgabe, von Russland aus Wirtschafts- und Technologiespionage zu betreiben. Telekommunikationsunternehmen und Internet-Service-Provider müssen sich den Einsatz von Verschlüsselungstechnik genehmigen lassen. Vor allem bei Grenzkontrollen sammelt der FSB biometrische, genomische und biologische Daten von Ausländern. Diese Daten lassen sich nutzen, um Zugriffskontrollen zu überwinden (Seiten 2/3).

China: PIPL und wesentlich mehr

Im Falle Chinas stellt das Papier das in Deutschland stark beachtete Gesetz zur Sicherheit personenbezogener Informationen (PIPL) in den größeren Zusammenhang von Vorschriften, die den Zugriff von Nachrichtendiensten sogar auf verschlüsselte Daten sicherstellen.

Eine wesentliche Funktion des PIPL besteht darin, die Lokalisierung wichtiger Daten in China durchzusetzen. Neben dem PIPL gibt es zahlreiche bereichsspezifische Regelungen mit Vorgaben zur Datenlokalisierung in China, etwa für den medizinischen Bereich oder den Finanzsektor (Seiten 3/4 des Papiers).

USA: große Intelligence Community

In den USA fällt auf, dass es dort sehr viele Geheimdienste gibt. Sie kooperieren als „US Intelligence Community (IC)". Eine Gesamtaufsicht erfolgt durch den Director of National Intelligence (DNI). Für Nicht-US-Bürger besteht kein Rechtsschutz gegenüber US-Nachrichtendiensten. National Security Letters zwingen Unternehmen oder Einzelpersonen zum Stillschweigen über die Kooperation mit dem FBI, das auch geheimdienstlich tätig ist (Seiten 1/2 des Papiers).

Umfassender Zugriff in Russland und China

Zusammenfassend stellt das Papier u.a. fest:

- „In Russland und China beherrschen die Nachrichtendienste den nationalen Kommunikationsraum beinahe vollständig. In beiden Staaten müssen Daten im eigenen Land gespeichert werden, um jederzeit auf sie zugreifen zu können."
- In allen drei untersuchten Staaten hätten die Nachrichtendienste „potenziell Zugriff auf alle dort gespeicherten Daten." Dies gelte auch für Daten bei Tochtereinrichtungen von Organisationen aus diesen Staaten.
- Alle drei Staaten sehen vor, dass Nachrichtendienste eigene (Tarn-) Unternehmen gründen können und eigene Mitarbeiter in bestehende Organisationen einschleusen dürfen (Seiten 4/5 des Papiers).

Pflichtlektüre nicht nur für DSB

Quelle: Wissenschaftliche Arbeitsgruppe Nationaler Cyber-Sicherheitsrat, Impulspapier „Auswirkungen ausländischer Gesetzgebung auf die deutsche Cybersicherheit" (Stand: 11/2021). Das sechsseitige Papier ist abrufbar unter https://ogy.de/impulspapier-gesetzgebung.

Dr. Eugen Ehmann ist Regierungspräsident von Unterfranken und im Datenschutz auch gern international unterwegs.

Bild: Microsoft

Die Datenflüsse an Microsoft sind wie bei Windows 10 die größte Krux

Betriebssysteme

Das bedeutet Windows 11 für den Datenschutz

Welche datenschutzrechtlichen Fragen stellen sich bei der neuesten Version des Microsoft-Betriebssystems? Ein Vergleich mit Windows 10.

Als im Oktober 2021 Windows 11 auf den Markt kam, konnte man sich schon kurz fragen, was das zu bedeuten hatte – schließlich hieß es vonseiten Microsofts bislang, dass Windows 10 die letzte Version sei und stattdessen regelmäßige (mehr oder weniger funktionsgeladene) Updates idealerweise automatisch auf den heimischen oder betrieblichen PC geladen werden sollen.

Im Folgenden geht es aber weniger um Marketing-Vokabular als vielmehr um die an sich einfache Frage „Was bedeutet Windows 11 für den Datenschutz?".

Änderungen auf den ersten Blick

Windows 11 ist offensichtlich zuallererst ein grafisches Update in der Windows-Oberflächengestaltung. So fallen vermutlich schnell die abgerundeten Ecken in den Fenstern sowie die Anordnung der Oberflächenelemente ins Auge. Auch der Datei-Explorer, das zentrale Softwaretool, um Dateien zu verwalten, erscheint in neuem Gewand.

Der Einfluss des Homeoffice-Arbeitens unter der Corona-Pandemie könnte ein Entscheidungskriterium für das sogenannte „Hybride Arbeiten" mit einem mobilen Notebook und Monitoren sein. Denn hier kann das mühsame Neuanordnen von bereits geöffneten Fenstern entfallen.

Auffällig ist zudem, dass die Hardwareanforderungen an Windows 11 äußerst hoch sind. Allerdings unterstützt Microsoft viele Notebooks/PCs nicht mehr, die bereits einige Jahre auf dem Buckel haben, aber an sich noch performant genug sind. Kurzfristig kann zwar der ein oder andere „Hack" helfen. Um einen gesicherten Business-Betrieb insbesondere mit Blick auf Software-Updates zu gewährleisten, dürfte es jedoch zu einem Konjunkturprogramm für die PC-Industrie kommen.

Teams vorinstalliert

Nach einer Neuinstallation von Windows 11 bzw. einem Update aus Windows 10 ist die Videokonferenzlösung Teams prägnant vorinstalliert. Sie lässt sich über die „Chat"-Funktion der Taskleiste starten. Unternehmen, die eine Teams-Version in einer eigenen Domäne integrieren wollen (z.B. über ein AzureAD-Konto), kommen weiterhin nicht darum herum, eine speziell lizenzierte Business-Version zu installieren.

Die Zielgruppe scheinen also eher Privatpersonen oder kleinere Unternehmen zu sein. Hier stellt sich jedoch die Frage, ob Microsoft nicht eine marktbeherrschende Stellung ausnutzt und alternative Videokonferenzlösungen benachteiligt. Das wird allerdings weniger das Datenschutzrecht als das Kartellrecht beantworten müssen.

Klein, aber fein: das Werkzeug WinGet

Während man es unter Windows 10 noch selbst installieren musste, ist unter Windows 11 ein Paketmanager namens WinGet vorinstalliert. Damit lässt sich – ähnlich wie mit dem Kommando apt-get unter Linux – Software auf einem Windows-11-Rechner über die Kommandozeile installieren.

PRAXIS-TIPP

Das ist interessant insbesondere für kleine Unternehmen, die keine ausdrückliche Paketverwaltung oder entsprechend konfigurierte Windows-Domäne ihr Eigen nennen. Denn sie können per Winget-Upgrade mittels selbst geschriebener Powershell-Skripts ihrer Verpflich- →

tung nachkommen, für aktuelle Softwarestände nach Art. 32 Datenschutz-Grundverordnung (DSGVO) zu sorgen.

Hürde Browserwechsel

Dass ein Internet-Browser auch unter dem Gesichtspunkt der Standardisierung und Marktmacht relevant ist, hat in der Vergangenheit der faktische Siegeszug des Chrome-Browsers gezeigt.

Zwar gibt es alternative Browser wie Firefox oder Opera, die datenschutzfreundlichere Funktionalitäten v.a. beim Tracking-Schutz bieten. Doch Anwenderinnen und Anwender müssen das Windows-Betriebssystem erst einmal dazu bringen, Internet-Links nicht in Edge, sondern in einem anderen Browser aufzurufen. Hierzu ist es nicht mehr wie bisher mit einer – mehr oder weniger umständlichen – einmaligen Einstellung getan. Stattdessen ist es nötig, die Standard-App für jede Dateiendung einzeln zu ändern. Wer das über die Benutzeroberfläche macht, hat ziemliche viele Änderungen vor sich.

Auch hier gilt mit Blick auf den Datenschutz, dass dies sicherlich eine hohe Hürde darstellt. Doch das Datenschutzrecht stuft Windows 11 insbesondere bei der Nutzung durch Verantwortliche allenfalls als kompliziert zu konfigurierendes Produkt nach Art. 25 Abs. 1 DSGVO ein, bei dem die „Ermutigung" des europäischen Gesetzgebers nach Erwägungsgrund 78 der DSGVO (Privacy by Design und by Default) bislang nicht vollständig angekommen sein könnte.

Zentraler Fokus: Telemetrie- und Diagnosedaten

Schon unter Windows 10 waren die Telemetrie- und Diagnosedaten das am meisten diskutierte Thema im Datenschutz, geht es dabei doch um Datenflüsse eines Windows-Rechners an Microsoft. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hatte für Windows 10 eine SySiPhus-Studie genannte Analyse in Auftrag gegeben, die sich auch intensiv mit den Telemetrie- und Diagnosedaten beschäftigte (siehe https://ogy.de/bsi-sisiphus).

Wofür nutzt Microsoft die Daten?

Wie sich Diagnose- und Telemetriedaten genau voneinander abgrenzen, ist weiterhin nicht ganz klar. Es geht aber im Prinzip darum, dass bestimmte Systemereignisse nach einer lokalen Speicherung über den Windows-Event-Logger an Server von Microsoft übertragen werden. Dort nutzt Microsoft sie für zwei Zwecke:

- zum einen, um die Systemstabilität des Senders zu gewährleisten (z.B. funktionelle Windows-Updates, Schadcode-Meldungen, Performance-/Stabilitätsprobleme).
- zum andern für eigene Zwecke wie Qualitätssicherung, Statistiken sowie Aufbau und Vertrieb von Antiviren-Signaturen.

Lässt sich der Datenfluss unterbinden?

Die deutschen Datenschutzaufsichtsbehörden haben sich in der Datenschutzkonferenz (DSK) schon bei Windows 10 mit der Frage beschäftigt, ob ein Verantwortlicher grundsätzlich die Datenflüsse an Microsoft unterbinden kann oder nicht (siehe https://ogy.de/dsk-telemetrie-windows).

Die DSK hat bei Nutzung der Windows 10 Enterprise Version und der Einstellung des Telemetrie-Levels „Security" grundsätzlich anerkannt, dass sich die Übertragung der Telemetriedaten an Microsoft wohl unterbinden lässt.

Keine Deaktivierung oder Deinstallation möglich

Die prinzipielle Fragstellung blieb aber weiterhin: Wieso lässt sich die Telemetrie-Komponente nicht nachhaltig deaktivieren, besser deinstallieren, wenn keine Daten an Microsoft übertragen werden? So bleibt das Risiko, dass durch Software- und Konfigurationsfehler oder gar durch einen Cyberangriff auf die Microsoft-Endpunkte plötzlich Zigtausende vermeintlich abgeschaltete Datensammler auf Endgeräten zum Leben erwachen.

Einstellungsmöglichkeiten unter Windows 11

Unter Windows 11 sind die Diagnosedaten weiterhin vorhanden und ausführlich beschrieben (https://ogy.de/diagnosedaten-konfigurieren). Es gibt drei verschiedene Einstellungsmöglichkeiten:

1. **Diagnosedaten aus**
   Diese Einstellung hieß laut Microsoft bislang „Security". Sie sollte nur in gut administrierten Umgebungen zum Einsatz kommen. Nur hier ist gewährleistet, Update-Probleme zu erkennen und in den Griff zu bekommen. Diese Einstellungsmöglichkeit bietet weiterhin allein die Enterprise-Version.
2. **Erforderliche Diagnosedaten**
   Diese Einstellung wurde je nach Windows-10-Version auch als „Standard" bezeichnet. Sie beinhaltet hauptsächlich technische Informationen, die aber auch eindeutige Gerätekennungen umfassen.
3. **Optionale Diagnosedaten**
   Diese Einstellung hieß laut Microsoft bislang „vollständig". Sie kann sowohl Browserverläufe als auch im Einzelfall Speicherabbilder mit personenbezogenen Daten umfassen.

Neben der Deaktivierung der – laut DSK möglicherweise zweifelhaft stabilen – Diagnosedatenübermittlung an Microsoft findet sich auch zu Windows 11 in der Microsoft-Dokumentation das sogenannte „Windows Restricted Traffic Limited Functionality Baseline-Paket" (Dokumentation siehe https://ogy.de/verbindungen-zu-ms-diensten). Das Paket soll über

ACHTUNG

Da die vorhandene Dokumentation keine Anhaltspunkte für Deaktivierungs- bzw. Deinstallationsmöglichkeiten der Windows-Telemetrie-Komponente bietet, dürfte es nur eine Frage der Zeit sein, bis sich die DSK auch Windows 11 mittels einer technischen Analyse zu Gemüte führt.

Gruppenrichtlinien eine vollständige Kontrolle über sämtliche Datenflüsse gewährleisten. Das gilt zumindest für die jeweiligen Enterprise-Versionen.

Unternehmen als eigene Verantwortliche bei Diagnosedaten?

Es ist mittlerweile möglich, dass Unternehmen oder Behörden, die Windows-10- bzw. Windows-11-Endgeräte einsetzen, bezüglich der Diagnosedaten selbst Verantwortliche im Sinne der DSGVO werden (siehe https://ogy.de/diagnosedaten-konfigurieren).

Technisch werden die Daten gemäß den anzusteuernden Endpunkten weiterhin an Microsoft-Server übertragen. Rechtlich wäre hier nach entsprechender Konfiguration zu prüfen, in welchem Verhältnis der Verantwortliche dann zu Microsoft steht und v.a. ob Microsoft weiterhin Diagnosedaten zu eigenen Zwecken verarbeitet. Der Sinn und Zweck derartiger Datenflüsse wäre noch zu klären. Es muss aber jedem Verantwortlichen klar sein, dass er dann insbesondere den Beschäftigtendatenschutz berücksichtigen muss.

Garantierter Streitfall: Online-Zwang bei Nicht-Enterprise-Versionen

Mit Windows 11 zieht ein „Feature" ein, das Microsoft schon in manchen Windows-10-Versionen etablieren wolle: der Zwang zu einem Microsoft-Konto.

Er mag für Nutzer und Nutzerinnen von Nicht-Enterprise-Versionen, die den Microsoft-Cloud-Speicherplatz oder gar ein Microsoft-365-Abo haben, unproblematisch sein. Andere Nutzer, denen die eigene Kontrolle über ein Betriebssystem wichtig ist, stellt es aber vor ein deutliches Problem. Denn Windows 11 ist offiziell ohne Online-Konto gar nicht installierbar.

Momentan gibt es noch Hacks, die eine Installation ohne Online-Konto zulassen. Beispielsweise lässt sich derzeit als E-Mail-Adresse „Microsoft" eingeben. Doch ob dies auch dauerhaft der Fall ist, steht in den Sternen. Datenschutzbeschwerden bei den Aufsichtsbehörden sind vorprogrammiert und werden die Frage aufwerfen, ob derartige „Zwänge" vonseiten der Nutzungsbedingungen zulässig sind, um eine datenschutzrechtliche Grundlage zu schaffen.

Fazit: keine allzu großen Änderungen gegenüber Windows 10

Zum jetzigen Zeitpunkt lässt sich aus Datenschutzsicht sagen, dass sich bei Windows 11 hauptsächlich die grafische Oberfläche geändert hat. Da es weiterhin halbjährliche Feature-Updates zu geben scheint, bleibt es aufgrund der Rechenschaftspflicht weiter im Verantwortungsbereich der Unternehmen und Behörden, den konkreten Einsatz von Windows 11 genau im Auge zu behalten.

Insbesondere die erweiterten Nachweispflichten bleiben wohl unter Windows 11 erhalten. Sind die Telemetrie-/Diagnosedaten-Flüsse an Microsoft wirksam unterbunden über „Diagnosedaten aus" sowie ggf. über den geprüften Einsatz des „Baseline-Pakets"?

Darüber hinaus dürfte der neue Online-Zwang beim Einsatz von Windows-11-Pro-Versionen – Windows Home ist im Unternehmenseinsatz tabu – zu größeren Problemen führen, eine Rechtsgrundlage zu finden.

Andreas Sachs ist Vizepräsident des Bayerischen Landesamts für Datenschutzaufsicht (BayLDA). Darüber hinaus leitet er das Referat Technischer Datenschutz und IT-Sicherheit beim BayLDA.

TPM 2.0

Das Trusted Platform Module

Ein Trusted Platform Module (TPM) ist im Prinzip eine eigene geschlossene Hardwarekomponente. Sie kann als Ablageort für vertrauliche Informationen abseits eines Betriebssystems wie etwa kryptografische (Wurzel-) Zertifikate dienen sowie einfache Rechenoperationen durchführen.

Das Windows-11-Startmenü

Bild: Microsoft

Pflicht unter Windows 11

Windows 11 macht diese Technik in der Version TPM 2.0 faktisch zur Pflicht, obwohl sie isoliert betrachtet schon seit vielen Jahren auf dem Markt ist und Bestandteil fast aller PCs und Notebooks sein dürfte.

Ein Vorteil ist sicher das Mehr an Sicherheit nach Art. 32 DSGVO insbesondere gegen Schadcode, der unterhalb der Betriebssystemebene ablaufen soll (z.B. BIOS-Schadcode). Ein weiterer Vorteil ist die Kopplung von Authentifizierungsinformationen an ein Endgerät (z.B. Windows Hello oder Bitlocker). Allerdings öffnet die Verpflichtung in Windows 11 möglicherweise die Tür für eine noch engere Bindung von Lizenzinformationen – auch für andere Softwareprodukte – an TPM, bei dem der höchste Vertrauensanker in den Händen des Privatunternehmens Microsoft liegt.

Insbesondere bei Diskussionen um offene Standards und digitale Unabhängigkeit wird die TPM-Pflicht bei Windows 11, die sich momentan wohl noch mittels „Hacks" umgehen lässt, sicher Einzug halten.

Bild: iStock.com/huettenhoelscher

Gut, wenn in solchen Situationen klar ist, welche Kontaktpersonen zu benachrichtigen sind

Rechtmäßigkeit der Verarbeitung

Notfallkontaktdaten im Betrieb

Auch bei größter Vorsicht können Notfälle auf dem Arbeitsweg oder im Betrieb passieren. Da ist es wichtig, die Daten von Notfallkontakten zur Hand zu haben. Wie lässt sich das datenschutzkonform organisieren?

Dass es zu Unfällen und Gefahrensituationen kommt oder dass Beschäftigte chronische oder akute gesundheitliche Probleme haben, ist keine Seltenheit. Neben einer angemessenen medizinischen Reaktion, etwa durch Absetzen eines Notrufs oder Tätigwerden von Ersthelfern, ist es oft wichtig, einen Notfallkontakt zu benachrichtigen.

Die Benachrichtigung dient nicht rein dazu, eine Kontaktperson über die Notlage zu informieren. Sie kann mit ihrem Wissen etwa über Vorerkrankungen, unbekannte Allergien oder regelmäßig einzunehmende Medikamente möglicherweise sogar akute Notsituationen verhindern oder zumindest abmildern.

Anwendbarkeit der DSGVO

Das Problem vieler Betriebe beginnt allerdings früher: Sie müssen die Kontaktdaten der Notfallkontaktperson erfassen und speichern. Damit liegt eine Verarbeitung personenbezogener Daten vor. Sie unterliegt nach Art. 2 Abs. 1 in Verbindung mit Art. 4 Nr. 1, 2 Datenschutz-Grundverordnung (DSGVO) datenschutzrechtlichen Bestimmungen. Insbesondere kommt hier nicht die sogenannte Haushaltsausnahme aus Art. 2. Abs. 2 Buchst. c DSGVO zum Tragen. Denn die Daten sind zwar privater Natur. Doch das Unternehmen oder die Behörde verarbeitet die Daten im beruflichen Kontext.

Rechtsgrundlagen der Datenverarbeitung

Für die Verarbeitung dieser personenbezogenen Daten muss damit eine Rechtsgrundlage eröffnet sein.

Einwilligung

Grundsätzlich kommt zunächst die Einwilligung der betroffenen Notfallkontaktperson nach Art. 6 Abs. 1 Buchst. a DSGVO in Betracht, also ihre vorherige, freiwillige und informierte Zustimmung. Allerdings ist es mit einigem Aufwand verbunden, diese Einwilligung einzuholen:

- Um die Einwilligungserklärung an die Notfallkontaktperson zu versenden, ist zusätzlich ihre Anschrift oder ihre E-Mail-Adresse notwendig. Das führt zu einem Mehr an Verarbeitung von personenbezogenen Daten.
- Der Betrieb muss die betroffene Person dokumentiert gemäß den Informationspflichten nach Art. 13 DSGVO belehren.
- Die Einwilligungserklärung muss nachweislich (Art. 7 Abs. 1 DSGVO) erfolgen, also im besten Fall von der Notfallkontaktperson unterschrieben beim Betrieb eingehen.
- Die übrigen für eine wirksame Einwilligung geltenden Voraussetzungen (Art. 7 Abs. 2 DSGVO) müssen erfüllt sein.

Neben dem Aufwand ist das „Risiko" zu bedenken, dass die Kontaktperson ihre Einwilligung jederzeit widerrufen kann. Allerdings dürfte ein solcher Widerruf kaum ohne Grund erfolgen. Notfallkontaktpersonen werden den Beschäftigten in der Regel nahestehen und ein Interesse an deren Gesundheit haben. Sollte sich dies etwa aufgrund einer Trennung bei Ehegatten oder Lebenspartnern ändern, läge es im allgemeinen Interesse, die Daten nicht mehr zu verarbeiten.

Geeignet, aber aufwendig

Die Einwilligung stellt folglich eine valide Rechtsgrundlage dar. Doch angesichts des Aufwands, der damit verbunden ist, ist es praxisnäher, die Daten ohne formelles Einholen einer Einwilligung zu erfassen. Dafür müsste sich die Verarbeitung der personenbezogenen Daten von Notfallkontaktpersonen auf eine andere Rechtsgrundlage stützen lassen.

Interessenabwägung

Art. 6 Abs. 1 Buchst. f DSGVO könnte ebenfalls als Rechtsgrundlage für die Verarbeitung der Notfallkontaktdaten infrage kommen. Danach ist eine Abwägung der

Eine Möglichkeit: Beschäftigte als Boten

Informationspflichten erfüllen

Erhebt ein Betrieb die Notfallkontaktdaten im Rahmen der Einwilligung bei der Notfallkontaktperson, hat er die Informationspflichten nach Art. 13 DSGVO zu erfüllen.
Sofern er die Notfallkontaktdaten nicht bei der Person, sondern im Rahmen der Interessenabwägung direkt von den Beschäftigten erhebt, muss der Betrieb die Informationspflichten nach Art. 14 DSGVO einhalten.
In der Praxis gibt es für Letzteres zwei Möglichkeiten:

- Zum einen lassen sich die Informationen aus Art. 14 DSGVO per E-Mail oder Brief übermitteln. Nachteil ist – wie bei der Einwilligung – die zusätzliche Verarbeitung der Daten „Anschrift" oder „E-Mail-Adresse" der Notfallkontaktperson.
- Daher ist es empfehlenswert, dass die Beschäftigten die Informationen nach Art. 14 DSGVO ihrer jeweiligen Notfallkontaktperson überbringen. Das stellt zum einen sicher, dass die betreffende Person von ihrer Funktion erfährt. Zum anderen ist es nicht erforderlich, personenbezogene Daten für den Versand zu verarbeiten.
- Zu Dokumentationszwecken ist es bei der zweiten Variante sinnvoll, sich von den Beschäftigten bestätigen zu lassen, dass sie das Informationsschreiben an ihre Notfallkontaktperson übergeben.

Interessen des Verantwortlichen (Betrieb) oder Dritter (Beschäftigte) mit den Interessen der betroffenen (Notfallkontakt-) Person erforderlich.

- Die Interessen der betroffenen Person beschränken sich hier auf das „abstrakte" Interesse, dass keine personenbezogenen Daten verarbeitet werden. Jedoch sind die verarbeiteten Daten – im Regelfall Name und (Mobil-)Telefonnummer – nicht von besonderer Intimität geprägt.
- Dem gegenüber steht das Interesse der Beschäftigten als „Dritte", dass der Betrieb z.B. Angehörige über Zwischenfälle informiert und sie ihnen in akuten Notsituationen helfen können.
- Aus der Fürsorgepflicht des Betriebs ist auch dessen Interesse betroffen.

Angesichts der nur minimal betroffenen Interessen der Notfallkontaktperson kommt diese Rechtsgrundlage damit in Betracht. Es sei jedoch darauf hingewiesen, dass auch hier das Risiko eines Widerspruchs (Art. 21 Abs. 1 Satz 1 DSGVO) besteht.

Schutz lebenswichtiger Interessen

Zuletzt sei Art. 6 Abs. 1 Buchst. d DSGVO betrachtet. Die Rechtsgrundlage verlangt für die Rechtmäßigkeit der Datenverarbeitung den Schutz lebenswichtiger Interessen der betroffenen Person oder Dritter. Diese Rechtsgrundlage soll nach Erwägungsgrund 46 der DSGVO nur angewandt werden, „wenn die Verarbeitung offensichtlich nicht auf eine andere Rechtsgrundlage gestützt werden kann".

Da die Einwilligung und die Interessenabwägung als offensichtlich alternative Rechtsgrundlagen in Betracht kommen, scheidet der Schutz lebenswichtiger Interessen als Rechtsgrundlage aus.

Aufbewahrung und Löschung der Notfallkontaktdaten

Abschließend stellt sich die Frage, wo und wie Unternehmen und Behörden die Notfallkontaktdaten aufbewahren und löschen. Zum einen besteht die Möglichkeit, dass die Personalabteilung die Daten in einer zentralen Datei speichert. Zum anderen könnte die jeweilige direkte Führungskraft die Notfallkontaktdaten dezentral aufbewahren. In beiden Fällen ist der Zugriff auf die Daten streng zu limitieren (Need-to-know-Prinzip), und die Daten sind durch technische und organisatorische Maßnahmen zu schützen.

Mit Blick auf Backups, die oft jahrelang vorhanden sind, empfiehlt sich die zweite Variante: die Aufbewahrung in Papierform bei der direkten Führungskraft. Sie wird zudem eine akute Notsituation ihrer Beschäftigten am schnellsten mitbekommen und kann den Notfallkontakt umgehend informieren.

Ändert sich der Notfallkontakt oder scheidet ein Beschäftigter aus, müssen Verantwortliche die Daten der (vormaligen) Notfallkontaktperson datenschutzkonform vernichten und die Daten der neuen datenschutzkonform aufbewahren.

KURZ GEFASST

Die Verarbeitung personenbezogener Daten von Notfallkontaktpersonen der Beschäftigten unterfällt der DSGVO. Hinsichtlich der Rechtsgrundlage kommen die Einwilligung oder die Interessenabwägung in Betracht.

- ***Bei der Einwilligung stellt der Betrieb der Notfallkontaktperson die Informationen nach Art. 13 DSGVO direkt zur Verfügung.***
- ***Bei der Interessenabwägung überbringen die Beschäftigten der Notfallkontaktperson die Informationen nach Art. 14 DSGVO als „Boten".***

Die Notfallkontaktdaten sind im Betrieb datenschutzkonform aufzubewahren und nach Zweckerfüllung, also z.B. wenn ein Beschäftigter aus dem Betrieb ausscheidet, datenschutzkonform zu vernichten.

Dennis Wienemann (LL.M.) ist stellvertretender Leiter des Stabsbereichs Compliance bei der Wirtschaftsbetriebe Duisburg – AöR und berät dort als Rechtsassessor vornehmlich zum Datenschutzrecht. Er ist in den Bereichen Compliance und Datenschutz jeweils als Fachkraft zertifiziert und führt Datenschutzaudits durch.

Bild: iStock.com/sefa ozel

Tun sich DSB und Compliance Officer zusammen, kann dies zu erheblichen Synergieeffekten führen

Unterschiede & Gemeinsamkeiten

Datenschutzbeauftragte und Compliance Officer

In einigen Unternehmen gibt es sowohl einen Datenschutzbeauftragten als auch einen Compliance Officer. Wer macht was, wie lassen sich die Aufgaben abgrenzen, in welchem Verhältnis stehen sie zueinander?

Verantwortliche im Unternehmen haben dafür zu sorgen, dass die Vorgaben der Datenschutz-Grundverordnung (DSGVO) sowie der nationalen Gesetzgebung zu Datenschutz und andere rechtsverbindliche Vorschriften zum Schutz personenbezogener Daten umgesetzt werden.

Datenschutzbeauftragte

Datenschutzbeauftragte (DSB) sind daher gesetzlich ab 20 Daten verarbeitenden Personen vorgeschrieben. Entsprechend gibt es sie in den meisten Unternehmen, für die diese Bedingung zutrifft.

Da sie ein Grundrecht schützen, sind DSB mit besonderen Privilegien ausgestattet. So sind sie in Sachen Datenschutz weisungsfrei. Der Arbeitgeber darf betriebliche DSB wegen ihrer Tätigkeit im Datenschutz nicht kündigen. Zudem darf er einen DSB bei Beförderungen und anderen Anlässen gegenüber Nicht-Datenschutzbeauftragten nicht benachteiligen.

Die steigenden Geldbußen in den letzten Monaten zeigen, dass die DSGVO kein zahnloser Tiger ist. Vor allem kleinere Geldbußen mit den entsprechenden Imageschäden nehmen zu. Insofern besteht die Aufgabe von DSB auch darin, Datenschutzverstöße zu verhindern, die zu einer massiven Geldbuße führen können.

Compliance Officer

Die Führungsgremien von Unternehmen haben dafür zu sorgen, dass die Mitarbeiterinnen und Mitarbeiter verbindliche gesetzliche Vorgaben und verbindliche interne Unternehmensrichtlinien tatsächlich umsetzen, also compliant handeln. Das können sie mit einer juristischen Abteilung tun, sie können aber auch eine verantwortliche Person mit diesen Aufgaben betrauen. Üblicherweise wird diese Person als Compliance Manager oder Compliance Officer bezeichnet.

Die zu beachtenden Gesetze werden immer zahlreicher und umfangreicher. Vor allem die internationale Rechtssituation gestaltet sich immer komplizierter. Daher ist die Aufgabe eines Compliance Officer eine sehr anspruchsvolle.

Die zu beachtenden Vorschriften betreffen alle Unternehmensbestandteile, grundsätzlich auch Datenschutz und Informationssicherheit. Da es jedoch für den Datenschutz eigene Beauftragte gibt und die Informationssicherheit mittlerweile v.a. durch Zertifizierungen weitgehend geregelt ist, besteht in der Praxis häufig Konsens, dass sich Compliance Officer zwar um sehr viele Rechtsgebiete kümmern, weniger aber um Datenschutz und Informationssicherheit.

Die Geldbußen, die bei einem Verstoß gegen internationale Gesetze anstehen, können gegenüber denen für Datenschutzverstöße deutlich höher sein. In der Praxis führt das oft dazu, dass versierte Compliance Officer mehr verdienen als Datenschutzbeauftragte, quasi als Ausgleich für die Privilegierung. Denn Compliance Officer genießen keinen besonderen gesetzlichen Kündigungsschutz.

Wer macht was?

Datenschutzbeauftragte kümmern sich um alles, was rechtlich im Zusammenhang mit dem Schutz personenbezogener Daten verpflichtend geregelt ist. Das beginnt bei der DSGVO, geht weiter über nationale Gesetze mit Vorschriften zum Datenschutz, für die es in der DSGVO eine Spezifizierungsklausel gibt, setzt sich fort im nationalen Vertiefungsgesetz, in Deutschland dem Bundesdatenschutzgesetz, dann über die Landesdatenschutzgesetze hin zu anderen verbindlichen

rechtlichen Vorgaben wie Satzungen oder Betriebsvereinbarungen.

Sie kümmern sich auch präventiv darum, dass es im Rahmen von Informationssicherheit und IT nicht zu Schutzverletzungen im Zusammenhang mit personenbezogenen Daten kommt, da diese meldepflichtig sind. Häufig sind solche Schutzverletzungen Auslöser für weitere Überprüfungen durch die Aufsichtsbehörde, die in Geldbußen enden können.

Compliance Officer kümmern sich in erster Linie um Rechtsgebiete wie

- Verhinderung von Kinderarbeit bei Zulieferern aus Drittländern,
- Verhinderung von Vorteilsnahme bei Einkauf oder Vertrieb,
- Sicherstellung der Gleichstellung im Unternehmen
- bis hin zur Unterstützung bei der Entscheidung, welcher Kantinenanbieter unter Abgabe welchen Angebots den Zuschlag erhält.

Es sind nicht nur Gesetze, die sie zu beachten haben, sondern auch Standards. Dazu gehören spezifische nationale und ausländische Gesetze und Vorgaben. Dazu gehören zudem Garantenstellungen, die vertraglicher oder anderer Art sein können. Auch ethische Vorgaben sind zu beachten. Gerade dann, wenn ein Unternehmen in Ländern tätig ist, in denen andere religiöse Vorstellungen herrschen.

Für beide zentral: Prozess- und Risikomanagement

DSB müssen im Prozessmanagement versiert sein. Das zeigt u.a. die Forderung, Verarbeitungstätigkeiten als Prozesse zu beschreiben. Außerdem beugen gut gestaltete Prozesse Datenschutzverstößen vor. Datenschutz ist zudem angewandtes Risikomanagement. Hierbei geht es v.a. um die Rechte und Freiheiten betroffener Personen, erst in zweiter Linie ums Geld.

Compliance Officer müssen im Prozessmanagement genauso versiert sein und betreiben ebenfalls angewandtes Risikomanagement. Allerdings geht es in erster Linie um finanzielle Folgen für das Unternehmen. Eine weitere Gemeinsamkeit: Beide sind wichtige Schnittstellen zu Gremien wie Betriebsrat, Recht und Qualitätsmanagement. Insofern sind bis auf die Rechtsgebiete die Aufgabenstellungen sehr ähnlich.

In welchem Verhältnis stehen sie zueinander?

Die Erfahrung lehrt, dass im Verhältnis von DSB und Compliance Officer oft Luft nach oben ist. Nicht selten stehen sich die Beteiligten misstrauisch gegenüber. Ich selbst habe die Ausbildung zum Compliance Officer auch deswegen gemacht, weil mir Kollegen immer wieder vorhielten, ich hätte doch von Recht und Gesetz keine Ahnung, ich würde ja „nur Datenschutz" machen. Tatsächlich hat sich in der Ausbildung herausgestellt, dass Datenschutz und Informationssicherheit etwa zwei Drittel der Zeit in Anspruch nehmen, die erforderlich ist, um Compliance-Anforderungen umzusetzen. Das kann bei international agierenden Unternehmen anders sein. Aber für den Durchschnitt der Unternehmen dürfte das zutreffen.

Synergieeffekte nutzen

Daraus folgt, dass sich DSB und Compliance Officer sehr gut ergänzen können, wenn sie vertrauensvoll zusammenarbeiten. Sie sind keine Konkurrenten! Auch wenn es dem Compliance Officer sauer aufstoßen mag, dass DSB unkündbar sind: Die Aufgabenfelder sind so gelagert, dass man sich zwar gegenseitig das Leben schwer machen, aber durch eine clevere Zusammenarbeit auch erleichtern kann. DSB benötigen immer wieder einen Blick in andere Rechtsgebiete. Compliance Officer tun gut daran, die Folgen für Datenschutz und Informationssicherheit zu prüfen, bevor sie Empfehlungen aussprechen und Schulungen durchführen.

PRAXIS-TIPP

Eberhard Häcker kennt beide Seiten: Als externer DSB berät er Unternehmen zum Datenschutz, und als Compliance Officer kennt er auch „die andere Seite".

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, 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: 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 245,00 €
(zzgl. MwSt. und Versandkosten)
Einzelheft 23 €
(zzgl. MwSt. und Versandkosten)

Druck:
Burscheid PrintKommunikation GmbH
Leonhardstraße 23, 88471 Laupheim

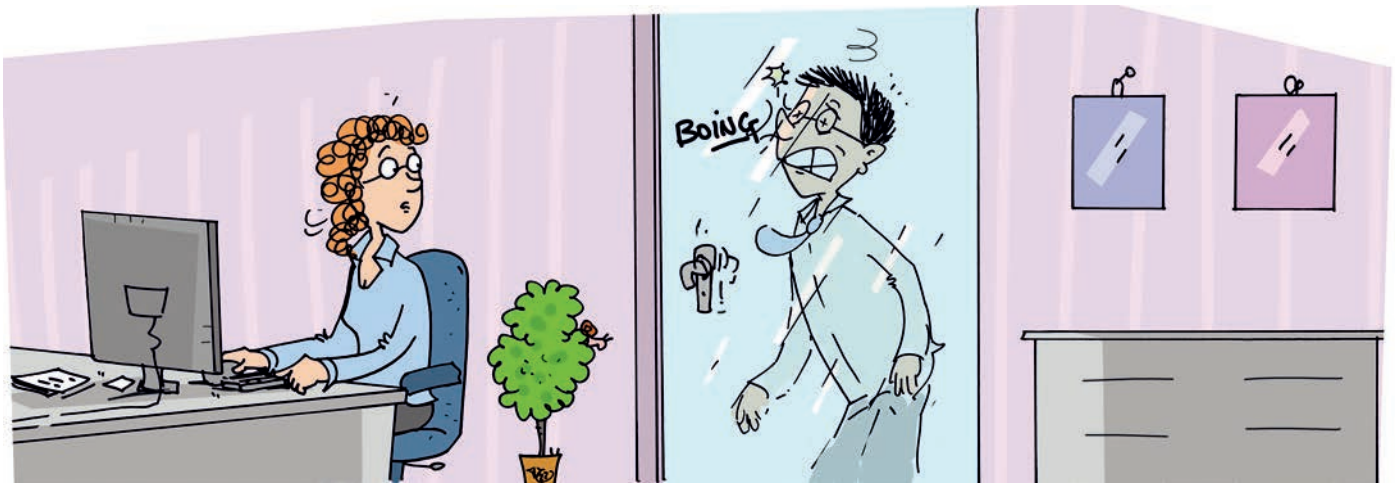
Layout & Satz:
METAMEDIEN
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4100

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 bzw. der Autorin.



Datenschutz-Begehungen

Ersthelfer bereithalten – der Datenschutz kommt!

Datenschutz-Begehungen fanden bei vielen Verantwortlichen v.a. wegen der Auswirkungen der Pandemie über längere Zeit nicht statt. Wenn sie nun wieder erfolgen, heißt das aber nicht, dass sie ihren „Schrecken" verloren haben. Ein schlechtes Gewissen bei beschäftigten Personen wegen nicht umgesetzter Empfehlungen ist dann gar nicht so selten und kann zu kuriosen Situationen führen.

Logistisch lösen Datenschutzbesuche in Unternehmen und Behörden manchmal so einiges aus. Zum Beispiel meldet der Empfang möglichst rasch allen die Ankunft des externen Datenschutzbeauftragten. So kann sich jeder „angemessen" vorbereiten und lieb gewordene Gewohnheiten zumindest vorübergehend abstellen, falls sie nicht ganz datenschutzkonform sein sollten.

Dass bei solchen Besuchen mitunter Kollateralschäden auftreten können, zeigt folgendes reales Beispiel: Datenschutzbeauftragte müssen bei Ortsbegehungen prüfen, inwieweit Schutzverletzungen möglich sind und wie sie sich möglichst im Vorfeld verhindern lassen. So etwa bei Glastüren in Büros. Sie sind wegen der offenen Unternehmenskultur beliebt, lassen aber Einblicke von Unbefugten zu.

„Tür zu!"

Sichtschutzfolie wäre in solchen Fällen besser. Sie kommt aber erfahrungsgemäß meist nicht sehr gut an. Doch zumindest erschwert eine Glastür, dass Unbefugte vertrauliche Telefonate mithören. Wenn die Tür denn zu ist. Und genau das „Tür zu" hatte der Datenschutzbeauftragte bei seiner letzten Begehung angeregt.

Ein unerwartetes Hindernis

Zu seinem Bedauern erfuhr der Datenschutzbeauftragte, dass er mit seiner darauf folgenden Begehung ungewollt einen Ersthelfer-Einsatz ausgelöst hatte. Eine Kollegin hatte ihre – sonst wohl stets offene – Glastür zugemacht, weil „der Datenschutz umgeht". Einer ihrer Kollegen wollte wie gewohnt in besagtes Büro stürmen – und knallte in vollem Tempo gegen die unerwartet geschlossene Tür.

Rascher Ersthelfereinsatz

Das Nasenbluten konnte der Ersthelfer rasch wieder stillen, die verbogene Brille ließ sich richten. Keine Schadenfreude beim Datenschutzbeauftragten. Ehrlich. Aber so ganz unverdient war's ja nicht …

Eberhard Häcker ist seit vielen Jahren externer Datenschutzbeauftragter. Nach der langen Abstinenz ist er froh, wieder Begehungen vor Ort machen zu können.

IN DER NÄCHSTEN AUSGABE

Metaverse & Datenschutz

Das Metaversum verspricht das nächste große Thema zu werden. Oder ist es nur ein Hype von vielen?

Datenschutzfolgen bewerten

Sicherheitslösungen werden immer intelligenter. Umso wichtiger ist es, die Datenschutzfolgen einzuschätzen.

Informationspflichten

Datenschutzhinweise transparent und nutzerfreundlich einbinden – so geht's bei Apps, auf Webseiten, für Kunden etc.