www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT

August 2021

Bild: iStock.com/agrobacter

Eine wichtige Neuerung: Zukünftig gibt es auch Standardvertragsklauseln für das Rechtsverhältnis zwischen Verantwortlichen und Auftragsverarbeitern

Zwei Musterformulare vom 4. Juni 2021

Die neuen EU-Standardvertragsklauseln

Für die Übermittlung personenbezogener Daten in Drittländer außerhalb der EU hat die Europäische Kommission völlig neu gestaltete Standardvertragsklauseln vorgelegt. Erstmals stehen zudem offizielle Standardvertragsklauseln für die Auftragsverarbeitung zur Verfügung.

Die neuen Standardvertragsklauseln ersetzen die bisherigen Standardvertragsklauseln, die noch aus der Zeit vor der Datenschutz-Grundverordnung (DSGVO) stammen.

Welche Standardvertragsklauseln gibt es zukünftig?

Zunächst sind das die neuen „Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer". Gesondert gibt es noch die völlig neuen „Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern".

Es heißt im Original tatsächlich „an" und nicht „in" Drittländer, obwohl „in" gemeint ist. Diese neuen Klauseln für die Übermittlung personenbezogener Daten in Drittländer bilden den Anhang zum Durchführungsbeschluss (EU) 2021/914 der Europäischen Kommission vom 4. Juni 2021. Der Durchführungsbeschluss ist abrufbar unter https://ogy.de/EU-Standardvertragsklauseln.

Die Klauseln ersetzen die „alten" Standardvertragsklauseln, die bisher für diese Konstellation zur Verfügung standen. Die zulässigen Varianten der „alten" Standardvertragsklauseln waren in der Entscheidung 2001/497/EG und im Beschluss 2010/87/EU enthalten. Der Durchführungsbeschluss (EU) 2021/914 hebt diese beiden Rechtsquellen auf, weil sie jetzt überholt sind (siehe Art. 4 Abs. 2 und 3 des Durchführungsbeschlusses).

Die neuen „Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern" bilden den Anhang zum Durchführungsbeschluss (EU) 2021/915 →

Editorial

Ricarda Veidt, Chefredakteurin

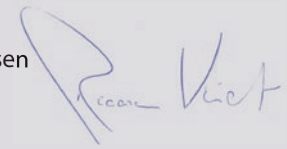
Kennen Sie schon das Hacker-Schaf?

Liebe Leserin, lieber Leser! Möglicherweise (besser gesagt: hoffentlich) ist es Ihnen bisher noch nicht persönlich begegnet – das Hacker-Schaf. Mit schwarzer Augenbinde und mit Unterstützung seiner Helfer, der Viren, treibt es sein Unwesen im Internet.

Das „Mal- und Rätselheft für Nachwuchsnerds", Heimat des Hacker-Schafs, ist nur eine von zahlreichen Broschüren, die das Bundesamt für Sicherheit in der Informationstechnik (BSI) in der Reihe „BSI für Bürger" herausgebracht hat. Gerade die neuen „Wegweiser für den digitalen Alltag" bereiten Themen wie die allgemeine Sicherheit im Internet, die sichere Nutzung von Smartphones, von sozialen Netzwerken, von Cloud-Diensten sowie dem Internet der Dinge (IoT) leicht verständlich auf. Vielleicht findet sich hier ja die eine oder andere Anregung für Ihre nächste Datenschutz-Schulung.

Die Broschüren sind abrufbar unter https://ogy.de/bsi-buerger-broschueren; das Schaf findet sich speziell unter https://ogy.de/bsi-hackerschaf.

Viel Freude beim Lesen
Ihre Ricarda Veidt



der europäischen Kommission vom 4. Juni 2021. Er ist abrufbar unter https://ogy.de/Standardvertragsklauseln-Auftragsverarbeitung.

Für sie gibt es kein Vorbild. Der Durchführungsbeschluss, der sie einführt, muss deshalb auch keine früheren Fassungen derartiger Klauseln aufheben.

Warum waren neue Standardvertragsklauseln für die Übermittlung in Drittländer notwendig?

Die bisherigen Standardvertragsklauseln für die Übermittlung in Drittländer stammten noch aus der Zeit vor dem Inkrafttreten der DSGVO am 25. Mai 2016. Formal waren sie trotzdem weiterhin anwendbar, weil die auf sie bezogenen „Feststellungen" der Europäischen Kommission über Standardvertragsklauseln weiterhin in Kraft blieben (Art. 46 Abs. 5 Satz 2 DSGVO). Das änderte aber nichts daran, dass ihr Inhalt nicht mehr zur DSGVO passte.

Hinzu kam, dass der Europäische Gerichtshof in der Entscheidung „Schrems II" vom 16. Juli 2020 eine ganze Reihe von Anforderungen an Datenübermittlungen ins Ausland aufstellte, die die vorhandenen Standardvertragsklauseln naturgemäß nicht berücksichtigten. Siehe dazu ausführlich Ehmann, Datenschutz PRAXIS Heft 9/2020, Seite 1. Auf diese Entscheidung nehmen die Erwägungsgründe des Durchführungsbeschlusses 2021/914 mehrfach Bezug (siehe etwa die Fußnoten 3, 10 und 11).

Wie ist das Verhältnis zwischen den beiden Arten von Standardvertragsklauseln?

Es gelten folgende Faustregeln:

- Die **Standardvertragsklauseln für die Übermittlung in Drittländer** sind definitionsgemäß immer relevant, wenn an einer Übermittlung eine Stelle in einem Drittland beteiligt ist. Das gilt auch dann, wenn diese Stelle die Rolle eines Auftragnehmers hat. Dazu, was genau ein „Drittland" ist, siehe Ehmann, Datenschutz PRAXIS Heft 1/2021, Seite 4.
- Die **Standardvertragsklauseln zwischen Verantwortlichen und Auftragsverarbeitern** sind dagegen für die Verwendung innerhalb der EU gedacht. Für Auftragsverhältnisse, bei denen Stellen in Drittländern beteiligt sind, sind sie nicht geeignet.

Diese Faustregeln beruhen auf dem unterschiedlichen Zweck der beiden Arten von Standardvertragsklauseln.

Standardvertragsklauseln für die Übermittlung in Drittländer

Standardvertragsklauseln für die Übermittlung in Drittländer kommen zum Einsatz, um ein – gemessen an den Vorgaben der Datenschutz-Grundverordnung – unzureichendes Datenschutzniveau im jeweiligen Drittland auszugleichen. Sie stellen „geeignete Garantien" dar, die eine Übermittlung in das Drittland dennoch rechtlich möglich machen.

Art. 46 Abs. 1 DSGVO fordert solche geeigneten Garantien, wenn das Datenschutzniveau in einem Drittland unzureichend ist. Art. 46 Abs. 2 Buchst. c DSGVO hält fest, dass Standarddatenschutzklauseln der Europäischen Kommission als eine solche geeignete Garantie anzusehen sind. Sie sorgen für „die Gewährleistung

Übermittlung in Drittländer und Auftragsverarbeitung

Warum ist das Verhältnis zwischen den beiden Arten von Standardvertragsklauseln wichtig?

Dass die Unterscheidung zwischen Standardvertragsklauseln für die Übermittlung in Drittländer und Klauseln für die Auftragsverarbeitung zentral ist, zeigt sich klar bei folgender Konstellation:

- Zwischen zwei Unternehmen innerhalb der EU besteht ein Vertrag über Auftragsverarbeitung auf der Basis der Standardvertragsklauseln für Auftragsverarbeitung.
- In dieses Vertragsverhältnis soll als Unterauftragnehmer ein weiteres Unternehmen einbezogen werden. Dieses Unternehmen ist in einem Drittland ansässig, das kein angemessenes Datenschutzniveau aufweist.
- In einem solchen Fall genügt es nicht, das Unternehmen im Drittland einfach zu einem weiteren Vertragspartner des vorhandenen Vertrags zu machen. Vielmehr müsste der Vertrag dann für alle drei Beteiligten auf die Standardvertragsklauseln für die Übermittlung an Drittländer umgestellt werden.
- Dieser Vertrag wiederum würde zugleich die Anforderungen für Verträge über eine Auftragsverarbeitung abdecken, die sich aus Art. 28 DSGVO ergeben – einschließlich der Anforderungen, die Art. 28 Abs. 4 DSGVO für den Einsatz von Unterauftragnehmern aufstellt.

Die geschilderte Konstellation behandelt Erwägungsgrund 15 zum Durchführungsbeschluss 2021/914 ausführlich. Beachten Sie ergänzend die Ausführungen in den Erwägungsgründen 8 und 9.

Das Beispiel zeigt, dass die Wahl der „richtigen" Standardvertragsklauseln durchaus eine Herausforderung darstellen kann. Alternative weitere Vertragsgestaltungen – etwa der Verzicht auf die Einbeziehung des Drittland-Unternehmens in den vorhandenen Vertrag und stattdessen der Abschluss eines geeigneten Vertrags zwischen dem Auftragnehmer in der EU und dem Drittland-Unternehmen – wären ebenfalls denkbar.

angemessener Datenschutzgarantien für internationale Datenübermittlungen." (so Erwägungsgrund 3 Satz 1 des Durchführungsbeschlusses 2021/914).

Standardvertragsklauseln für das Verhältnis zwischen Verantwortlichen und Auftragsverarbeitern

Standardvertragsklauseln für das Verhältnis zwischen Verantwortlichen und Auftragsverarbeitern sollen dagegen zum einen sicherstellen, dass die Beteiligten die Vorgaben der Grundverordnung für die Gestaltung des Rechtsverhältnisses zwischen Auftraggeber (Verantwortlichem) und Auftragsverarbeiter einhalten. Diese Vorgaben ergeben sich aus Art. 28 Abs. 3 DSGVO.

Kommen weitere Auftragsverarbeiter als Unterauftragnehmer ins Spiel, gewährleisten die Standardvertragsklauseln zum anderen auch die Beachtung der hierfür geltenden Vorgaben. Sie ergeben sich aus Art. 28 Abs. 4 DSGVO. Dass die Standardvertragsklauseln beide Aspekte abdecken, hält Art. 1 des Durchführungsbeschlusses 2021/915 fest.

Für Auftragsverhältnisse, bei denen Vertragspartner in einem Drittstaat beteiligt sind, gilt folgende Abgrenzung:

- Finden die Standardvertragsklauseln für die Übermittlung an Drittländer Verwendung, deckt ein solcher Vertrag „nebenbei" auch die Anforderungen ab, die sich für Auftraggeber und Auftragnehmer aus Art. 28 Abs. 3 und 4 DSGVO ergeben. Dies hält Art. 1 Abs. 2 des Durchführungsbeschlusses 2021/914 ausdrücklich fest. Erwägungsgrund 9 zum Durchführungsbeschluss 2021/914 und Erwägungsgrund 10 Sätze 1 und 2 zum Durchführungsbeschluss 2021/915 unterstreichen es. Der Vertrag wird dann also ausschließlich auf Basis dieser Standardvertragsklauseln abgeschlossen. Die Standardvertragsklauseln für die Auftragsverarbeitung spielen keine Rolle.
- Umgekehrt gilt: Ein Vertrag lediglich auf der Basis der Standardvertragsklauseln für die Auftragsverarbeitung deckt nicht die Anforderungen ab, die sich für die Übermittlung in Drittländer aus Art. 46 Abs. 1 DSGVO ergeben (so Erwägungsgrund 10 Satz 3 zum Durchführungsbeschluss 2021/915). Er kann also nicht einen Vertrag auf der Basis der Standardvertragsklauseln für die Übermittlung in Drittländer ersetzen.

Was hat es mit dem „modularen Aufbau" der Standardvertragsklauseln auf sich?

Bei den Standardvertragsklauseln für die Auftragsverarbeitung beschränkt sich der modulare Aufbau darauf, dass die Vertragspartner an einer Reihe von Stellen eine Auswahl zwischen jeweils zwei Optionen treffen müssen:

- Meist betrifft dies nur die Frage, ob die jeweilige Klausel an Bestimmungen der DSGVO anknüpfen soll („Verordnung (EU) 2016/679") oder an →

die „Verordnung (EU) 2018/1725“. In der Regel trifft es zu, die „Option 1“ zu wählen, also den Bezug auf die DS-GVO. Etwas anderes gilt nur, wenn ein Unternehmen für Organe, Einrichtungen oder sonstige Stellen der EU tätig wird. Dann wäre „Option 2“ die richtige. Denn die Verordnung (EU) 2018/1725 regelt den Datenschutz, der dort zu beachten ist. Sie ist bei Bedarf abrufbar unter https://ogy.de/VO-2018-1725.

- Lediglich an einer Stelle geht es bei der Wahl zwischen „Option 1“ und „Option 2“ um einen echten inhaltlichen Unterschied. Das betrifft die Frage, unter welchen Voraussetzungen der Auftragsverarbeiter Unterauftragnehmer einsetzen darf (Klausel 7.7). Bei „Option 1“ braucht der Auftragsverarbeiter dazu in jedem Einzelfall eine vorherige gesonderte Genehmigung. „Option 2“ sieht eine allgemeine schriftliche Genehmigung für diese Konstellation vor.

Unterscheidung je nach Konstellation

Bei den Standardvertragsklauseln für die Übermittlung an Drittländer prägt der modulare Aufbau dagegen das gesamte Vertragsmuster. In den einzelnen Klauseln sind maximal vier unterschiedliche Module vorgesehen. Sie knüpfen jeweils daran an, welche Konstellation vorliegt. Dabei unterscheiden die Module vier Konstellationen (Modulbezeichnungen in Großbuchstaben und mit ausgeschriebenen Ziffern):

- MODUL EINS: Übermittlung von Verantwortlichen an Verantwortliche
- MODUL ZWEI: Übermittlung von Verantwortlichen an Auftragsverarbeiter
- MODUL DREI: Übermittlung von Auftragsverarbeitern an Auftragsverarbeiter
- MODUL VIER: Übermittlung von Auftragsverarbeitern an Verantwortliche

Dürfen die Standardvertragsklauseln in einen umfassenderen Vertrag „eingebaut“ werden?

Diese Frage war bei den „alten“ Standardvertragsklauseln für die Übermittlung an Drittländer umstritten. Argument: Dies könnte dem Grundsatz widersprechen, dass die Klauseln, die die Europäische Kommission gebilligt hat, nicht abgeändert werden dürfen, wenn sie als „geeignete Garantie“ im Sinn von Art. 46 Abs. 1 DSGVO gelten sollen.

Die neuen Standardvertragsklauseln lassen ein solches Vorgehen ausdrücklich zu. Klausel 2 („Unabänderbarkeit der Klauseln“) der Standardvertragsklauseln für die Auftragsverarbeitung formuliert dies unter Buchst. b so: „Dies hindert die Parteien nicht daran, die in diesen Klauseln festgelegten Standardvertragsklauseln in einen umfangreicheren Vertrag aufzunehmen.“ Klausel 2 Buchst. a der Standardvertragsklauseln für die Übermittlung an Drittländer enthält eine entsprechende Formulierung.

Kann man vorsehen, dass weitere Vertragsparteien einem vorhandenen Vertrag „beitreten“?

Ja, beide Arten von Standardvertragsklauseln enthalten eine „Kopplungsklausel“, die den Beitritt weiterer Vertragsparteien durch „Ankoppeln“ möglich macht (siehe Klausel 7 der Standardvertragsklauseln für die Übermittlung an Drittländer und Klausel 5 der Standardvertragsklauseln für die Auftragsverarbeitung). Die Kopplungsklausel ist jeweils als „fakultativ“ gekennzeichnet. Man kann sie also einbauen – zur Not erst nachträglich –, man kann sie aber auch entfallen lassen.

Unternehmen, die miteinander verbunden sind, etwa in einem Konzern, werden die Klausel gerne nutzen. So lassen sich nämlich im Ergebnis „konzernweite Standardverträge“ gestalten, bei denen immer wieder neue Konzernunternehmen hinzukommen oder wegfallen, je nach Bedarf.

PRAXIS-TIPP

Die Modulbezeichnungen sind in allen Standardvertragsklauseln für die Übermittlung an Drittländer identisch. Das erleichtert es erheblich, das Vertragsmuster anzuwenden:

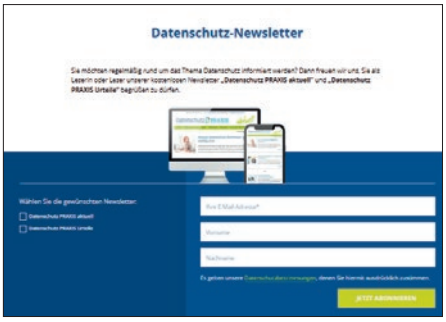
- ***Zunächst muss man einmal feststellen, welche der vier Konstellationen im konkreten Fall vorliegt (also z.B. MODUL ZWEI).***
- ***Dann wählt man überall dort, wo unterschiedliche Module zur Auswahl stehen, das dafür vorgesehene Modul aus (also z.B. MODUL ZWEI).***
- ***Die verschiedenen Module zu mischen, ist nicht zulässig. Liegt also z.B. die Konstellation „Übermittlung von Verantwortlichen an Auftragsverarbeiter“ vor, muss man bei allen Klauseln das jeweils dafür vorgesehene MODUL ZWEI wählen. Unzulässig wäre es dagegen, etwa bei Klausel 12 (Haftung) stattdessen MODUL EINS zu wählen, weil einem dies besser gefällt.***

Ab wann gelten die neuen Standardvertragsklauseln?

Die Standardvertragsklauseln für die Auftragsverarbeitung lassen sich faktisch ab sofort nutzen. Rechtlich korrekt: Sie stehen seit dem 27.6.2021 zur Verfügung – also ab dem 20. Tag nach ihrer Veröffentlichung im Amtsblatt der Europäischen Union vom 7.6.2021, so Art. 4 des Durchführungsbeschlusses 2021/915. Entsprechendes gilt für die neuen Standardvertragsklauseln für die Datenübermittlung in Drittländer (siehe Art. 4 Abs. 1 des Durchführungsbeschlusses 2021/914).

Verträge, die auf der Basis der „alten“ Standardvertragsklauseln für die Datenübermittlung in Drittländer geschlossen wurden, bieten noch bis zum 27. Dezember 2022 „geeignete Garantien“ (so Art. 4 Abs. 4 des Durchführungsbeschlusses 2021/914).

Dr. Eugen Ehmann ist seit vielen Jahren im Datenschutz aktiv. Wer regelmäßig über wichtige Gerichtsurteile im Datenschutz auf dem Laufenden bleiben möchte, abonniert seinen kostenlosen Urteils-Newsletter unter www.datenschutz-praxis.de/datenschutz-newsletter:



Rechtsgrundlagen für die Datenverarbeitung

Berechtigte Interessen und ihre Dokumentation im VVT

Mit Art. 6 Abs. 1 Buchst. f brachte die DSGVO eine neue Rechtsgrundlage für die Datenverarbeitung: das „berechtigte Interesse". Was genau verbirgt sich dahinter, und welche Voraussetzungen müssen erfüllt sein, um die Verarbeitung personenbezogener Daten darauf stützen zu können?

Das Grundprinzip des Datenschutzes, das sogenannte „Verbot mit Erlaubnisvorbehalt", war schon vor Anwendbarkeit der Datenschutz-Grundverordnung (DSGVO) im alten Bundesdatenschutzgesetz (BDSG a.F.) verankert. Die DSGVO greift es in Art. 6 auf. Es besagt, dass die Verarbeitung personenbezogener Daten grundsätzlich verboten und nur dann ausnahmsweise erlaubt ist, wenn es hierfür eine rechtliche Grundlage gibt.

Diese rechtliche Grundlage kann z.B. eine Einwilligung oder die Erfüllung eines Vertrags bzw. einer gesetzlichen Verpflichtung sein. Mit Art. 6 Abs. 1 Buchst. f DSGVO kam eine neue Rechtsgrundlage hinzu: das sogenannte „berechtigte Interesse". Was genau ist das eigentlich, und wann kann sich ein Verantwortlicher darauf stützen? Machen Sie dieses – zugegebenermaßen recht sperrige Thema – einmal zum Gegenstand Ihrer Datenschutzschulung. Denn oft nutzen Unternehmen nicht das Potenzial dieser Regelung.

Der Begriff des „berechtigten Interesses"

Der Begriff des „berechtigten Interesses" ist im Datenschutzrecht alles andere als neu. Bereits die Datenschutzrichtlinie (RL 95/46/EG), der Vorgänger der DSGVO, hat sie verwendet. Die Artikel-29-Datenschutzgruppe definierte sie seinerzeit als „(…) das Bestreben im weiteren Sinne, das ein für die Verarbeitung Verantwortlicher an dieser Verarbeitung haben kann, oder der Nutzen, den der für die Verarbeitung Verantwortliche aus der Verarbeitung zieht – oder den die Gesellschaft daraus ziehen könnte."

Diese reichlich schwammige Definition vermag auch die DSGVO nur teilweise zu konkretisieren. Die Erwägungsgründe 47 bis 49 greifen den Begriff des berechtigten Interesses auf und nennen Voraussetzungen sowie praktische Fallbeispiele für berechtigte Interessen.

Fallbeispiele aus den Erwägungsgründen

Als Indiz für das Vorliegen eines berechtigten Interesses sieht Erwägungsgrund 47 ein gewisses Beziehungsverhältnis zwischen dem Verantwortlichen und der betroffenen Person. Ein derartiges Beziehungsverhältnis liegt z.B. vor, wenn die betroffene Person eine Kundin oder ein Beschäftigter des Verantwortlichen ist.

Als berechtigte Interessen nennt Erwägungsgrund 47 die Verhinderung von Betrug sowie die Direktwerbung. Erwägungsgrund 48 ergänzt diese doch recht übersichtliche Aufzählung um das sogenannte „kleine Konzernprivileg". Er nennt als berechtigtes Interesse die Übermittlung personenbezogener Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke.

ACHTUNG!

Art. 6 Abs. 1 Buchst. f DSGVO gilt nicht für die Verarbeitung personenbezogener Daten durch Behörden in Erfüllung ihrer Aufgaben! Grund hierfür ist der Gedanke, dass staatliche Stellen personenbezogene Daten nur aufgrund gesetzlicher Regelungen verarbeiten dürfen.

Schließlich zählt nach Erwägungsgrund 49 auch die Gewährleistung der Netz- und Informationssicherheit zu den berechtigten Interessen des Verantwortlichen.

BEISPIELE

Fassen wir Fallbeispiele, die die Erwägungsgründe nennen, übersichtlich zusammen, so ergibt sich:

- *Betrug verhindern*
- *Direktwerbung*
- *personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke übermitteln*
- *Netz- und Informationssicherheit gewährleisten*

Auch wenn diese Beispiele in der Praxis sicherlich nicht alle Fallkonstellationen abdecken, so geben sie in wichtigen Bereichen eine Richtschnur vor, an der sich Verantwortliche und Datenschutzbeauftragte entlanghangeln können.

Voraussetzungen für die Verarbeitung aufgrund berechtigter Interessen

Mit der reinen Begriffsdefinition und der Aufzählung von Fallbeispielen ist es im Rahmen von Art. 6 Abs. 1 Buchst. f DSGVO jedoch nicht getan. Hinzutreten müssen vielmehr zwei weitere Voraussetzungen:

- Die Verarbeitung personenbezogener Daten muss für den Verantwortlichen **erforderlich** sein, um seine berechtigten Interessen zu wahren.
- Die **Abwägung** der widerstreitenden Interessen von betroffener Person und Verantwortlichem muss zugunsten des Verantwortlichen ausfallen.

Die Erforderlichkeit

Was der Jurist bereits aus dem Studium kennt, ist v.a. für Menschen ohne juristischen Hintergrund im ersten Moment etwas undurchsichtig. Auch hier hilft die DSGVO selbst weiter. Erwägungsgrund 39 erläutert die wichtigsten Grundsätze der Datenverarbeitung und geht dabei →

in Satz 9 auch auf das Merkmal der Erforderlichkeit ein: „Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann."

WICHTIG

Kurz und knapp zusammengefasst bedeutet das, dass von einer Erforderlichkeit immer dann ausgegangen werden darf, wenn es keinen anderen, einfacheren und genauso effektiven Weg für den Verantwortlichen gibt, um das gewünschte Ziel zu erreichen.

Hier ist erstmals eine konkrete Argumentation gefragt: Lässt sich die Erforderlichkeit mit ein bis zwei sachlichen Argumenten begründen? Hilfreich kann es sein, den Datenschutzgrundsatz der Datensparsamkeit und Datenminimierung im Hinterkopf zu haben. Denn grundsätzlich greifen hier sehr ähnliche Argumente.

Die Interessenabwägung

Etwas schwieriger, als die Erforderlichkeit zu bestimmen, gestaltet es sich, die Interessen abzuwägen.

Zentraler Ausgangspunkt für eine erfolgreiche Interessenabwägung ist die Zusammenstellung und Gewichtung der Interessen von betroffener Person und Verantwortlichem. Am besten gelingt dies in Tabellenform. So lässt sich auf einen Blick erkennen, wer die besseren bzw. gewichtigeren Argumente auf seiner Seite hat.

- Kommt man nach Gegenüberstellung der Interessen der betroffenen Person und des Verantwortlichen zu dem Schluss, dass die Interessen des Verantwortlichen überwiegen, lässt sich die Datenverarbeitung auf Art. 6 Abs. 1 Buchst. f DSGVO stützen.
- Kommt man dagegen zu dem Schluss, dass die Interessen der betroffenen Person überwiegen, kann der Verantwortliche die Datenverarbeitung in ihrer derzeitigen Form nicht auf Art. 6 Abs. 1 Buchst. f DSGVO stützen.

Interessen Verantwortlicher	Interessen betroffene Person
Die Betroffenen sind Mitarbeiter/Kunden des Verantwortlichen.	Es besteht keinerlei persönliche oder geschäftliche Beziehung zum Verantwortlichen.
Personenbezogene Daten werden nur in geringem Umfang verarbeitet.	Personenbezogene Daten werden in großem Umfang verarbeitet.
Betroffene müssen mit einer Datenverarbeitung rechnen, da sie ausdrücklich darauf hingewiesen wurden.	Betroffener wurde nicht über die geplante Datenverarbeitung aufgeklärt.
Datenverarbeitung ist branchenüblich und erwartbar.	Betroffener muss im vorliegenden Kontext vernünftigerweise nicht mit einer Verarbeitung seiner personenbezogenen Daten rechnen.
Es werden keine besonderen Kategorien personenbezogener Daten nach Art. 9 DSGVO verarbeitet.	Es werden auch besondere Kategorien personenbezogener Daten nach Art. 9 DSGVO verarbeitet.
Der Kreis der Betroffenen ist klein.	Der Kreis der Betroffenen ist groß.
Personenbezogene Daten werden nicht an Dritte übermittelt.	Personenbezogene Daten werden in großem Umfang an Dritte übermittelt.
Die verarbeiteten personenbezogenen Daten wurden beim Betroffenen selbst erhoben.	Die verarbeiteten personenbezogenen Daten wurden über Dritte oder öffentlich zugängliche Quellen erhoben.
Die Datenverarbeitung erfolgt nur während eines kurzen Zeitraums.	Die Datenverarbeitung erfolgt über einen längeren Zeitraum.

Beispiele für typische widerstreitende Interessen bei einer Interessenabwägung

Eine Möglichkeit, das Blatt doch noch zu wenden, bestünde dann z.B. darin, einen oder mehrere der Datenverarbeitungsparameter, die die unten stehende Tabelle nennt, positiv zu beeinflussen.

Nur wenn tatsächlich ein berechtigtes Interesse besteht, die Datenverarbeitung wirklich erforderlich ist und zusätzlich die Interessenabwägung zugunsten des Verantwortlichen ausfällt, kann ein Unternehmen die Datenverarbeitung auf Art. 6 Abs. 1 Buchst. f DSGVO stützen.

Eingriffsmöglichkeiten der betroffenen Person

Erfolgt die Verarbeitung personenbezogener Daten auf Grundlage des berechtigten Interesses, steht den betroffenen Personen nach Art. 21 DSGVO eine besondere Eingriffsmöglichkeit gegen diese Datenverarbeitung zu: das Widerspruchsrecht.

Da Betroffene durch Datenverarbeitungsvorgänge, die sich allein auf das berechtigte Interesse des Verantwortlichen stützen, besonderen Risiken und Gefahren ausgesetzt sein können, müssen Verantwortliche im Fall eines Widerspruchs gegen die Datenverarbeitung zwingende schutzwürdige Gründe nachweisen, wenn sie sie fortsetzen möchten. Etwas anderes gilt nur für Widersprüche gegen Direktwerbung. Diese muss der Verantwortliche ohne Wenn und Aber akzeptieren.

WICHTIG

Ein wichtiger Hinweis im Rahmen der Schulung: Verantwortliche müssen betroffene Personen bei Datenverarbeitungsvorgängen, die sich auf Art. 6 Abs. 1 Buchst. f DSGVO stützen, spätestens zum Zeitpunkt der ersten Kommunikation verständlich und getrennt von anderen Informationen auf ihr Widerspruchsrecht hinweisen.

Dokumentation des berechtigten Interesses

Art. 30 DSGVO gibt den Rahmen dafür vor, was Verantwortliche im Verzeichnis von Verarbeitungstätigkeiten (VVT) dokumentieren müssen. Obwohl Art. 30 DSGVO die Rechtsgrundlage der Daten-

verarbeitung nicht ausdrücklich nennt, empfiehlt es sich auch aus Sicht der Datenschutzkonferenz, sie in das Verzeichnis von Verarbeitungstätigkeiten aufzunehmen (siehe https://ogy.de/DSK-VVT, S. 2).

Während es bei anderen Rechtsgrundlagen genügt, rein den jeweiligen Artikel bzw. Paragrafen ggf. unter Verweis auf eine entsprechende Betriebsvereinbarung zu nennen, darf es bei Art. 6 Abs. 1 Buchst. f DSGVO „etwas mehr sein". Nicht zuletzt wird die lückenlose Dokumentation berechtigter Interessen im Verzeichnis von Verarbeitungstätigkeiten allen Verantwortlichen eine große Stütze sein, wenn z.B. die Datenschutzaufsichtsbehörde eine Kontrolle durchführt:

- Zum einen lässt sich damit nachweisen, dass der Verantwortliche auch über den eigentlichen Rahmen von Art. 30 DSGVO hinaus dokumentiert.
- Zum anderen ist der Ort, an dem das berechtigte Interesse dokumentiert ist, schnell und einfach auffindbar.

Berechtigtes Interesse häufiger als Rechtsgrundlage nutzen!

Speziell in Deutschland herrscht im Vergleich zu unseren Nachbarländern bezüglich der Rechtsgrundlage von Art. 6 Abs. 1 Buchst. f DSGVO große Zurückhaltung. Es bleibt zu hoffen, dass sich diese Praxis langfristig ändert.

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

Rechtsgrundlage(n) der Datenverarbeitung gem. Art. 5, 6 DSGVO:

Rechtsgrundlage	Anwendbarkeit
Einwilligung, Art. 6 Abs. 1 Buchst. a DSGVO	☐
(Vor-)Vertrag, Art. 6 Abs. 1 Buchst. b DSGVO	☐
gesetzliche Pflicht, Art. 6 Abs. 1 Buchst. c DSGVO	☐
berechtigtes Interesse, Art. 6 Abs. 1 Buchst. f DSGVO	☒
Beschäftigungsverhältnis, § 26 BDSG	☐
Sonstige Rechtsgrundlage:	☐

Dokumentation des berechtigten Interesses:

Vorliegen eines berechtigten Interesses des Verantwortlichen

z. B.:
– Verhinderung von Betrug
– Direktwerbung
– Übermittlung personenbezogener Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke
– Gewährleistung der Netz- und Informationssicherheit etc.
Die Datenverarbeitung beruht auf einem berechtigten Interesse des Verantwortlichen.

Erforderlichkeit

Individuelle Begründung mit ein bis zwei stichhaltigen Argumenten, ggf. unter Berücksichtigung der Datenschutzgrundsätze der Datensparsamkeit und Datenminimierung. Warum ist die Datenverarbeitung zur Wahrung der berechtigten Interessen des Verantwortlichen erforderlich? Warum gibt es für den Verantwortlichen keinen anderen, einfacheren und genauso effektiven Weg, um das gewünschte Ziel zu erreichen?

Interessenabwägung

Verantwortlicher	betroffene Person
Betroffene sind Mitarbeiter/Kunden des Verantwortlichen	*hat keinerlei persönliche oder geschäftliche Beziehung zum Verantwortlichen*
personenbezogene Daten werden nur in geringem Umfang verarbeitet	*personenbezogene Daten werden in großem Umfang verarbeitet*
Betroffene müssen mit einer Datenverarbeitung rechnen, da sie ausdrücklich darauf hingewiesen wurden	*wurde nicht über die geplante Datenverarbeitung aufgeklärt*
…	…

Ergebnis der Interessenabwägung

Begründete Entscheidung über die besseren bzw. gewichtigeren Argumente.
Die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen die Interessen des Verantwortlichen nicht, weil … *oder*
Die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person überwiegen die Interessen des Verantwortlichen, weil …

Eingriffsmöglichkeiten

Dokumentation des Prozesses für die Ausübung des Widerspruchsrechts nach Art. 21 DSGVO.

Checkliste für die Dokumentation des berechtigten Interesses im Verzeichnis von Verarbeitungstätigkeiten für den nicht-öffentlichen Bereich. Abonnenten der Datenschutz PRAXIS finden die Checkliste unter https://ogy.de/CL-VVT-berechtigte-Interessen.

Bild: iStock.com/metamorworks

Datenübermittlung

Schutzverletzung bei Wartungszugriffen von außen vermeiden (Teil 2)

Wie verhindern Verantwortliche, dass es bei Wartungsarbeiten zu Datenpannen kommt, weil Techniker auf Daten zugreifen, die nicht für sie bestimmt sind? Wir stellen weitere Maßnahmen zur Absicherung der Fernwartung vor und beleuchten, wie es sich mit der Sicherheit bei IoT-Geräten verhält.

PRAXIS-TIPP

Prüfen Sie im Sinne von Art. 32 DSGVO die Anforderungen an die Verfügbarkeit: Welche Kommunikationsschnittstellen werden für die Wartungsarbeiten genutzt und welche Sicherungen sind eingebaut? Prüfen Sie im Sinne der Vertraulichkeit, wie sichergestellt ist, dass die Verbindungen verlässlich unterbunden werden, nachdem die Wartungsarbeiten abgeschlossen sind, und wie das dokumentiert ist, sodass es sich einfach prüfen lässt.

Für jeden Fernwartungsvorgang sollte eindeutig geklärt sein, welche Kommunikationsschnittstellen und möglichen Zugänge für einen Verbindungsaufbau von außen erforderlich sind. Die Schnittstellen sollten sich auf das absolut notwendige Maß beschränken.

Tolerieren Sie auf keinen Fall, dass Wartungszugriffe hinter der Firewall im allgemeinen informationstechnischen Netz des Unternehmens landen und möglicherweise sogar auf Clients oder Server zugreifen können. Hier sind Netzsegmentierungen oder ähnliche technische Maßnahmen wie weitere Firewalls intern unabdingbar. Auch wenn es eher unwahrscheinlich klingt, dass hier Daten abfließen: Das hat es alles schon gegeben.

Zugänge nach Abschluss der Wartung kappen

Ist der Wartungszugriff aus der Ferne abgeschlossen, müssen alle zuvor geöffneten Kommunikationsverbindungen und sonstigen Zugänge wieder gekappt werden. Hier stellt sich die Frage, wer das auslöst:

- Überlässt ein Verantwortlicher die gesamte Fernwartung dem Dienstleister, so ist dieser auch dafür zuständig, die vorher aufgebauten Verbindungen zu kappen. Beim Verantwortlichen muss dann in der Folge jemand überprüfen, ob tatsächlich wieder alle Wartungszugänge unterbunden sind.
- Möglich ist auch, eine Zeitlimitierung für die Kommunikationsschnittstellen einzubauen, die der Dauer des üblichen Wartungsintervalls entspricht. Sobald absehbar ist, dass die Wartung im Einzelfall länger dauert, muss der Wartungsdienst Verbindung mit dem zu wartenden Unternehmen aufnehmen und eine Verlängerung initiieren. Ansonsten ist die Verbindung nach Abschluss der Arbeiten verlässlich gekappt.

Prüfen Sie, ob im Zusammenhang mit sicheren Schnittstellen zudem diese Fragen geklärt sind:

- Ist eine ausreichende Verschlüsselung vorhanden, wenn vertrauliche oder personenbezogene Daten im Rahmen der Wartung übertragen werden oder wenn ein War-

tungsdienstleister darauf zugreifen könnte (Art. 32 DSGVO)?
- Sind die Übertragungsprotokolle in der Lage, eine zufällige oder absichtliche Veränderung übertragener Daten zu erkennen und eine weitere Übertragung zu blockieren bzw. zufällige Übertragungen zu beheben (Art. 32 DSGVO – Integrität – zumindest wenn personenbezogene Daten beteiligt sind)?
- Falls erforderlich: Ist sichergestellt, dass bei kritischen Wartungsvorgängen redundante Übertragungswege und Schnittstellen zur Verfügung stehen? Das erfordert mehrere zusätzliche Sicherheitsmaßnahmen, kann aber bei Wartungszugriffen mit möglichen hohen finanziellen Folgeschäden bei Ausfällen der Maschinen und Anlagen durchaus lohnend sein. Bitte immer daran denken, dass mindestens die Daten der an der Maschine oder Anlage arbeitenden beschäftigten Personen mit übertragen werden!
- Kommen Protokollfunktionen zum Einsatz? Um die Kommunikation bei Wartungsvorgängen nachvollziehbar zu machen, sollten Protokollierungen vorhanden sein, über die sich nachträglich feststellen lässt, welche Daten wer wann an wen übertragen hat.

Internet of Things (IoT) und seine Wartung – sehr praktisch, aber was ist mit Datenschutz und Sicherheit?

Schaffen Verantwortliche IoT-Geräte oder -Messinstrumente an, achten sie oft mehr auf den Preis als auf die Sicherheit und den Datenschutz. Solche Geräte müssen dann mit VLAN, dem WLAN oder dem LAN verbunden werden. Der Wartungszugriff – oder wozu auch immer der Zugriff dann dient – erfolgt, ohne dass der Verantwortliche beteiligt ist.

Zugegeben, aus Sicht des Datenschutzes und der IT-Sicherheit ein Horrorszenario. Vor allem dann, wenn der Anbieter die Firmware dieser Geräte auch dann nicht aktualisiert, wenn Sicherheitslücken auftauchen. Solche Softwarebugs können Angreifer gezielt ausnutzen, um Schadsoftware einzuschleusen. Dazu benötigen sie eine IP-Adresse des Geräts. Mithilfe einer Suchmaschine wie Shodan lassen sich diese Geräte finden. Das oft nicht veränderte Passwort zu knacken, ist dann für Angreifer eher einfach. Das alles können schlecht gesicherte Online-Dienste fördern.

Versuchen Sie, herauszubekommen, wie viele IoT-Geräte oder -Messeinrichtungen es in Ihrem Unternehmen gibt. Dazu können auch Kaffeemaschinen oder Klimakomponenten gehören. Suchen Sie dann nach einer verantwortlichen Person für alle diese Gerätekomponenten! Und prüfen Sie zusammen mit dieser Person, ob und wie sich die unbefugte Übermittlung personenbezogener Daten über Online-Dienste bei Wartungen ausschließen lässt.

Besonders kritisch prüfen: unkontrollierten Einsatz von Online-Diensten

Je komplexer Maschinen oder Anlagen sind, desto vielfältiger sind die Hersteller für einzelne Komponenten. So sind möglicherweise Steuerungs- oder Messgeräte im Einsatz, die gar nicht vom Hersteller der Maschine oder Anlage stammen, aber dennoch gewartet werden. Hier richten Sie jetzt die kritischen Fragen an die Informationssicherheit:

- Sind die Komponenten mit einer Software versehen, die gepatcht wird, wenn Sicherheitslücken auftreten?
- Gilt das auch für Firmware?
- Wie erfahren die Betreiber der Maschine von den Sicherheitslücken?
- Wie wird der Onlinedienst initiiert? Geschieht das automatisch, oder muss der Zugriff per Onlinedienst für das Wartungsunternehmen freigeschaltet werden? Da nahezu jeder Datenverlust auch zum Verlust personenbezogener Daten führt, ist der Datenschutz hier ebenso betroffen.

Ermitteln Sie, welche Steuerungs- und Messgeräte im Besonderen, jedoch auch andere IoT-Geräte im Allgemeinen gewartet werden, ohne dass klar ist, ob die Firmware Sicherheitslücken hat, und wenn, ob und unter welchen Umständen diese gepatcht werden.

Den automatisierten Verbindungsaufbau verhindern!

Alle Beteiligten müssen sich darüber im Klaren sein, dass mit jedem automatisierten Verbindungsaufbau die Gefahr besteht, dass sich Angreifer zwischengeschaltet haben. Von daher sollten automatisierte Verbindungsaufbaumöglichkeiten die absolute Ausnahme bleiben. Gerade bei sehr günstigen Geräten sind →

WICHTIG

Achten Sie darauf, dass für jede zu wartende Maschine oder Anlage eine verantwortliche Person benannt ist. Sie muss in der Lage sein, die Wartungsvorgänge hinreichend zu überwachen, auch wenn das bei automatisierter Wartung erst im Nachhinein möglich ist. Ohne Kontrolle sollte hier nichts gehen. Prüfen Sie also, wer für welchen Wartungsvorgang die Verantwortung trägt und wer kontrolliert, ob die Wartungsvorgänge korrekt stattgefunden haben und ebenso korrekt beendet wurden. Auch sollte die Kappung der Zugänge für die Wartung dokumentiert sein.

sie jedoch eher die Regel. Oft sind sich Verantwortliche dieses Risikos nicht bewusst oder ignorieren die Risiken. Ist eine Sicherheitslücke nicht gepatcht, können Angreifer zumindest die äußeren Grenzen der IT-Infrastruktur überwinden. Empfehlen Sie daher, wo irgend möglich automatisierte Wege des Verbindungsaufbaus zu vermeiden.

Prüfen Sie, ob, und wenn ja, wie viele Möglichkeiten des automatisierten Verbindungsaufbaus vorhanden sind und ob sich die Verantwortlichen für die Wartung des Risikos bewusst sind. Gehen Sie zusätzlich der Frage nach, ob die Risiken aktuell bewertet sind, wie das Art. 24 DSGVO verbindlich vorgibt! Besteht Handlungsbedarf, zögern Sie nicht, die Verantwortlichen darauf anzusprechen.

PRAXIS-TIPP

Prüfen Sie, wie umfassend die Wartungszugriffe sind und in welchem Umfang und mit welchen Risiken auch personenbezogene Daten betroffen sind. Ermitteln Sie die Schutzstufen der Datenkategorien. Prüfen Sie die ganze Palette der technisch-organisatorischen Maßnahmen! Sie werden oft feststellen: Nicht nur Sie als Datenschutzbeauftragte(r) kennen das Unternehmen erstaunlich genau. Auch Wartungsdienste sind nicht selten in dieser Lage. Prüfen Sie, welche Wartungsunterlagen die Dienstleister haben und welche Zugänge zu personenbezogenen Daten sie damit auftun können!

Und wenn es sich schon nicht vermeiden lässt, dass die IoT-Geräte automatisiert Verbindungen aufbauen, dann sollte auf jeden Fall jede einzelne Verbindung mit neuen Zugangsdaten arbeiten, die frisch generiert und möglichst über eine Mehrfaktorauthentifizierung an das Gerät, das die Verbindung aufbauen will, übermittelt werden.

Dokumentation bei der Fernwartung

Nicht nur für Rechnungszwecke sollte selbstverständlich sein, jeden Fernwartungszugriff angemessen zu dokumentieren. In der Regel enthalten diese Unterlagen der Dokumentation vertrauliche oder streng vertrauliche Informationen. In eher geringerem Umfang werden auch personenbezogene Daten dabei sein.

Anders liegt der Fall bei Wartungsarbeiten an medizinischen Geräten, wenn dort Dokumentationen in Form von Patientendaten vorliegen, beispielsweise bei der Wartung von Röntgengeräten. Es ist also bei der Fernwartung von Maschinen und Anlagen oft ebenso eine Frage des Datenschutzes, wie die Dokumentation der Fernwartung erfolgt, nicht nur eine Frage der Informationssicherheit. Erstreckt sich die Fernwartung dazu auf Serversysteme, Clients, Notebooks oder auf Software, ist der Datenschutz praktisch immer betroffen.

In zahlreichen Fällen greift ein Dienstleister bei der Fernwartung auf ein Betriebshandbuch zurück. Dies ist umso öfter der Fall, je komplexer die zu wartenden Maschinen oder Anlagen sind. Dieses Betriebshandbuch regelt, von welchem System aus mit welchen Rechten und durch welche Fachabteilung oder durch welchen Supportdienstleister auf Maschinen, Anlagen und Dokumentationen zugegriffen werden darf. Nutzen Sie, sofern vorhanden, solch ein Betriebshandbuch für Ihre Recherche.

Fernwartung durch Dritte

Immer häufiger führt der Hersteller der Anlagen und Maschinen die Fernwartung nicht mit eigenen Ressourcen durch, sondern arbeitet mit Dritten, also Subunternehmern. Normalerweise ist das schon im Vertrag zur Lieferung und Wartung von Anlagen und Maschinen als Auftragsverarbeitung geregelt. Wenn nicht, müssen Sie prüfen, ob es sich bei der Wartung um Auftragsverarbeitung handelt.

Klären Sie zur Fernwartung durch Dritte darüber hinaus folgende Punkte:

- Nimmt ein Wartungsdienstleister bei der Fernwartung Änderungen vor, etwa bei der Konfiguration von Maschinen und Anlagen, muss er dokumentieren, welche Änderungen das waren, und diese Dokumentation dem Auftraggeber der Fernwartung übergeben. Ist das gegeben?
- Soweit möglich sollten eigene Spezialisten alle Fernwartungszugriffe überwachen oder zumindest beobachten. Geht das nicht, muss jemand die Protokolle über den Wartungszugriff genau auswerten. Die Support-Techniker des Wartungsdienstleisters kennen sich mit der von ihnen gewarteten Anlage sehr gut aus, sind aber nicht immer in alle Einzelheiten der Informationstechnik beim Kunden eingewiesen. Hier kann es leicht zu Konfigurationsfehlern kommen, die später im schlimmsten Fall eine offene Netzstruktur zur Folge haben. Ist diese Überwachung der Fernwartungszugriffe gewährleistet?
- Kann niemand die Fernwartung durch Dritte intern überwachen, sollte sie zumindest in Zeiten stattfinden, in denen die Produktion ruht. Jede „Operation am offenen Herzen" birgt Risiken. Das kann dann auch den Datenschutz betreffen. Denn wenn allgemeine Netze während des Wartungszugriffs offen sind, können leicht weitere Daten abgegriffen werden. Wie sieht es da bei Ihnen aus?

Aufgabe	Umsetzung
Wartungsvertrag auf Auftragsverarbeitung prüfen	Klären Sie für jeden einzelnen Wartungsfall, ob hierfür ein Wartungsvertrag vorliegt, ob dabei personenbezogene Daten betroffen sein können, und wenn das so ist, ob der Wartungsvertrag auch als Vertrag über Auftragsverarbeitung ausgelegt ist. Weisen Sie andernfalls darauf hin, dass die Verträge zu erstellen oder zu ergänzen sind.
Anbindung ans Internet	Klären Sie intern, in welcher technischen Form Messgeräte, auf die der Support des Wartungsdienstes direkt zugreifen kann, ans Internet angebunden sind. Dies ist eine Frage der technischen und organisatorischen Maßnahmen, betrifft aber auch die Informationssicherheit. Zu klären ist zudem, wie Sicherheitsüberprüfungen stattfinden, ob Updates oder Patches erfolgen und wie sichergestellt ist, dass sich nach Einspielen der Updates oder Patches die Sicherheit der Abläufe und damit des Datenschutzes sowie der Informationssicherheit garantieren lassen (siehe dazu Häcker, Datenschutz PRAXIS Heft 5/2021, S. 8–11). Prüfen Sie hier also auch, ob vollständige und aktuelle Wartungsprotokolle sowie Protokolle für Sicherheitsüberprüfungen vorliegen. Möglicherweise sind diese Daten Rechnungsdaten. Insofern ist auch die Buchführung betroffen.
Differenzierte Verarbeitungstätigkeiten	In der Folge sind je nach Art des technischen Zugriffs unterschiedliche Verarbeitungstätigkeiten zu dokumentieren. Nehmen Sie außerdem eine Risikoermittlung hinsichtlich der Verarbeitung personenbezogener Daten vor und überprüfen Sie sie regelmäßig auf Aktualität und Vollständigkeit.
Datenschutz-Folgenabschätzung prüfen	Gegebenenfalls ist eine Datenschutz-Folgenabschätzung erforderlich, nämlich dann, wenn sich auf technische Weise nicht sicherstellen lässt, dass die personenbezogenen Daten nicht in fremde Hände gelangen können.
Abstimmung mit dem Beauftragten für Informationssicherheit	Da in jedem Fall auch die Informationssicherheit betroffen ist, binden Sie – soweit vorhanden – den Informationssicherheitsbeauftragten ein.
Aufnahme in Ihre Berichte	Nehmen Sie das Ergebnis der Beschreibungen der Verarbeitungstätigkeiten und der Überprüfungen in Ihren Jahresbericht auf.

Die sechs wichtigsten Aufgaben von Datenschutzbeauftragten im Rahmen der Prüfung von Wartung

- Grundsätzlich muss es möglich sein, die Fernwartung zu unterbrechen oder abzubrechen. Geht das bei Ihnen?
- Legt der Wartungstechniker während des Wartungsvorgangs Daten auf Systemen des Auftraggebers ab, muss dies sauber dokumentiert sein. Nicht mehr erforderliche Daten sind nach Ende des Wartungsvorgangs wirksam zu entfernen. Nach außen übermittelte Messroutinen können zwar während eines Wartungszugriffs erforderlich sein, sind aber während einer laufenden Produktion sicherlich kontraproduktiv. Ist sichergestellt, dass nach Ende des Wartungsvorgangs alles wieder „auf Anfang“ gestellt ist?
- Das Personal des Support-Dienstleisters muss in ähnlicher Weise vertraglich gebunden und unterwiesen sein, wie das für eigene beschäftigte Personen auch gilt. Mindestanforderung ist eine angemessene Vertraulichkeitsvereinbarung. Sicherzustellen ist auch, dass Zugriffsdaten nach Abschluss der Wartungsarbeiten, sofern sie nicht aus rechtlichen Gründen protokolliert werden müssen, zu löschen sind. Außerdem ist festzulegen, welche Pflichten das externe Wartungspersonal hat und über welche Kompetenzen das Personal verfügen muss. Sicher waren Sie als Datenschutzbeauftragte(r) in die Vertragsgestaltung involviert. Wenn nicht, überprüfen Sie jetzt die Wartungsverträge.

Berichten und dokumentieren

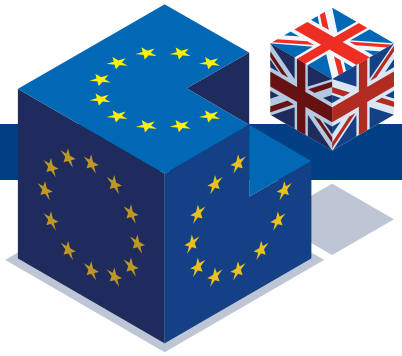
Im Rahmen Ihrer Überwachungsaufgabe ist es sinnvoll, diesen – zugegebenermaßen sehr umfangreichen – Themenbereich in Ihre Prüfroutine aufzunehmen. Besprechen Sie das Ergebnis mit dem Verantwortlichen und führen Sie es in Ihrem (Jahres-)Bericht auf.

Für Datenschutzbeauftragte ist die Wartung eine interessante Herausforderung. Nicht umsonst ist Datenschutzbeauftragte(r) einer der interessantesten Berufe der Welt.

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

Je komplexer, desto kritischer

Je komplexer Produktionsanlagen sind, desto mehr Hersteller können hier beteiligt sein und desto komplexer sind die Wartungsvorgänge. Umso kritischer sind aber auch Ausfälle von Anlagen und Maschinen, weil dies hohe Kosten verursacht und weil meistens weitere Schnittstellen zu Datenbanken im Unternehmen vorhanden sind. Je größer der Grad an Automatisierung und je intensiver der Einsatz von Robotern, desto größer können die Schäden sein, wenn Dritte unkontrolliert per Fernwartung auf Anlagen zugreifen.



Bewältigung des Brexit

Adäquater Datenschutz in Großbritannien

Die Europäische Kommission hat förmlich festgestellt, dass im Vereinigten Königreich ein angemessenes Datenschutzniveau herrscht. Der Angemessenheitsbeschluss gemäß Art. 45 DSGVO umfasst nicht weniger als 92 Seiten (plus Deckblatt). Dabei besteht der „verfügende Teil" des Beschlusses aus nur fünf recht kurzen Artikeln. Den Löwenanteil nimmt der „begründende Teil" des Beschlusses mit 292 Erwägungsgründen ein.

Mit Ablauf des 27. Juni 2025 tritt der Beschluss automatisch außer Kraft, wenn bis dahin kein neuer Angemessenheitsbeschluss ergangen ist (so Art. 4 des Beschlusses). Diese „Auslaufklausel" („sunset clause") führt dazu, dass die Planungssicherheit für Unternehmen zeitlich relativ begrenzt ist. Das ist v.a. dann zu berücksichtigen, wenn es um Verträge geht, deren Laufzeit über den 27. Juni 2025 hinausreicht.

Breiten Raum nehmen in den Erwägungsgründen 175 bis 272 die Zugriffsbefugnisse von britischen Behörden für Zwecke der nationalen Sicherheit ein. Solche Befugnisse haben der Security Service (MI5), der Secret Intelligence Service (SIS) und die Government Communications Headquarters (GCHQ). Die Möglichkeiten des Rechtsschutzes („judicial redress") gegen Maßnahmen dieser Nachrichtendienste sprechen die Erwägungsgründe 263 bis 269 ausführlich an. Zuständig hierfür ist „The Investigatory Powers Tribunal" (IPT) Dieses Gericht gibt es erst seit dem Jahr 2016. Es verfügt unter https://www.ipt-uk.com über einen umfangreichen Internetauftritt. Rechtsschutzmöglichkeiten bestehen dabei auch für Personen, die weder britische Staatsangehörige noch im Vereinigten Königreich ansässig sind.

Der Angemessenheitsbeschluss vom 28.6.2021 – C (2021) 4800 final ist abrufbar unter https://ogy.de/angemessenheitsbeschluss-uk. Eine Pressemitteilung der Europäischen Kommission vom 28. Juni 2021 erläutert ihn aus Sicht der Kommission. Sie ist abrufbar unter https://ogy.de/pm-angemessenheitsbeschluss.

Bild: iStock.com/id-work

Biometrische Zeiterfassung

Einwilligung denkbar, aber …

„Es ist … nicht auszuschließen, dass Arbeitgeber ein biometrisches Zeiterfassungssystem auf Basis wirksamer Einwilligungserklärungen der Beschäftigten datenschutzkonform einführen und nutzen können. Die Anforderungen an eine wirksame Einwilligungserklärung sollten von Verantwortlichen jedoch nicht unterschätzt werden." Diese Auffassung vertritt die hessische Datenschutzaufsicht.

Zentrale Fragen

Ein Arbeitgeber, der eine solche Einwilligungslösung anstrebt, muss sich aus Sicht der hessischen Aufsichtsbehörde die folgenden Fragen stellen:

1. Ist die Einwilligung überhaupt für die geplante Datenverarbeitung geeignet?

Das setzt voraus, dass die betroffenen Beschäftigten die Einwilligung jederzeit (mit Wirkung für die Zukunft) widerrufen und sich der Datenverarbeitungsprozess – je nach Willensbekundung der betroffenen Beschäftigten – „unterschiedlich" ausgestalten lässt (Alternativverhalten). Speziell für die biometrische Arbeitszeiterfassung muss der Arbeitgeber daher eine alternative Möglichkeit der Zeiterfassung vorsehen (z.B. mittels Chipkarte oder Token).

2. Kann von einer informierten Willensbekundung ausgegangen werden?

Mit Blick auf die Rechenschaftspflicht des Verantwortlichen empfiehlt es sich, den Beschäftigten die Informationen in Textform in einer klaren und einfachen Sprache zur Verfügung zu stellen.

3. Wurden die betroffenen Beschäftigten über ihr Widerrufsrecht aufgeklärt?
4. Erfolgt die Einwilligung der Beschäftigten auf freiwilliger Basis?
5. Werden die Formerfordernisse für die Einwilligung im Beschäftigungsverhältnis beachtet?

Nach § 26 Abs. 2 Satz 3 Bundesdatenschutzgesetz (BDSG) hat die Einwilligung schriftlich oder elektronisch zu erfolgen, soweit nicht wegen der besonderen Umstände eine andere Form angemessen ist.

6. Kann der Verantwortliche nachweisen, dass die betroffene Person wirksam in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat?

Keine Alternative zur Einwilligung

Angesichts der hohen Hürden dürften die meisten Arbeitgeber eine Einwilligungslösung für die biometrische Zeiterfassung kaum als attraktiv empfinden. Ohne sie geht es aber nicht. Denn auf andere Rechtsgrundlagen in der DSGVO lässt sich nach Auffassung der hessischen Datenschutzaufsicht eine biometrische Zeiterfassung nicht stützen.

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

Bild: iStock.com/Guzaliia Filimonova

Das TTDSG setzt u.a. die Cookie-Regelung der ePrivacy-Richtlinie um

Ein paar neue und viele alte Anforderungen

Das TTDSG kommt: ein Überblick

Das Telekommunikations-Telemedien-Datenschutzgesetz (TTDSG) regelt die Anforderungen an den Datenschutz im Bereich Telekommunikation und Telemedien – schreibt aber in einigen Bereichen nur die alten Regelungen fort. Das kann Segen und Fluch zugleich sein.

Bereits seit dem Anwendungsbeginn der Datenschutz-Grundverordnung (DSGVO) am 25.05.2018 besteht Bedarf, die speziellen Datenschutzbestimmungen im Telekommunikationsgesetz (§§ 88 ff. TKG) und im Telemediengesetz (§§ 11 ff. TMG) anzupassen. Hinzu kommt, dass das TKG insgesamt im Zuge des Telekommunikationsmodernisierungsgesetzes neu gestaltet wird und es – anders als bisher – zum 01.12.2021 ohne Datenschutzregelungen gelten soll. Gerade die Frage nach der Geltung der TKG-Regelungen für sogenannte OTT-Dienste ist dabei inhaltlich ein wesentlicher treibender Faktor.

Die Entscheidung „Cookie-Einwilligung II", in der der Bundesgerichtshof (BGH) dem deutschen Gesetzgeber attestiert, dass er seit rund zehn Jahren versäumt hat, die Cookie-Regelung umzusetzen, dürfte sich ebenfalls ausgewirkt haben (siehe dazu Eckhardt, Datenschutz PRAXIS Heft 10/2020, S. 4–6). Großer Druck ist aber kein ein Garant für wohlüberlegte Regelungen. Diese Kritik wird sich auch das TTDSG gefallen lassen müssen. Denn im Wesentlichen „alter Wein in neuen Schläuchen" ist eben keine Modernisierung.

ACHTUNG!

Das TTDSG tritt am 01.12.2021 in Kraft. Eine Übergangsfrist ist nicht vorgesehen. Mit anderen Worten: Das Zeitfenster für Anpassungen ist klein!

Das Verhältnis TTDSG – DSGVO

Die Datenschutzbestimmungen im TTDSG sind zwar fachlich spezieller als die DSGVO. Aber die DSGVO hat als EU-Verordnung dennoch Anwendungsvorrang vor nationalen Datenschutzbestimmungen. Das gilt aufgrund der technologieneutralen Geltung der DSGVO (Erwägungsgrund 15 DSGVO) auch für Telekommunikation und Telemedien. Die Öffnung ist Art. 95 DSGVO: Die DSGVO „erlegt natürlichen oder juristischen Personen in Bezug auf die Verarbeitung in Verbindung mit der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste in öffentlichen Kommunikationsnetzen in der Union keine zusätzlichen Pflichten auf, soweit sie besonderen in der Richtlinie 2002/58/EG festgelegten Pflichten unterliegen, die dasselbe Ziel verfolgen."

Mit anderen Worten: Soweit das TTDSG Regelungen der Datenschutzrichtlinie für Elektronische Kommunikationsdienste 2002/58/EG – auch bezeichnet als ePrivacy-Richtlinie – für öffentlich zugängliche elektronische Kommunikationsdienste in öffentlichen Kommunikationsnetzen umsetzt, gilt die DSGVO nicht.

Was auf den ersten Blick nach wenig relevanter „Hintergrundbeleuchtung" klingt, wird zukünftig in der Praxis des TTDSG immer wieder bedeutsam werden. Denn: Der deutsche Gesetzgeber überschreitet den Spielraum, den Art. 95 DSGVO zwar schafft, aber ausdrücklich auf „öffentlich zugängliche Telekommunikationsdienste" begrenzt, immer wieder, indem er mit dem TTDSG schlicht an „alten Zöpfen" festhält. Das wirkt sich etwa bei der Bewertung der privaten TK-Nutzung (siehe unten) und § 19 TTDSG (siehe unten) aus.

Die Struktur des TTDSG

Die endgültige Fassung des TTDSG wurde am 28.06.2021 im Bundesgesetzblatt veröffentlicht (siehe https://ogy.de/text-ttdsg-bgbl). Wer beim Einarbeiten in das TTDSG im Hinterkopf hat, dass der deutsche Gesetzgeber im Wesentlichen nur Datenschutzbestimmungen aus dem bisherigen TKG und dem bisherigen TMG zusammenführt, dem erschließt sich der Aufbau des TTDSG recht gut: →

- Teil 1 und 4 regeln die Allgemeinen Vorschriften und die Straf- und Bußgeldvorschriften sowie die Aufsicht.
- Teil 2 des TTDSG regelt den Datenschutz und den Schutz der Privatsphäre in der Telekommunikation.
- Teil 3 regelt den Telemediendatenschutz und Endeinrichtungen.

Kurzum: Beim TTDSG handelt es sich nicht um ein Datenschutzgesetz, das beide Bereiche gemeinsam verzahnt regelt, sondern um ein Gesetz, das zwei verschiedene Gesetze unter einem gemeinsamen Titel zusammenfasst.

Dementsprechend ist die Struktur des TTDSG nicht durchgängig schlüssig. Während sich der persönliche Anwendungsbereich der Telemedien-Datenschutzbestimmungen aus der Definition im Allgemeinen Teil (dort § 2 TTDSG) ergibt, ist der persönlichen Anwendungsbereich der TK-Datenschutzbestimmungen nicht im Allgemeinen Teil, sondern in Teil 2 des TTDSG geregelt. Wenn man's einmal weiß, ist es nicht mehr kompliziert …

Die Gleichstellung von Daten juristischer Personen mit personenbezogenen Daten und die Einbeziehung in den TK-Datenschutz durch § 1 Abs. 2 TTDSG ist nicht neu. Das ist in § 91 Abs. 1 des bisherigen TKG ebenso gestaltet und trägt dem Umstand des grundrechtlichen Schutzes des Fernmeldegeheimnisses durch Art. 10 Grundgesetz Rechnung. Die Erweiterung ist unionsrechtlich wohl unbedenklich.

Abgrenzung der Regelungsbereiche

Bereits seit die Vorgängerregelungen der Datenschutzbestimmungen des TMG galten – nämlich das Teledienstedatenschutzgesetz (TDDSG) –, war die Abgrenzung der Anwendungsbereiche der Datenschutzbestimmungen von TKG und TMG umstritten und durch den Gesetzgeber nicht geklärt. Diese Klarstellung erfolgt auch vorliegend nicht (§ 1 TTDSG). Es bleibt beim Nebeneinander von zwei Datenschutzgesetzen. Denn das TTDSG nennt beide Bereich hintereinander als Anwendungsbereich und regelt sie dann eigenständig und voneinander unabhängig in Teil 2 oder in Teil 3.

PRAXIS-TIPP

Für die Praxis bedeutet das: Der Verantwortliche muss den Dienst, um den es geht, zunächst einordnen: Handelt es sich um einen Telekommunikationsdienst? Dann ist Teil 2 des TTDSG relevant. Geht es um ein Telemedium, ist Teil 3 einschlägig.

§ 1 TTDSG nimmt für die Begriffsbestimmung auf das TKG, das TMG und die DSGVO Bezug mit Ausnahme der in § 2 TTDSG definierten Begriffe. Das TTDSG lässt sich also nicht anwenden, ohne zugleich das (ebenfalls ab 01.12.2021 geltende) TKG und das TMG hinzuzunehmen.

Telekommunikation: „Alter Wein in neuen Schläuchen"

Die zentrale Regelung für den persönlichen Anwendungsbereich der TK-Datenschutzbestimmungen ist § 3 Abs. 1 TTDSG. Er definiert, wer das Fernmeldegeheimnis zu beachten hat. Die weiteren TK-Datenschutzbestimmungen des TTDSG nehmen hierauf Bezug, um die Verpflichteten festzulegen.

Inhaltlich lehnen sich die Regelungen zum TK-Datenschutz von §§ 3 bis 18 TTDSG stark an die bisherigen Datenschutzregelungen im TKG an. Große Veränderungen finden hier nicht statt. Das ist mit Blick auf die kurze Zeitspanne zwischen der Verabschiedung des TTDSG und dessen Geltung auch positiv.

Neu: OTT-Anbieter müssen schärfere Datenschutzregelungen beachten

Eine wesentliche Neuerung soll sein, dass die TK-Datenschutzbestimmungen die sogenannten „Over-The-Top"-(OTT-) Dienste erfassen. Diese Dienste werden über Internetverbindungen angeboten. Der Internetanbieter selbst hat aber keinen Einfluss auf solche Dienste. Der Dienst und die dafür genutzte Infrastruktur sind voneinander getrennt. Beispiele sind etwa gmail oder Messengerdienste.

Ihre Einbindung erfolgt dadurch, dass die Definition von Telekommunikationsdienst in § 3 Nr. 61 des zukünftigen TKG auch sogenannte interpersonelle Telekommunikationsdienste (definiert in § 3 Nr. 24 des zukünftigen TKG) umfasst. Das modernisiert tatsächlich den TK-Datenschutz.

In Bezug auf OTT-Dienste bedeutet das für die Praxis: Anbieter von OTT-Diensten müssen sich ab dem 01.12.2021 an die Vorgaben des TTDSG halten, die in einigen Aspekten strenger sind als die DSGVO.

Rechtsunsicherheit bei privater E-Mail- und Internetnutzung im Unternehmen

Weiterhin sollen die TK-Datenschutzbestimmungen auch geschäftsmäßige Erbringer von Telekommunikationsdiensten umfassen (§ 3 Abs. 2 Nr. 2 TTDSG). Nach zutreffender und überzeugender Ansicht fallen Arbeitgeber, die ihren Mitarbeiterinnen und Mitarbeitern die private Nutzung der Telekommunikation gestatten – oder dulden – hierunter. Der praktische Unterschied besteht darin, dass nach der DSGVO eine Lösung über die Interessenabwägung in Betracht kommt, aber der TK-Datenschutz im TTDSG das nicht vorsieht.

Allerdings ist diese Ausdehnung der Anwendung der TK-Datenschutzbestimmungen nicht mit Art. 95 DSGVO vereinbar (siehe oben). Denn eine Öffnung der DSGVO besteht nur für „öffentlich zugängliche" Dienste, auf die sich § 2 Abs. 2 Nr. 1 TTDSG bezieht. In diesem Punkt schreibt der deutsche Gesetzgeber schlicht die bisherige Regelung im TKG-Datenschutz (§§ 88, 91 des bisherigen TKG) fort, ohne die notwendige inhaltliche Anpassung an die DSGVO vorzunehmen.

In Bezug auf private Nutzung von Telekommunikation im Unternehmen bedeutet das für die Praxis: Formal gilt die Vorgabe des TTDSG. Tatsächlich ist aber davon auszugehen, dass die DSGVO die-

se Gestaltung verdrängt und die Datenschutzbestimmungen des TTDSG nicht maßgeblich sind. Bis zur Klärung durch den Europäischen Gerichtshof schafft das TTDSG also Rechtsunsicherheit.

Rechtslage bei der privaten TK-Nutzung

Zur Rechtslage in Bezug auf die private Telekommunikationsnutzung in Unternehmen siehe Eckhardt, Datenschutz PRAXIS Heft 04/2020, S. 1–4. Hieran hat sich aufgrund von Art. 95 DSGVO nichts dadurch geändert, dass der deutsche Gesetzgeber dasselbe wieder in das TTDSG hineinschreibt.

Neu: Rechte der Erben

Neu ist auch eine Klarstellung der Rechte der Erben des Endnutzers und anderer berechtigter Personen in § 4 TTDSG. Das Fernmeldegeheimnis steht der Wahrnehmung von Rechten gegenüber dem Anbieter des Telekommunikationsdienstes nicht entgegen, wenn ein Erbe oder eine andere berechtigte Person diese Rechte wahrnimmt. Es stellt sich jedoch die Frage, ob es nicht sinnvoller gewesen wäre, die Regelung im Interesse der Rechtsklarheit auch auf Telemedien auszudehnen.

Telemedien: Was ist neu?

Für was und wen die Regelungen in Teil 3 (§§ 19–24) des TTDSG gelten, ergibt sich aus der Definition für „Anbieter von Telemedien" in § 3 Abs. 2 Nr. 1 TTDSG. Was ein Telemedium ist, ergibt sich durch die Verweisung von § 2 Abs. 1 TTDSG auf die Begriffsbestimmungen des TMG. Der Anwendungsbereich wird damit gegenüber dem bisherigen § 11 TMG neu geregelt.

Die Bestimmungen von §§ 19 bis 23 TTDSG sind aus dem bisherigen TMG übernommen und dienen überwiegend dazu, staatliche Auskunftsverfahren zu regeln. Soweit § 19 TTDSG Regelungen von § 13 des bisherigen TMG übernimmt, liegt nahe, dass sie durch den Anwendungsvorrang der DSGVO verdrängt werden.

Cookie-Regelung

§ 25 TTDSG setzt erstmals die Cookie-Regelung von Art. 5 Abs. 3 der ePrivacy-Richtlinie in der Fassung der Richtlinie 2009/136/EG um. Der BGH hat dieser Regelung faktisch bereits durch seine Entscheidung „Cookie-Einwilligung II" Geltung verschafft. Die Umsetzung erfolgt eng an der Vorgabe der Richtlinie. Sie lässt sich vereinfacht auf die folgende Formel bringen:

- Die Speicherung von Informationen in der Endeinrichtung des Endnutzers oder der Zugriff auf Informationen, die bereits in der Endeinrichtung gespeichert sind, sind nur zulässig, wenn der Endnutzer eingewilligt hat (ausführlicher in § 25 Abs. 1 TTDSG).
- Ausnahmen: Es sei denn,
  - es ist der alleinige Zweck, eine Nachricht über ein öffentliches Telekommunikationsnetz zu übertragen (ausführlicher in § 25 Abs. 2 Nr. 1 TTDSG), oder
  - es ist unbedingt erforderlich, damit der Anbieter eines Telemediendienstes einen Telemediendienst zur Verfügung stellen kann, den der Nutzer ausdrücklich wünscht (ausführlicher in § 25 Abs. 2 Nr. 2 TTDSG).

Die Regelung zeigt, dass die Vorgabe nicht nur für Cookies in der bisherigen Form gilt, sondern auch für sogenannte Fingerprints oder zukünftige Tracking-Technologien. § 25 TTDSG gilt dabei unabhängig davon, ob die Dienste personenbezogene Daten enthalten oder damit personenbezogene Daten verarbeitet werden.

Die Zulässigkeit der Verarbeitung personenbezogener Daten regelt das TTDSG nicht. Hierfür und insbesondere für ein Profiling sowie für Analysen gelten die Anforderungen der DSGVO.

Dienste zur Einwilligungsverwaltung

§ 26 TTDSG führt sogenannte Anerkannte Dienste zur Einwilligungsverwaltung und Endnutzereinstellungen ein. Die Idee ist, vereinfacht gesagt, eine vertrauenswürdige Instanz, der die betroffene Person ihre Einwilligungen mitteilt und die diese dann an die Datenverarbeiter „verteilt".

Sanktionen

Der Sanktionsrahmen für Verstöße ist ebenfalls dem TKG entnommen und damit – abweichend von der DSGVO – auf 300.000 € begrenzt. In bestimmten Konstellationen lässt sich der Bußgeldrahmen über Bestimmungen des Ordnungswidrigkeitengesetzes (OWiG) verzehnfachen.

Für Sanktionen wird es in der Praxis dann sehr genau darauf ankommen, ob gemäß § 28 TTDSG gegen eine Regelung des TTDSG oder der DSGVO verstoßen wurde.

Fazit: wenig Neues

Die Gesamtschau zeigt, dass das TTDSG praktisch keine materiellen Regelungen zum Datenschutz oder zu formellen Anforderungen vorsieht. Die Anforderungen an die Verarbeitung personenbezogener Daten durch Anbieter von Telemedien bestimmen sich damit im Kern nach der DSGVO. Damit greift auch für Telemedien anders als nach dem bisherigen TMG-Datenschutz die Interessenabwägungsregelung. In der Praxis neu ist dies nicht wirklich. Denn es hat sich bereits durchgesetzt, dass die DSGVO die TMG-Datenschutzbestimmungen verdrängt. Das zeigt sich z.B. bei der Zulässigkeit von Reichweitenmessungen auf der Grundlage von Art. 6 Abs. 1 Buchst. f DSGVO.

Das TTDSG zeigt wenig Innovationen und schreibt im Wesentlichen bestehende Regelungen fort. Einerseits macht das die kurze Zeitdauer bis zum Anwendungsbeginn handhabbar. Andererseits löst es bestehende Unklarheiten nicht und schreibt sie fort. Es kann schon jetzt als sicher gelten, dass dies Gegenstand von Entscheidungen des Europäischen Gerichtshofs werden wird.

Dr. Jens Eckhardt ist Rechtsanwalt und Fachanwalt für IT-Recht, Datenschutz-Auditor (TÜV) und Compliance Officer (TÜV) bei Derra, Meyer & Partner Rechtsanwälte.

Bild: iStock.com/gorodenkoff

Penetrationstests decken Sicherheitslücken auf, über die externe, aber auch interne Angreifer z.B. Daten abziehen könnten

Sicherheit der Verarbeitung

Penetrationstests: So lässt sich die Sicherheit überprüfen

Angesichts der wachsenden Bedrohung müssen Unternehmen nachhaltige Cyber-Resilienz, also Widerstandsfähigkeit, anstreben, um Angriffe zu verhindern und bei Sicherheitsvorfällen schnell zu reagieren. Dazu eignen sich Sicherheitsaudits, sogenannte Penetrationstests, besonders gut.

Cyberkriminelle nutzen immer noch verstärkt die Situation aus, dass viele Beschäftigte von zu Hause aus arbeiten, um Phishing-Angriffe und Cyberattacken zu platzieren. Die Pandemie hat die Arbeitswelt verändert. Man vernetzt sich mit seinen Arbeitskollegen, arbeitet online und kommuniziert via Chats oder Videokonferenzen. Informationen, Daten und Anwendungen sind dabei über das Internet ständig verfügbar, was ein ortsunabhängiges Arbeiten möglich macht.

Im Fokus: Kollaborationslösungen

Das wissen aber auch Cyberkriminelle. Sie greifen z.B. vermehrt Kollaborationslösungen an, um über Sicherheitslücken Schadsoftware im jeweiligen Unternehmensnetzwerk zu verteilen sowie Informationen und Daten zu stehlen. Häufig verbreiten dabei Phishing-Kampagnen Malware. So versuchen die Angreifer, an sensible persönliche Daten wie Passwörter oder Bankdaten von Internetnutzern zu gelangen. Kommt es hierbei zur Verletzung des Schutzes personenbezogener Daten – etwa wenn Passwörter unbefugt offengelegt wurden – liegt eine meldepflichtige Datenpanne vor.

Forderungen aus dem Datenschutz

Eine Forderung der Datenschutz-Grundverordnung (DSGVO) bezüglich der Sicherheit der Verarbeitung von personenbezogenen Daten ist die erwähnte Resilienz oder Belastbarkeit.

„Belastbar" sind IT-Systeme, wenn sie ausreichend widerstandsfähig sind, um auch bei Störungen oder externen Angriffen wie z.B. einer DDoS-Attacke funktionsfähig zu bleiben. Bei einem DDoS-Angriff (Distributed-Denial-of-Service-Angriff) führen Cyberkriminelle die Nichtverfügbarkeit von bestimmten Diensten oder Servern gezielt herbei. Zudem müssen diese (widerstandsfähigen) Systeme im Hinblick auf die Verarbeitung personenbezogener Daten Vertraulichkeit und Integrität garantieren.

Forderungen aus Sicht der Informationssicherheit

Neben dem Datenschutz misst auch die Informationssicherheit der Resilienz bzw. ihrer Überprüfung große Bedeutung zu. So muss sichergestellt sein, dass das Informationssicherheitsmanagementsystem (ISMS) wirksam bzw. die Informationssicherheit in Verfahren und Prozessen sichergestellt ist. In diesem Zusammenhang fordert die ISO/IEC 27001 neben der „Einhaltung von Sicherheitsrichtlinien und -standards" und der „Überprüfung der Einhaltung von technischen Vorgaben" eine „unabhängige Überprüfung der Informationssicherheit".

Was sind Penetrationstests?

Um den Forderungen des Datenschutzes und der Informationssicherheit gerecht zu werden, eignen sich Sicherheitsaudits, sogenannte Penetrationstests (Pentests), sehr gut. Bei einem solchen Sicherheitstest agieren die Tester mit Erlaubnis des jeweiligen Unternehmens wie Hacker und überprüfen so Firewalls, Serversysteme, Netzwerke, Netzsegmente oder Webanwendungen auf Sicherheitslücken bzw. auf ihre Verwundbarkeit.

Welche Arten von Penetrationstests gibt es?

Innerhalb des Begriffs „Penetrationstests" lässt sich u.a. nach Art, Vorgehensweise und Ausgangspunkt unterscheiden.

Unterscheidung nach Informationsbasis

Ein erstes Unterscheidungskriterium bildet die Informationsbasis, d.h. mit welchem Vorwissen überprüft der Tester das Unternehmen? Hier lassen sich drei Varianten unterscheiden.

Black-Box-Penetrationstest

Bei dieser Variante weiß der beauftragte Pentester nicht, welche IT-Systeme und IT-Infrastruktur ihn beim eigentlichen Test erwarten. Dieses Verfahren beschreibt vielleicht am besten die Bedingungen, die auch einem externen Angreifer, also einem Cyberkriminellen, vorliegen würden.

Nachteil dieses Verfahrens ist das ungünstige Verhältnis zwischen tatsächlichem Erkenntnisgewinn und den Kosten. Beispielsweise kostet es Zeit, die Unternehmens-IP-Adressen und die eingesetzten Software- und Hardwarekomponenten zu ermitteln. Doch generieren diese Informationen keinen (neuen) Erkenntnisgewinn im eigentlichen Sinne.

White-Box-Penetrationstest

Das Gegenteil ist beim White-Box-Penetrationstest der Fall. Hier bekommt der Tester vorab alle Informationen über die IT-Infrastruktur des zu überprüfenden Unternehmens: Welche Server, Betriebssysteme, Dienste und Anwendungen im Einsatz sind; welche Ports offen sind/sein sollten. Darum decken White-Box-Pentests auch Angriffsszenarien ab, die ein Black-Box-Test nicht berücksichtigt – z.B. die Attacke eines gut informierten internen Angreifers aus den Reihen des eigenen Unternehmens. Da der Pentester bei dieser Variante kaum Zeit für die Recherche einsetzen muss, sind White-Box-Tests viel effektiver als Black-Box-Tests.

Grey-Box-Penetrationstest

Den Mittelweg beschreibt das sogenannte Grey-Box-Testverfahren. Hier hat der Penetrationstester bereits einige Informationen über die IT-Infrastruktur. Dieses Verfahren wird dann eingesetzt, wenn zu testende IP-Bereiche festgelegt oder bestimmte Systeme beim Test nicht berücksichtigt werden sollen.

Unterscheidung nach Vorgehensweise

Ein weiteres Unterscheidungskriterium beschreibt die Vorgehensweise. Ist der Test angekündigt oder nicht? Ist der Ausgangspunkt des Tests intern oder extern?

Verdeckte und bekannte Tests

Bei der Vorgehensweise unterscheidet man zunächst zwischen verdeckten und offensichtlichen bzw. bekannten Penetrationstests. Sind also die betreffenden Mitarbeitenden wie die IT-Administration über die Durchführung des Sicherheitstests informiert oder nicht?

Der Vorteil eines verdeckten Tests besteht darin, dass der Dienstleister auch die Informations- bzw. Eskalationsprozesse prüft. Allerdings kann ein solcher Test die IT-Abteilung u.U. in Schwierigkeiten bringen. Sie kann eventuell auf Probleme wie Störungen und Ausfälle bei den IT-Systemen, die der Pentest hervorruft, nicht so schnell reagieren, wie wenn sie eingeweiht worden wäre. Darüber hinaus könnte ein verdeckter Test zu negativer Stimmung bei den Mitarbeitenden führen, weil er gewisse Arbeitsprozesse prüft.

Interner oder externer Test?

Beim Ausgangspunkt des Pentests wird zwischen externen und internen Tests unterschieden. Häufig streben Unternehmen v.a. einen externen Test an, weil sie wissen möchten, ob bzw. wie sicher sie gegen Angriffe von außen sind.

Hat das zu testende Unternehmen aber eine gewisse Größe erreicht – ab etwa 100 bis 200 Mitarbeitern –, gewinnen auch interne Faktoren an Wert. So steigt die Gefahr eines internen Angriffs mit der Mitarbeiteranzahl des Unternehmens.

Fazit: Individuell entscheiden

Abschließend lässt sich sagen, dass Unternehmen bei einem Penetrationstest immer zwischen dem Erkenntnisgewinn, der sich aus dem Test generiert, und dem möglichen Risiko wie Schäden und Ausfällen bei den IT-Systemen abwägen und danach erst entscheiden sollten, welche Vorgehensweise in ihrem Fall die sinnvollste ist.

Markus Vollmuth ist Informationssicherheitsberater bei der atarax Unternehmensgruppe, einem Dienstleister für strategische Unternehmenssicherheit und Haftungsmanagement. Seine Schwerpunkte sind Informationssicherheit und Datenschutz.

Ideal als ganzheitlicher Sicherheitstest

Red Teaming

Da Angriffe oft nicht nur über einen Weg stattfinden, sondern verschiedene Angriffspunkte kombinieren, reicht Cyber-Resilienz allein nicht aus. Möchten Unternehmen einen ganzheitlichen Sicherheitstest durchführen (lassen), sind die Maßnahmen des Red Teamings das Mittel der Wahl. Red Teaming überprüft Sicherheitsstrukturen durch Austesten. Üblicherweise betreffen die Tests

- Technologien bzw. Technik (Pentests),
- Personen (Social Engineering) und
- die physische Sicherheit (physisches Eindringen in die Liegenschaften des Unternehmens).

Mit Methoden des Social Engineering versuchen die Angreifer, Mitarbeiter zwischenmenschlich so zu beeinflussen, dass die angesprochene Person vertrauliche Informationen wie Passwörter herausgibt. Diese Methode ist auch sehr beliebt, um in einem zweiten Schritt z.B. Schadsoftware auf die Firmenrechner zu spielen.

Bild: iStock.com/Prostock-Studio

Sprechen Sie mit der IT-Leitung oder IT-Administration nicht nur über die seit Langem bekannten DNS-Risiken, sondern insbesondere über die Sicherheitserweiterungen

ODoH: Besserer Schutz für DNS

Gegen die Ausspähung im Domain Name System (DNS)

Das DNS ist das „Telefonbuch" für das Internet und daher im Fokus von Hackern und Datendieben. Der neue Standard ODoH (Oblivious DNS over HTTPS) will den Datenschutz bei der DNS-Nutzung erhöhen. Um davon zu profitieren, raten Sie im Unternehmen, aktiv zu werden.

Möchten Sie eine bestimmte Website aufrufen, kennen Sie entweder die Webadresse oder Sie nutzen eine Suchmaschine. Was Sie sicherlich nicht wissen, ist die IP-Adresse des Webservers, der die Website vorhält.

Der Wegweiser im Internet

Damit sich der Browser mit dem Webserver verbindet, braucht er jedoch diese IP-Adresse. Denn eine Webadresse wie www.datenschutz-praxis.de ist eine für uns Menschen gemachte, verständliche Adresse. Die IP-Adresse jedoch ist die Adresse des Webservers im Internet, die technisch nötig ist. Deshalb führt Ihre Eingabe der Webadresse im Browser zu einer Abfrage im Domain Name System (DNS). Es kennt die Zuordnung zwischen Webadressen und IP-Adressen.

Das DNS ist also wie ein Telefonbuch zu verstehen. Ohne DNS wird eine Webadresse nicht in die IP-Adresse übersetzt.

DNS-Risiken: fehlende Erreichbarkeit, Entführung, Spionage

Das DNS nutzt bestimmte Server, die DNS-Server, um die „Telefonbuch-Dienste" für das Internet zu erbringen. Werden diese Server blockiert oder fallen sie durch eine gezielte Überlastung aus (DDoS-Attacken), kann das DNS die IP-Adressen zu den Webadressen nicht mehr liefern, die Webseiten sind nicht erreichbar. Die Folge aus Datenschutzsicht: mangelnde Verfügbarkeit und Belastbarkeit nach der Datenschutz-Grundverordnung (DSGVO).

Manipulieren Angreifer die DNS-Abfragen oder die DNS-Server, werden gezielt die falschen IP-Adressen zu den gewünschten Webadressen geliefert (mangelnde Integrität nach DSGVO). Hacker können so die Aufrufe von Webseiten umlenken und die Opfer zu verseuchten, manipulierten Seiten führen, um z.B. Phishing bei Kunden einer Online-Bank zu starten.

Die zentrale Stellung des DNS macht noch eine weitere Attacke möglich: Angreifer könnten genau nachverfolgen, welche Webadressen ein bestimmtes Unternehmen oder ein bestimmter Nutzer aufruft. Sie können also die Ziele des Datenverkehrs im Internet „abhören" (mangelnde Vertraulichkeit nach DSGVO).

Bestehende Sicherheitserweiterungen für das DNS

Nun sind die Sicherheitsrisiken im DNS nicht neu. Es gibt bereits mehrere Ansätze, um für mehr DNS-Sicherheit zu sorgen. Aber bislang haben die Bemühungen noch keinen ausreichenden Erfolg.

Die Gründe dafür sind einfach: Nur wenn alle beteiligten Stellen ihre DNS-Implementierung erweitern, lässt sich ein sicherer DNS-Kanal aufbauen. Gefordert sind neben den Betreibern der DNS-Server die Internetprovider, die Browserhersteller, die Betriebssystemhersteller und nicht zuletzt die Nutzerinnen und Nutzer.

DNSSEC: Prüfung der Echtheit

DNSSEC erweitert das DNS um eine zusätzliche Sicherheitsebene, indem es kryptografische Signaturen zu bestehenden DNS-Einträgen ergänzt. Die digitalen Signaturen speichern die DNS-Server zusätzlich zu üblichen Einträgen. Eine Überprüfung der zugehörigen Signatur verifiziert, ob ein angefragter DNS-Eintrag von seinem autorisierenden Nameserver stammt und unterwegs nicht verändert wurde. Damit lassen sich gefälschte Einträge erkennen, die Webseiten-Aufrufe umlenken, um den Nutzer z.B. auf eine Phishing-Seite zu locken.

DoH & DoT: Verschlüsselung

Eine wesentliche Schwachstelle im Konzept des DNS ist, dass die Anfragen an die

DNS-Server, wie die IP-Adresse zu einer bestimmten Webadresse lautet, ebenso im Klartext gesendet werden wie die Antworten des Servers an den Client, also z.B. an den Browser des Nutzers.

Damit unbefugte Dritte diese Nachrichtenströme nicht auswerten können, bietet sich Verschlüsselung an: DNS over HTTPS (DoH) und DNS over TLS (DoT). Wie bei Verschlüsselung üblich müssen Absender und Empfänger damit arbeiten. Die Zahl der Unterstützer wächst derzeit zwar, doch die Durchdringung muss weiter gehen.

Ein weiteres Problem: Der Datenschutz durch Verschlüsselung hat Grenzen. Denn um die Anfrage zu bearbeiten und eine Antwort an den Client zu senden, entschlüsselt der „Übersetzer Webadresse – IP-Adresse" die DNS-Anfragen. An dieser Stelle sind alle IP-Adressen (Webadressen) bekannt, die eine bestimmte IP-Adresse (also der Nutzer) aufgerufen hat. Entsprechend muss der Datenschutz beim Betreiber des DNS-Dienstes angemessen und vertrauenswürdig sein. Doch lässt sich der Datenschutz noch weiter verbessern. Und zwar mit einem neuen Ansatz: Oblivious DNS over HTTPS (ODoH).

Neu: Mehr Datenschutz durch ODoH

ODoH ergänzt die Verschlüsselung durch einen Proxy-Server-Ansatz. Wie bei einem Proxy-Ansatz üblich wird ein weiterer „Partner" in den Nachrichtenfluss eingebracht, der den echten Sender – also den Nutzer, der eine Webadresse aufruft – verbirgt und selbst als Sender gegenüber dem DNS-Server auftritt. Der Proxy-Server kennt zwar den echten Sender, kann aber die DNS-Abfrage nicht lesen, da sie verschlüsselt ist. Der DNS-Server kann die Anfrage entschlüsseln, sieht aber den echten Absender (den Nutzer) nicht.

Es versteht sich, dass der Proxy- und der DNS-Server strikt getrennt sein müssen, also nicht etwa den gleichen Betreiber haben dürfen. Angreifer müssten also sowohl den Proxy- als auch den DNS-Server erfolgreich attackieren, um die Datenströme ausspähen und das Internetverhalten des Nutzers nachvollziehen zu können.

Open-Source-Lösungen für Tests

Zu ODoH gibt es Open-Source-Lösungen, die einen Test der Sicherheitserweiterungen erlauben:

- https://github.com/cloudflare/odoh-client-rs/
- https://github.com/cloudflare/odoh-client-go/

Außerdem bietet Cloudflare eine App, die die DNS-Datenströme absichern will (https://1.1.1.1/). Unter anderem lässt sich die App unter Windows nutzen (https://developers.cloudflare.com/warp-client/setting-up/windows). Die Wirtschaftsprüfungsgesellschaft KPMG hat bereits ihre Datenschutzeigenschaften untersucht (siehe https://ogy.de/KPMG-Cloudflare).

Weitere Prüfungen durch die Datenschutz-Gemeinde sind wünschenswert, ebenso eine umfassende Umsetzung von mehr DNS-Sicherheit, die bereits seit Jahren gefordert wird und nun einen weiteren Baustein erhalten hat.

ONLINE-TIPP

Unternehmen und öffentliche Stellen müssen DNS-Server umfassend gegen Angriffe schützen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat dazu einen Baustein im IT-Grundschutz-Kompendium veröffentlicht. Es beschreibt neben den Risiken auch die Schutzmaßnahmen, die das BSI empfiehlt. Der Baustein ist zu finden unter https://ogy.de/BSI-DNS.
Wer sich einen Überblick über bestehende DNS-Risiken und -Schwachstellen verschaffen möchte, findet bei CERT-Bund eine jeweils aktuelle Übersicht unter https://ogy.de/DNS-Schwachstellen.

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

IMPRESSUM

Verlag:
WEKA MEDIA GmbH & Co. KG
Römerstraße 4, 86438 Kissing
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-74 00
Website: www.weka.de

Herausgeber:
WEKA MEDIA GmbH & Co. KG
Gesellschafter der WEKA MEDIA GmbH & Co. KG sind als Kommanditistin:
WEKA Business Information GmbH & Co. KG und als Komplementärin:
WEKA MEDIA Beteiligungs-GmbH

Geschäftsführer:
Stephan Behrens, Michael Bruns, Kurt Skupin

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

Anzeigen:
Anton Sigllechner
Telefon: 0 82 33.23-72 68
Fax: 082 33.23-5 72 68
E-Mail: anton.sigllechner@weka.de

Erscheinungsweise:
Zwölfmal pro Jahr

Aboverwaltung:
Telefon: 0 82 33.23-40 00
Fax: 0 82 33.23-740
E-Mail: service@weka.de

Abonnementpreis:
12 Ausgaben 232,00 €
(zzgl. MwSt. und Versandkosten)
Einzelheft 22 €
(zzgl. MwSt. und Versandkosten)

Druck:
Geiselmann Printkommunikation GmbH
Leonhardstraße 23, 88471 Laupheim

Layout & Satz:
METAMEDIEN
Spitzstraße 31, 89331 Burgau

Bestell-Nr.:
09100-4091

ISSN-Nr.:
1614-6867

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

Datensicherheit

Wenn der Chef das Unternehmen abschießt

USB-Sticks, auf denen sich Schadsoftware versteckt, sind ein klassisches Einfallstor für Cyberkriminelle. Testen Sie doch mal, wie gut die letzten Schulungen zu diesem Thema gewirkt haben …

Ein Weg, den Schadsoftware nutzt, um sich auf Systemen zu manifestieren, sind verseuchte USB-Sticks. Um zu verhindern, dass Beschäftigte sie nutzen, gibt es grundsätzlich zwei Wege:

- Der technische Weg verhindert alle nicht zugelassenen USB-Sticks.
- Der organisatorische Weg verbietet, andere als die zugelassenen USB-Sticks zu nutzen.

Schulen ist gut, …

Den zweiten Weg sollten Verantwortliche jedoch nur gehen, wenn sie absolut nicht darauf verzichten können, solche USB-Sticks zu nutzen. In diesem Fall heißt es, die beschäftigten Personen in Schulungen und durch Datenschutzrichtlinien zu verpflichten, nur zugelassene USB-Sticks zu verwenden.

Testen ist besser.

Test in einem Unternehmen. Der Datenschutzbeauftragte vereinbart mit dem Geschäftsführer, auf dem Betriebsgelände insgesamt zwölf präparierte USB-Sticks zu „verlieren". Für den Fall, dass jemand einen solchen Stick findet und am dienstlichen Rechner einsteckt, erhält der Administrator eine Meldung, von wo aus das passiert ist. Ansonsten geschieht, anders als bei einer echten Schadsoftware, nichts.

Verführerische USB-Sticks

Die Sticks waren attraktiv beschriftet. Da war zu lesen: „Beförderungsliste" oder „Fotos von der Feier Betriebsrat" und „Fotos Abele" (angenommen, der Geschäftsführer hieß Abele und war über diese Aktion in Kenntnis gesetzt). Von den zwölf verteilten USB-Sticks steckten die Beschäftigten trotz intensiver Schulung und trotz unterschriebener Datenschutzrichtlinie, keine gefundenen Datenträger zu verwenden, elf in ihre Dienstrechner. Der zwölfte ist bis heute nicht mehr aufgetaucht.

Bemerkenswert war, dass ein wohlmeinender Mitarbeiter den Stick „Fotos Abele" zum – über die Aktion informierten! – Chef brachte, dieser bass erstaunt war, wie auf diesen Stick Fotos von ihm kämen – und dann den USB-Stick selbst an seinem Rechner ausprobierte. Im Ernstfall hätte damit der Chef das Unternehmen höchstpersönlich „abgeschossen". Merke: Schulen ist gut, Testen ist besser.

Eberhard Häcker ist seit vielen Jahren selbstständig mit Schwerpunkt Datenschutzberatung. Als externer DSB hat er schon viel erlebt und weiß: „Es gibt nichts, was es nicht gibt."

IN DER NÄCHSTEN AUSGABE

Abmahnungen bei Datenschutzverstößen

Welche Risiken ergeben sich aktuell aus der wettbewerbsrechtlichen Abmahnung?

Tätigkeitsberichte im Überblick

Lesen Sie, womit sich die Datenschutzaufsichtsbehörden im letzten Jahr schwerpunktmäßig beschäftigt haben.

Zoom aus deutschen Rechenzentren

Mit dem Meeting Connector können Organisationen eigene Zoom-Server hosten.