www.datenschutz-praxis.de

WEKA

Datenschutz PRAXIS

RECHTSSICHER | VOLLSTÄNDIG | DAUERHAFT | Juli 2017

Foto: iStock.com/Warchi

Wer die Hinweise der Art.-29-Gruppe zur Umsetzung berücksichtigt, ist bestens vorbereitet

Working Paper der Art.-29-Gruppe

Datenübertragbarkeit praktisch umsetzen

Das Recht auf Datenübertragbarkeit ist gewissermaßen eine Mogelpackung: Außen steht zwar Datenschutz drauf, aber innen verbirgt sich eine verbraucher- und wettbewerbsrechtliche Regelung.

Eines der neuen Instrumente der Datenschutz-Grundverordnung (DSGVO) ist das Recht auf Datenübertragbarkeit. Es soll dem Betroffenen eine bessere Kontrolle über seine Daten bieten. Dahinter steckt der Gedanke, dass der Betroffene mit seinen Daten ohne großen Aufwand zu einem anderen Anbieter „umziehen" kann. Und das soll wiederum den Wettbewerb um datenschutzfreundliche Produkte und Dienstleistungen stärken.

Die Datenmenge verdoppelt sich

Dieser Ansatz ist zwar löblich, hat aber mit dem Schutz der Rechte und Freiheiten der Betroffenen wenig zu tun. Ganz im Gegenteil – die Menge an schützenswerten Daten verdoppelt sich und somit auch das Risiko für die Betroffenen. Trotzdem sind die Verantwortlichen verpflichtet, ab Mai 2018 auf Verlangen die Portabilität der Daten zu gewährleisten.

Nicht nur soziale Netzwerke ...

Im Gesetzgebungsverfahren standen zunächst die sozialen Netzwerke im Fokus. Doch damit nicht genug. Das Recht auf Datenübertragbarkeit kommt bei unzähligen Datenverarbeitungen in Betracht. Zu denken ist dabei z.B. an einen „Datenumzug" beim Kontowechsel, beim Kauf eines neuen Fitness-Armbands oder beim Abschluss eines neuen Leasingvertrags.

WICHTIG

Bevor es an die Umsetzung geht, werfen Sie einen genauen Blick in die DSGVO. Denn der Betroffene kann nicht in jedem Fall seine Daten herausverlangen. Erst wenn alle Voraussetzungen des Art. 20 DSGVO erfüllt sind, muss der Verantwortliche dem Betroffenen die Daten bereitstellen oder direkt an einen anderen Verantwortlichen übermitteln.

Verantwortliche sollten sich daher zunächst klar werden, bei welchen Verarbeitungsvorgängen überhaupt ein Recht auf Datenübertragbarkeit in Betracht kommt. Die einzelnen Voraussetzungen des Art. 20 DSGVO schließen bereits viele Prozesse aus. Die Voraussetzungen lassen sich einfach prüfen, indem Sie in das bereits →

Editorial

Ricarda Veidt,
Chefredakteurin

Schönheits-Operation

Um Sie noch besser als bisher bei Ihren vielfältigen Aufgaben als Datenschutzbeauftragter zu unterstützen, hat die Datenschutz PRAXIS ein neues Gesicht bekommen. Das neue Layout und die neue Art, Texte aufzubereiten, erleichtern es Ihnen, das Wichtigste auf einen Blick zu erfassen. Mit den Rubriken bilden wir die Anforderungen der Grundverordnung an den DSB ab, wie sie Art. 39 DSGVO formuliert: Er soll „zumindest" beraten und überwachen. Schulen und sensibilisieren muss er zwar nicht mehr direkt selbst. Aber er muss auch das „überwachen" – und in der Praxis wahrscheinlich letztlich doch höchstpersönlich übernehmen.

Das heißt natürlich nicht, dass die Inhalte nur auf die Zukunft gerichtet sind. Immerhin gilt das alte Bundesdatenschutzgesetz noch eine ganze Weile. In guter Tradition kommt die Unterhaltung auf der letzten Seite nicht zu kurz: Der „Daten-Schluss" stellt komische und skurrile (aber wahre!) Fälle aus der Praxis vor.

Ich hoffe, die Operation ist auch in Ihren Augen gelungen. Geben Sie mir gern Rückmeldung unter ricarda.veidt@weka.de.

Herzlichst Ihre Ricarda Veidt

vorhandene Verfahrensverzeichnis nach dem Bundesdatenschutzgesetz (BDSG) oder – noch besser – in das Verzeichnis über Verarbeitungstätigkeiten nach der DSGVO blicken. Wer sich hier nicht genau an den Wortlaut des Art. 20 hält, macht sich im Zweifel mehr Arbeit als nötig.

Technische Umsetzung

Eine weitere Anforderung ergibt sich nicht direkt aus Art. 20 DSGVO, sondern aus den allgemeinen Regelungen über die Betroffenenrechte (Art. 12 DSGVO). Dazu gehört, dass sich der Verantwortliche von der Identität desjenigen überzeugen muss, der das Recht geltend macht. Unterläuft hier ein Fehler oder verzichtet man aus Nachlässigkeit auf eine Identitätsfeststellung und stellt die Daten einem Dritten bereit, liegt immer eine meldepflichtige Datenpanne vor.

PRAXIS-TIPP

Verantwortliche sollten nicht erst bei begründeten Zweifeln, sondern in jedem Fall die Identität des Betroffenen prüfen. Denn das Recht auf Datenübertragbarkeit kann zum Einfallstor für Identitätsdiebstahl werden.

Das lässt sich leicht vermeiden. Bei vielen Online-Diensten hat der Nutzer für sein Kundenkonto bereits einen Benutzernamen und ein Passwort. Hat sich der Nutzer beim Login damit legitimiert, können seine Daten innerhalb des Kundenkontos zum Download bereitgestellt werden. Das Gleiche gilt, wenn der Betroffene die direkte Übermittlung an einen anderen Verantwortlichen fordert. Dass diese Übermittlung nur verschlüsselt erfolgen darf, versteht sich von selbst.

Wie sollen die Daten bereitgestellt werden?

Die Daten sollen in einem strukturierten, gängigen und maschinenlesbaren Format übermittelt werden. Das ist im Allgemeinen keine besondere Hürde. Fachverbände müssen also nicht zwingend interoperable Standards oder Formate entwickeln. Die gängigen Formate für Datenbanken genügen in der Regel diesen Voraussetzungen. Wer also die Daten in den Formaten XML oder CSV übermittelt, erfüllt die Anforderungen in den meisten Fällen.

Foto: iStock.com/Anatolii Babii

Ein „Datenumzug" wird nicht nur, aber häufig soziale Netzwerke betreffen

Was ist, wenn sich die Daten auf andere Personen beziehen?

Personenbezogene Daten betreffen oftmals auch Daten anderer Personen. Das gilt beispielweise für das Bankkonto, das Angaben über denjenigen enthält, an den Geld überwiesen wurde, oder für das E-Mail-Konto, in dem die Kontaktdaten der Absender und Empfänger zu finden sind.

Dies führt aber nicht dazu, dass der Verantwortliche die Bereitstellung der Daten verweigern kann. Vielmehr ist der andere Verantwortliche, der die Daten übermit-

telt bekommt, verpflichtet, die Daten nur für solche Zwecke zu verarbeiten, die die Rechte und Freiheiten der anderen Personen nicht beeinträchtigen.

Verhältnis zu anderen Betroffenenrechten

Das Recht auf Datenübertragung steht neben weiteren Betroffenenrechten. Verlangt der Betroffene, dass seine Daten bereitgestellt werden, bedeutet das nicht ohne Weiteres, dass seine Daten zu löschen sind oder er das Vertragsverhältnis beenden möchte. Es ersetzt auch nicht das Recht auf Auskunft, sondern ergänzt den Katalog an Betroffenenrechten.

ONLINE-TIPP

Das Working Paper der Artikel-29-Gruppe finden Sie unter http://ogy.de/workingpaper-242 (PDF).

Was ist noch zu beachten?

Der Verantwortliche muss die Daten unentgeltlich bereitstellen (Art. 12 Abs. 5 Satz 1 DSGVO). Außerdem muss er unverzüglich, spätestens jedoch innerhalb eines Monats tätig werden. Auch das macht klar, dass Verantwortliche unbedingt von Anfang an bei der Produktentwicklung eine Funktion zur Datenübertragung berücksichtigen sollten. Denn nur so lässt sich fristgerecht auf Anfragen der Betroffenen reagieren.

Fazit: Nicht auf manuelles Abarbeiten setzen!

Das neue Instrument stellt die Verantwortlichen vor keine leichte Aufgabe. Anders als bei anderen Betroffenenrechten wie der Auskunft oder dem Recht auf Löschung spielt die technische Umsetzung die entscheidende Rolle. Wer hier glaubt, dass er wenige Anfragen im Jahr schon irgendwie manuell bewältigen kann, der täuscht sich gewaltig. Die Möglichkeit, die Daten zu übertragen, sollte frühestmöglich im Prozess implementiert werden, um den hohen Anforderungen der Datenschutz-Grundverordnung zu genügen.

Genau hinschauen lohnt sich

Wann greift das Recht auf Datenportabilität überhaupt?

Welche Voraussetzungen müssen erfüllt sein, damit der Verantwortliche die Daten bereitstellen oder an einen anderen Verantwortlichen übermitteln muss?

1. Vom Betroffenen bereitgestellt

Von zentraler Bedeutung ist die Voraussetzung, dass der Betroffene die Daten direkt bereitgestellt haben muss. Das ist in erster Linie dann der Fall, wenn der Betroffene die Daten bewusst offenlegt, indem er sie dem Verantwortlichen übermittelt oder durch sonstige Weise verbreitet hat. Dazu zählen beispielsweise das Erstellen eines Profils in einem Dating-Portal oder das Ausfüllen von Bestellformularen und Vertragsunterlagen. Für die Praxis bedeutet das: Hier sind v.a. die Stammdaten des Kunden gemeint. Vom Betroffenen bereitgestellt sind aber auch solche Daten, die ein Dienst bei der Nutzung automatisch erzeugt. Als Orientierung kann hier der noch geltende § 15 Telemediengesetz (TMG) dienen:

- So gehören Standortdaten, Suchhistorien oder Log-Files zu den Daten, die der Betroffene bereitstellt.
- Nicht zu vergessen sind Daten des Fitness-Trackers oder der Black-Box im KfZ bei Telematik-Versicherungstarifen.

Fitness-Tracker-Daten stellt der Betroffene selbst dem Anbieter zur Verfügung

Nicht darunter fallen solche Daten, die erst die Datenverarbeitung als solche erzeugt und die auf Rückschlüssen des Verantwortlichen beruhen. Das bedeutet im Klartext, dass Bonitätsbewertungen oder die Zuordnung von Interessen oder Merkmalen, also das klassische Profiling, nicht darunter fallen.

2. Vertrag oder Einwilligung erlauben die Verarbeitung

Auch die nächste Voraussetzung schränkt das Recht unter Umständen erheblich ein: Das Recht auf Datenportabilität umfasst nur solche Daten, die aufgrund eines Vertrags oder einer Einwilligung des Betroffenen verarbeitet werden dürfen. Häufig wird jedoch die Datenverarbeitung aufgrund der Interessenabwägung legitimiert sein, sodass diese Daten nicht darunterfallen.

Außerdem gilt: Um zu erkennen, dass es im Grunde um eine verbraucher- und wettbewerbsrechtliche Regelung geht, dürfen die Verantwortlichen ausnahmsweise die „Datenschutz-Brille" abnehmen. Denn nur so kann man die Anforderungen des neuen Instruments besser verstehen und rechtskonform umsetzen. Unerlässlich dabei ist auch ein Blick in das Working Paper 242 der Art.-29-Gruppe.

Kristin Benedikt ist Referatsleiterin für die Themen Internet, Telemedien und Apps beim Bayerischen Landesamt für Datenschutzaufsicht.

Foto: yacobchuk/iStock/Thinkstock

Foto: grinvalds/iStock/Thinkstock

Jeder fünfte Internetnutzer ist bereits Opfer von Online-Betrug geworden. Trotzdem glaubt die Mehrheit, gefälschte Online-Shops erkennen zu können.

Schutz vor Online-Betrug

So erkennt man Fake-Shops

Bei Fake-Shops bezahlen Kunden, erhalten jedoch keine Ware oder gefälschte Produkte. Zusätzlich besteht die Gefahr, dass Kundendaten anderweitig missbraucht werden. Wie lassen sich Fake-Shops entlarven?

Der Online-Betrug kann viele Gesichter haben, wenn Internetnutzer bei einem Webshop bestellen:

- Der Online-Shop ist gefälscht und ahmt einen bekannten Webshop nach, in der Internetadresse und/oder im Erscheinungsbild und Logo. Die angebotenen und ggf. gelieferten Waren sind ebenfalls Fälschungen oder Hehlerware.
- Der Online-Shop ist nicht gefälscht, aber die Waren sind Fälschungen oder stammen aus Diebesgut.
- Ein echter, seriöser Online-Shop wurde gehackt und manipuliert. Die Produktinformationen sind gefälscht, die Kundendaten werden gestohlen, und/oder die IT-Systeme der Kunden werden mit Malware verseucht.
- Auf einem echten, seriösen Online-Marktplatz treten Online-Betrüger als Händler auf. Sie imitieren einen seriösen Anbieter, handeln mit gefälschten oder gestohlenen Waren, oder aber das Benutzerkonto eines echten Anbieters auf dem Marktplatz wurde durch Hacking übernommen.

Betroffen sein können nicht nur private Online-Shopper, sondern auch die Einkaufsabteilung oder andere Beschäftigte, die eine Beschaffung für das Unternehmen machen. Daher ist das Thema durchaus für eine Datenschutzschulung oder eine Mitarbeiterinformation wichtig.

Datenmissbrauch statt Warenlieferung

Für den Datenschutz spielt es eine besondere Rolle, was mit den Kundendaten geschieht. Gerade bei der scheinbar bequemen Möglichkeit, sich einmal zu registrieren, um später schnell und einfach bestellen zu können, drohen große Datenrisiken. Sowohl die Bestell- und Lieferanschrift als auch die Zahlungsinformationen können an Dritte verkauft oder anderweitig missbraucht werden. Außerdem geben viele Nutzer im Kundenprofil weitaus mehr Daten an, als es für die Bestellung an sich erforderlich wäre, um dadurch z.B. passendere und bessere Angebote zu bekommen.

Wie bei vielen anderen Online-Diensten ist es leider nicht unwahrscheinlich, dass der Nutzer für sein Kundenkonto sein „Allzweck-Passwort" nutzt und kein neues Passwort vergibt. Entsprechend kann es zu einem Passwortdiebstahl und -missbrauch kommen, ganz ohne Keylogger, also eine Hard- oder Software, die die Eingaben des Benutzers an der Tastatur protokolliert. Online-Shops lassen sich somit auch für Phishing-Attacken nutzen.

Internetnutzer fühlen sich (zu) sicher

Trotz der Vielfalt an Online-Betrugsmöglichkeiten und der hohen Datenrisiken glauben erstaunlich viele Internetnutzer, gefälschte Online-Shops zu erkennen: Die Mehrheit der Deutschen traut sich zu, seriöse von unseriösen Online-Händlern zu unterscheiden, so Bitkom. Drei von vier Online-Einkäu-

Aufschlussreiche Zahlen

Online-Shopping ist zum Massenphänomen geworden. Laut einer Umfrage des Bitkom-Verbands kaufen vier Prozent der Nutzer täglich im Internet ein, jeweils 14 Prozent shoppen einmal oder mehrmals pro Woche online, knapp die Hälfte (47 Prozent) mehrmals pro Monat. Entsprechend hoch ist das Angebot an Online-Shops: Gut jedes dritte Unternehmen (36 Prozent) betreibt einen unternehmenseigenen Webshop. Jedes vierte Unternehmen bietet seine Produkte oder Dienste auf Online-Marktplätzen oder digitalen Plattformen wie Ebay, Amazon, Alibaba oder Mercateo an.

Mitarbeiterinformation

Fake-Shops und Online-Betrüger erkennen

Wie Umfragen zeigen, glauben viele Internetnutzer, seriöse und unseriöse Online-Shops unterscheiden zu können. Doch Vorsicht: Fake-Shops sind inzwischen sehr professionell gemacht. Mitunter sind die betrügerischen Angebote exakte Kopien seriöser Webshops, oder Angreifer hacken echte Online-Shops.

Online-Betrug bei Webshops kann sehr vielfältig sein, achten Sie daher auf die entscheidenden Details. Nur ein Blick ins Impressum reicht nicht. So kann Ihnen z.B. Folgendes unterkommen:

- Der Online-Shop nutzt ohne Berechtigung ein bekanntes (!) Gütesiegel: Ob das Gütesiegel echt ist, prüfen Sie in der Zertifikatsliste der genannten Gütesiegel-Stelle. Dazu nutzen Sie nicht den Link, den der Shop für das Gütesiegel nennt, sondern suchen die Gütesiegel-Webseite direkt auf. Hilfe bietet auch die Seite http://internet-guetesiegel.de.
- Der an sich seriöse Online-Shop wurde manipuliert und enthält Inhalte krimineller Dritter: Webbrowser zeigen an, wie sich die Webseiten-Inhalte zusammensetzen und ob es ein legitimes Digitales Zertifikat gibt (Firefox-Funktion: Extras > Seiteninformationen)
- Der Anbieter verlangt grundsätzlich Vorkasse: Nutzen Sie stattdessen Kauf auf Rechnung, bekannte Bezahldienste – oder gleich einen anderen Online-Shop.
- Der Shop nutzt eine Internetadresse, die nach einer bekannten Marke aussieht: Prüfen Sie unter https://www.denic.de/webwhois/ den Inhaber der Domain.

Das BSI schätzt, dass mindestens 1.000 deutsche Online-Shops manipuliert sind

Foto: Ridofranz/iStock/Thinkstock

fern (73 Prozent) geben an, Fake-Shops im E-Commerce entlarven zu können. Spannend ist, woran die Internetnutzer unseriöse Online-Shops erkennen wollen:

- an der Auswahl an Bezahlmöglichkeiten (71 Prozent)
- an den Versand- und Rückversandkonditionen (67 Prozent)
- an den Online-Bewertungen anderer Käufer (63 Prozent)
- am Ruf des Händlers (63 Prozent)
- an Gütesiegeln (58 Prozent)
- an Empfehlungen von Familie und Freunden (45 Prozent)
- an der Qualität der Produktpräsentation auf der Homepage (42 Prozent)

Jeder Zweite (47 Prozent) schaut laut Umfrage auf das Impressum. Deutlich weniger sehen sich die Datenschutzerklärung an (37 Prozent).

Online-Betrüger werden unterschätzt

Die zuvor genannten Kriterien sind leider zum großen Teil unzuverlässig. Die Online-Betrüger werden also unterschätzt. So können Online-Betrüger durchaus

- bekannte Bezahlmöglichkeiten vortäuschen,
- gute Versand- und Rückversandkonditionen nennen,
- Online-Bewertungen anderer Käufer fälschen, insbesondere auf den eigenen Shop-Seiten,
- den Ruf eines ehrlichen Händlers missbrauchen,
- unerlaubt das Logo eines Gütesiegels auf ihrem Online-Shop einfügen,
- bei Familie und Freunden bekannt sein,
- tolle Produktpräsentationen auf der Homepage haben sowie
- das Impressum und die Datenschutzerklärung fälschen.

Auch zahlreiche deutsche Anbieter betroffen

Machen Sie als Datenschutzbeauftragte oder Datenschutzbeauftragter Fake-Shops zum Thema Ihrer Datenschutzunterweisung. Auch deshalb, weil z.B. das BSI (Bundesamt für Sicherheit in der Informationstechnik) eindrücklich davor warnt, dass mindestens 1.000 deutsche Online-Shops von Online-Skimming betroffen sind. Dabei nutzen Cyber-Kriminelle Sicherheitslücken in veralteten Versionen der Shop-Software, um schädlichen Programmcode einzuschleusen. Dieser späht dann beim Bestellvorgang die Zahlungsinformationen der Kunden aus und übermittelt sie an die Täter.

Internetnutzer besser aufklären

Gegen diese Gefahr helfen die in der Umfrage genannten Kriterien nicht. Denn die Angreifer missbrauchen seriöse Online-Shops und machen sie zu einem Fall von Online-Betrug. Nutzen Sie deshalb die Mitarbeiterinformation zur Aufklärung über die verschiedenen Varianten von Fake-Shops und über die Anzeichen, auf die man als Nutzer achten sollte.

Oliver Schonschek, Dipl.-Physiker, ist IT-Fachjournalist und Technology Analyst (Insider Research). Er gehört zu den Sprechern auf der IDACON 2017 und untersucht insbesondere, wie sich neue Technologien auf den Datenschutz auswirken.

Foto: Ralwel/iStock/Thinkstock

Gerade bei größeren Rechenzentren kann es reichen, die vorhandenen Zertifikate unter die Lupe zu nehmen

Datenschutzkontrolle

Wie prüfen Sie ein Rechenzentrum?

Ein Datenschutzbeauftragter kann immer wieder vor der Aufgabe stehen, ein Rechenzentrum zu prüfen. Sehr häufig geht es um eine Kontrolle bei einem externen Auftragsverarbeiter. Wie gehen Sie die Prüfung am besten an?

Der Beitrag ...

... stellt zunächst die wesentlichen Anforderungen an ein Audit dar, um anschließend auf ein praxiserprobtes Vorgehensmodell zur Prüfung einzugehen. Der Schlussteil fasst die wesentlichen Empfehlungen kurz zusammen. Nachfolgend wird die Prüfung eines Rechenzentrums hinsichtlich der Datenschutzanforderungen „Datenschutzaudit" oder kurz „Audit" genannt.

Typischerweise besteht ein Rechenzentrum, neben einer Vielzahl von Servern, Netzwerkkomponenten und sonstigen Systemen, aus infrastrukturellen Komponenten wie Energieversorgung und Klimatechnik sowie baulichen Aspekten wie Räumen oder Türen. Für eine Prüfung ist neben der Fachkenntnis im Datenschutz also auch die Kenntnis der technischen und physikalischen Beschaffenheit von Vorteil.

Übersicht über die wesentlichen Anforderungen

Die Anforderungen für Datensicherheitsmaßnahmen ergeben sich insbesondere aus den technischen und organisatorischen Maßnahmen (TOMs) gemäß der Anlage zu § 9 Satz 1 BDSG. Die dort definierten Sicherheitsziele bieten einen ersten Ansatz für konkrete Auditanforderungen. Mit der DSGVO bleiben diese Sicherheitsziele weitestgehend erhalten, auch wenn sich die Begrifflichkeiten und die Struktur geändert haben (vgl. Art. 32 DSGVO; lesen Sie zu den TOMs ausführlicher den Beitrag auf den Seiten 13 und 14).

Ziehen Sie ergänzend dazu spezifische Sicherheitsanforderungen aus gängigen Standards der Informationssicherheit heran, wie z.B. aus der ISO/IEC 27001 ff. oder aus den IT-Grundschutzkatalogen des Bundesamts für Sicherheit in der Informationstechnik (BSI). Letztere behandeln konkrete bausteinbasierte Sicherheitsmaßnahmen. Folgende Themen aus den IT-Grundschutzkatalogen lassen sich z.B. direkt mit einigen TOMs abdecken:

- **Allgemeine datenschutzrechtliche Anforderungen:**
  Baustein 1.5 Datenschutz
- **Zutritts- und Zugangskontrolle:**
  Baustein 1.1 Organisation
- **Zugangs- und Zugriffskontrolle:**
  Baustein 1.18 Identitäts- und Berechtigungsmanagement

- **Verfügbarkeitskontrolle:**
  Baustein 1.3 Notfallmanagement
- **Physische und umgebungsbezogene Sicherheitsmaßnahmen:**
  Baustein 2.1 Allgemeines Gebäude
  Baustein 2.4 Serverraum
  Baustein 2.9 Rechenzentrum

Praxiserprobte Vorgehensweise

Auch die vorgestellte Vorgehensweise zur Auditierung eines Rechenzentrums richtet sich an den Methoden und Empfehlungen des BSI aus. Das Vorgehen besteht aus drei Phasen:

1. Vorbereitung: Dokumentensichtung und Feinplanung
2. Durchführung: Verifikation der Umsetzung durch Vor-Ort-Kontrolle
3. Nachbereitung: Erstellung eines Auditberichts und Maßnahmenumsetzungs-Planung

Phase 1: Vorbereitung

1. Schritt: Ansprechpartner feststellen

Ziel der ersten Phase eines Datenschutzaudits ist es, sich einen Überblick über den derzeitigen Stand der umgesetzten datenschutzrechtlichen Anforderungen zu verschaffen und die Durchführung des Audits im Detail zu planen. Dazu müssen Sie in einem ersten Schritt die relevanten Ansprechpartner identifizieren.

In der Regel betreibt die IT-Abteilung bzw. der IT-Bereich das Rechenzentrum. Sind Rechenzentrumsdienstleistungen ausgelagert, so sind auch die Ansprechpartner wichtig, die diese IT-Dienstleister steuern. Um infrastrukturelle, bauliche und sonstige physische Maßnahmen zu identifizieren, beziehen Sie den Ansprechpartner für das Gebäudemanagement ein. Aufgrund der großen Schnittmenge mit Aspekten der Informationssicherheit kommt dem Informationssicherheitsbeauftragten (ISB) ebenfalls eine wesentliche Rolle beim Datenschutzaudit zu. Führen Sie Prüfungen bei einem Rechenzentrum idealerweise in Abstimmung oder in Begleitung mit dem ISB durch.

2. Schritt: Dokumente eintreiben

Im nächsten Schritt bereiten Sie die relevanten Anforderungen adressatengerecht auf. Dazu fertigen Sie am besten je Thema und Ansprechpartner eine Liste mit bereitzustellenden Dokumentationen an und erläutern sie in einem Gespräch mit den Ansprechpartnern.

BEISPIEL

In vielen Fällen bietet es sich z.B. an, folgende Dokumente anzufordern:

- *Informationssicherheits-(Datenschutz-) Leitlinie*
- *Informationssicherheits- und Datenschutzrelevante Richtlinien (z.B. Berechtigungswesen, Datensicherung, Notfallwesen, Umgang mit Sicherheitsvorfällen)*
- *Betriebshandbücher und organisatorische Vorgaben*
- *Testate von Wirtschaftsprüfern, Revision, Auditoren o.Ä.*
- *ggf. Verträge mit Unterauftragnehmern*

Die Dokumentenliste inklusive der darin aufgeführten Referenzdokumente bildet die Grundlage für Sie, um die Umsetzung der Anforderungen beurteilen zu können.

Das Ergebnis des Dokumentenaudits ist eine Übersicht von Umsetzungslücken und Themen, die Sie bei der Vor-Ort-Kontrolle und Begehung oder im direkten Gespräch (Interview) näher untersuchen müssen.

3. Schritt: Auditschwerpunkte risikoorientiert auswählen

Wählen Sie die Auditschwerpunkte der zweiten Phase risikoorientiert aus. Das bedeutet, zuvor zu bewerten, welchen Schaden die fehlende oder unvollständige Umsetzung von Anforderungen in der Organisation anrichten kann. Ziehen Sie dazu insbesondere die Schutzbedürftigkeit der betroffenen personenbezogenen Daten heran (zur Bewertung eines Risikos siehe näher Datenschutz PRAXIS 06/17, S. 14–15). Überführen Sie die risikoorientierte Schwerpunktbildung anschließend in einen Auditplan. Er bestimmt die Vor-Ort-Kontrolle. Stellen Sie den Plan den Ansprechpartnern im Vorfeld zur Verfügung, damit sie sich vorbereiten können.

Klären Sie ab, welche Audits im Rechenzentrum in der Vergangenheit stattgefunden haben. Da-

Rechtliche Grundlagen

Das Bundesdatenschutzgesetz (BDSG) schreibt vor, dass der Datenschutzbeauftragte die ordnungsgemäße Anwendung von Datenverarbeitungsprogrammen, mit denen personenbezogene Daten verarbeitet werden, überwacht (vgl. § 4g Abs. 1 Nr. 1 BDSG). Auch nach der EU-Datenschutz-Grundverordnung (DSGVO) gehört ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen (TOMs) zu den Pflichten im Rahmen einer funktionierenden Datenschutzorganisation (vgl. Art. 32 Abs. 1 Buchst. d).

Synergieeffekte nutzen

Das vorgestellte dreistufige Vorgehensmodell orientiert sich am üblichen Vorgehen zur Durchführung von internen Audits im Rahmen eines Informationssicherheitsmanagementsystems (ISMS). Damit lassen sich Synergieeffekte zwischen Datenschutz und Daten- bzw. Informationssicherheit schaffen.

mit vermeiden Sie überflüssige Audits und sorgen dafür, dass ein möglichst breites Spektrum abgedeckt ist. Prüfen Sie, ob sicherheitsrelevante Zertifikate vorhanden sind und ziehen Sie sie ebenfalls als Grundlage für Ihr Audit heran. Typische Beispiele:

- IT-Grundschutz- oder ISO/IEC-27001-Zertifizierung
- rechenzentrumsspezifische Zertifizierungen wie die Europäische Norm EN 50600
- „Trusted Site Infrastructure"-Zertifizierung (TSI) des TÜV
- eine vergleichbare US-spezifische Zertifizierung wie der Standard ANSI/TIA-942

PRAXIS-TIPP

Formulieren Sie bei nicht zertifizierten Rechenzentren im Vorfeld sogenannte kritische Ausschlusskriterien (K.-o.-Kriterien). Je nach Schutzbedarf der Daten kann beispielsweise die Datenverarbeitung außerhalb sicherer Länder ein Kriterium sein. Auch eine mangelnde Zutrittskontrolle sollte in der Regel ein K.-o.-Kriterium sein.

Phase 2: Durchführung

Ziel der zweiten Phase ist die Prüfung vor Ort, ob die Anforderungen, die Sie im Dokumentenaudit identifiziert bzw. beschrieben haben, umgesetzt sind. Die Verifikation sollte einerseits durch eine Begehung des Rechenzentrums (Inaugenscheinnahme) und andererseits durch Interviews mit fachlichen Ansprechpartnern erfolgen. Bei der Auditierung von extern betriebenen Rechenzentren, d.h. bei ausgelagerten Rechenzentrumsdienstleistungen, empfiehlt es sich, analog zu verfahren. Eine wesentliche Rolle spielen dabei Nachweisdokumente, die die Umsetzung und regelmäßige Umsetzungsprüfung faktisch belegen. Üblicherweise sind dies

- Zutrittsprotokolle zum Rechenzentrum,
- Stichproben von Zugangs- und Zugriffsberechtigungen zu relevanten Applikationen,
- Auswertungs- und Abschlussbericht zu durchgeführten Notfalltests und Notfallübungen (Nachweis der Wirksamkeit von implementierten Maßnahmen, die die Verfügbarkeit sicherstellen) sowie
- Protokolle von Funktionstests von Notfallstromgeneratoren, Klima- und Löschanlagen sowie mechanischen Schließmechanismen von Sicherheitstüren.

Im Ergebnis sollten Ihnen vollständige und belastbare Nachweise vorliegen, die Auskunft über den Umsetzungsgrad der Datensicherheit geben. Diese bilden die Basis für das Gesamtvotum des Audits und dienen als Grundlage für den in der Phase 3 zu erstellenden Auditbericht.

Phase 3: Nachbereitung

Das Ziel der dritten Phase ist es, die Vor-Ort-Kontrolle sowie die vorgelegten Nachweisdokumente auszuwerten und einen Auditbericht zu erstellen. Dieser Bericht gibt Aufschluss über vorhandene Abweichungen. Des Weiteren gehört ein priorisierter Maßnahmenplan zu den Ergebnissen dieser Phase. Der Auditbericht erfüllt v.a. zwei Zwecke:

- Im Allgemeinen beschreibt er den gesamten Auditprozess. Das umfasst sämtliche Phasen und Aktivitäten der Vorbereitung, Durchführung und Nachbereitung.
- Im Speziellen stellt er Konformitätsabweichungen hinsichtlich der nicht oder nur teilweise erfüllten Datensicherheitsanforderungen dar. Hierbei bietet sich eine Unterteilung

Mit der DSGVO werden Rechenzentrumsdienstleister stärker in die Pflicht genommen. Sie können direkt für Datenschutzverstöße verantwortlich gemacht werden.

Foto: AKodisinghe/iStock/Thinkstock

Zertifikate vorlegen lassen

Umgang mit größeren Rechenzentrumsdienstleistern

In der Praxis kann sich die Prüfung von größeren Rechenzentrumsdienstleistern etwas anders darstellen. Insbesondere bei Rechenzentren, die nach gängigen Sicherheitsstandards zertifiziert sind (z.B. IT-Grundschutz- oder ISO/IEC-27001-Zertifizierung oder rechenzentrumsspezifische Zertifizierungen), ist eine Vor-Ort-Kontrolle beim Dienstleister vertraglich häufig nicht vorgesehen. Das ist auch nachvollziehbar, da Rechenzentren mit mehreren tausend Kunden andernfalls einen regelrechten „Kontrolltourismus" bewältigen müssten. Das ist aus Sicht der Rechenzentren aus Sicherheitsgründen zu vermeiden. In aller Regel verweist der Dienstleister darauf, dass sein Rechenzentrum regelmäßig durch unabhängige externe Auditoren geprüft wird und dass sich damit die Umsetzung von Datensicherheitsmaßnahmen auf Basis dieser Sicherheitsstandards nachweisen lässt.

Eine Kontrolle kann in diesen Fällen dadurch erfolgen, dass Sie die aktuellen Zertifikate anfordern. Achten Sie hierbei darauf, dass das Zertifikat gültig ist und dass der Zertifizierungsgegenstand (Scope) sich tatsächlich auf die Dienstleistung bezieht, die für Sie als Auftraggeber relevant ist. Gegebenenfalls können Sie auch Auditberichte anfordern, um die Prüfmethodik und die Kontrolltiefe nachvollziehen zu können.

in die Kategorien Hauptabweichungen (HA) und Nebenabweichungen (NA) an. HA beschreiben Abweichungen, die einen verhältnismäßig hohen Schaden für die auditierte Organisation bedeutet, während NA einen geringen Schaden bewirken.

Weisen Sie die Abweichungen den verantwortlichen Ansprechpartnern, die Sie in der Vorbereitungsphase identifiziert und festgelegt haben, zu. Das stellt sicher, dass Sie die richtigen Leute adressieren. Stellen Sie die jeweiligen Anforderungen und den Umsetzungsstand sowie die vorgelegten Nachweisdokumente im Auditbericht direkt gegenüber. Das macht den normativen Charakter dieses Audits deutlich.

Ist der Auditbericht erstellt und verabschiedet, stellen Sie unter Einbeziehung des ISB sicher, dass die definierten Maßnahmen auch wie vorgesehen umgesetzt werden. Vereinbaren Sie dazu mit den Umsetzungsverantwortlichen Regeltermine und halten Sie die Umsetzung nach.

Zusammenfassende Empfehlungen

- Die Datenschutz-Grundverordnung verzahnt Datenschutz und Informationssicherheit stärker miteinander. Vor allem angesichts der neuen Dokumentations- und Kontrollpflichten ist zu empfehlen, den Datenschutz in – eventuell schon bestehende – Managementsysteme der Informationssicherheit zu integrieren.
- Um Synergien zu nutzen, ist eine enge Zusammenarbeit zwischen Datenschutzbeauftragtem und Informationssicherheitsbeauftragtem sinnvoll. Denn die Methoden und Verfahren zur Durchführung von Audits im Informationssicherheitsbereich lassen sich effizient auch für Ihre Datenschutzaudits adaptieren.
- Gerade vor dem Hintergrund, dass Datenschutzbeauftragte oftmals keinen tiefer gehenden technischen Hintergrund besitzen, bieten sich die IT-Grundschutzkataloge des BSI als gute Orientierungshilfe an, um konkrete Anforderungen an die Datensicherheit und Datensicherheitsmaßnahmen in die Kontrolle einfließen zu lassen.


Wirtschaftsinformatiker (M.Sc.) Marc Ragg und Rechtsanwalt Boris Arendt sind als Experten in den Bereichen Datensicherheit, Cybersicherheit und Datenschutz für die Unternehmensberatung PricewaterhouseCoopers (PwC) tätig.

Es bietet sich an, im Anhang des Auditberichts einen Maßnahmenplan festzulegen, der mit den verantwortlichen Ansprechpartnern abgestimmt ist, um die Abweichungen zu beheben. Idealerweise terminieren Sie die Handlungsfelder, die sich aus dem Audit ergeben, und weisen sie einem Umsetzungsverantwortlichen zu.

Ihre Erfolgsfaktoren

Zusammenfassend sind bei der datenschutzrechtlichen Überprüfung eines Rechenzentrums folgende Erfolgsfaktoren besonders wichtig:

- **Berücksichtigen Sie bei Ihrer Auditplanung vorhandene Zertifizierungen und bereits durchgeführte Audits.**
- **Verwenden Sie am besten standardisierte Methoden für Audits.**
- **Stimmen Sie die Auditschwerpunkte mit dem ISB und dem Gebäudemanagement ab.**
- **Sofern vorhanden: Sorgen Sie dafür, dass Ihre Ergebnisse in das ISMS zurückfließen.**
- **Halten Sie nach, ob die Maßnahmen wirklich umgesetzt werden, um Abweichungen frühzeitig zu erkennen.**

Landesbeauftragter Bayern

Schutz gegen Ransomware

Ransomware stellt eine neue Form der Trojanischen Pferde dar. Der Begriff setzt sich aus den Wörtern „Ransom" (englisch für „Lösegeld") und „Software" zusammen. Der Bayerische Landesbeauftragte für den Datenschutz gibt folgende Hinweise zum Schutz vor Ransomware:

- Wichtigste Vorbeugemaßnahme ist, regelmäßig Datenbackups auf externen, nicht dauerhaft angeschlossenen Datenträgern zu erstellen.
- Permanent angeschlossene Laufwerke oder Datenträger sind ein Risiko. Denn Ransomware kann das gesamte Netzwerk – und damit angeschlossene Sicherungsdatenträger – befallen.
- Damit eine zentrale Datensicherung möglich ist, sind die Benutzer anzuhalten, ihre Daten auf Netzlaufwerken abzuspeichern.
- Die eingesetzten Betriebssysteme (auch auf Tablets und Smartphones), Virenscanner, Webbrowser sowie Browser-Erweiterungen sollten immer auf dem neuesten Stand sein, indem Updates und Patches eingespielt werden.
- Hersteller von Antivirensoftware bieten Spezialtools gegen Verschlüsselungsversuche an. Sobald das Tool entsprechende Versuche registriert, stoppt es diese Vorgänge und erzeugt eine Warnmeldung.
- Um Drive-by-exploits-Angriffen vorzubeugen, sollten die Webbrowser mithilfe von Werbeblockern gegen die Ausführung unnötiger Scripts und anderer eingebundener aktiver Inhalte geschützt werden.
- Da Ransomware häufig über Spam-Mails kommt, sollte ein Spamfilter solche E-Mails als Spam markieren.
- E-Mails mit ausführbaren Dateien im Anhang (z.B. .exe, .scr, .chm, .bat,.com, .msi, .jar, .cmd, .hta, .pif, .scf) sollten geblockt und nicht an den Empfänger weitergeleitet werden.
- Grundsätzlich sollte die Makroausführung in Office-Programmen deaktiviert sein.
- Lässt es sich nicht vermeiden, dass Makros in Office-Dokumenten genutzt werden, sollten diese digital signiert und nur die Ausführung von Makros mit festgelegten digitalen Signaturen erlaubt sein.

Quelle: Bayerischer Landesbeauftragter für den Datenschutz, 27. Tätigkeitsbericht 2015/2016, S. 30/31, abrufbar unter http://ogy.de/bericht-baylfd.

Foto: nicescene/iStock/Thinkstock

Landesbeauftragter Hessen

Mitarbeiter-Passwörter im Tresor?

Manche Unternehmen verpflichten alle Mitarbeiter dazu, ihre Passwörter in einem verschlossenen Umschlag zu übergeben, und bewahren diese Umschläge zentral in einem Tresor auf. Gegen diese Praxis wendet sich der Hessische Landesbeauftragte für den Datenschutz. Er vertritt folgende Auffassung: Aus Sicht des IT-Betriebs gibt es keinerlei Gründe für dieses Vorgehen. Vielmehr stehen Belange des Mitarbeiterdatenschutzes dem entgegen. Sofern solche Maßnahmen angeordnet sind, sind sie unverzüglich einzustellen. Die geschilderte Vorgehensweise unterläuft den Grundsatz, dass nur dem Benutzer das Passwort zu seinem Konto bekannt ist und dass somit jedes Handeln mit dem Benutzerkonto ihm zuzurechnen ist.

Vergisst ein Mitarbeiter sein Passwort, kann der Administrator über die Benutzerverwaltung einfach und schnell ein neues, temporäres Passwort vergeben. Der Mitarbeiter muss es unverzüglich wieder in ein nur ihm bekanntes Passwort ändern. Für verwaltende Tätigkeiten steht den Administratoren das Administratorkonto des Systems zur Verfügung. Es ist zumindest bei der Betriebssysteminstallation vorhanden. Aus Gründen der Nachvollziehbarkeit – insbesondere wenn wechselweise mehrere Mitarbeiter administrieren – sollten hierfür jedoch personalisierte Administratorkonten zum Einsatz kommen. Über die als Windows-Standard eingestellte Anzeige des zuletzt erfolgreich angemeldeten Benutzers erhält der Mitarbeiter bei der nächsten eigenen Anmeldung dann den Hinweis, welcher Administrator sich an seinem System angemeldet hat (und kann diesen ggf. nach dem Grund hierfür fragen).

Quelle: 45. Tätigkeitsbericht des Hessischen Landesbeauftragten für den Datenschutz, vorgelegt zum 31.12.2016, S. 165/166, abrufbar unter http://ogy.de/bericht-hdsb.

Foto: phive2015/iStock/Thinkstock

Dr. Eugen Ehmann ist Regierungsvizepräsident von Mittelfranken (Bayern) und Mitherausgeber eines neuen Kommentars zur Grundverordnung.

Foto: Rawpixel Ltd/iStock/Thinkstock

Sofern noch nicht vorhanden, stellen Sie Regeln auf, wie die Mitarbeiter die Besprechungsräume nutzen sollten. „Licht aus und Fenster zu" reicht hier nicht.

Datenschutzkontrolle

Datenschutz in Besprechungsräumen

Operationslisten, Bewerbungsmappen, Passwörter, … – das und vieles mehr können Sie bei einer Vor-Ort-Kontrolle in Besprechungsräumen finden. Worauf müssen Sie achten?

Ortsbegehung Datenschutz. Der Bereichsleiter führt den Datenschutzbeauftragten von Büro zu Büro. Im Bürotrakt befindet sich auch ein Besprechungsraum. Dort läuft gerade ein Meeting. Der Bereichsleiter schlägt vor, diesen Raum nicht zu begehen, da dort „nur" Besprechungen stattfinden. Was haben die schon mit Datenschutz zu tun? Außerdem darf jetzt nicht gestört werden. Der DSB stimmt zu …

Spannende Fundstücke

Was kann in Besprechungsräumen schon Verfängliches sein? Sehr viel! Hier eine kleine Auswahl von mir tatsächlich gefundener personenbezogener Unterlagen in Besprechungsräumen:

- Bewerbungsmappen
- OP-Liste in einem Klinikum (Überbleibsel der Frühbesprechung), die Rückseite wurde als Notizblatt verwendet
- handgeschriebene Notizen über die Preise und die Leistungen von Mitbewerbern
- Ausdruck mit Fehltagen und -zeiten eines namentlich genannten Mitarbeiters
- USB-Stick, der in einem Rechner steckt

Konsequenz: Verantwortung und Kontrollen müssen eindeutig geregelt sein. Auf welche Punkte kommt es dabei an?

Netzwerkzugänge & Bildschirme

Viele Besprechungsräume halten die erforderliche Technik dauerhaft vor. Dann befindet sich dort ein fest installierter Rechner, der ans Netzwerk angeschlossen ist. Personen, die das Gerät für eine Besprechung oder Schulung benötigen, müssen sich anmelden. Leider wird nicht selten das Abmelden vergessen. Die Teilnehmer der Folgebesprechung, oft Externe, finden ein offenes Netzwerk vor. Gleiches gilt für Bildschirme. Auch sie sind beim Verlassen des Raums zu sperren, etwa in Pausen und natürlich am Ende der Besprechung.

BEISPIEL

Bei einer Begehung fand ich einen beschriebenen Flipchart-Block vor. Er enthielt das Passwort für einen Schulungszugang zur Personalsoftware. Drei Blätter weiter stand, wie man vom Testzugang aus den Resturlaubsanspruch mitsamt der Urlaubshistorie aufrufen kann. Die dazu nötigen Personalnummern fanden sich im Papierkorb auf einem zusammengeknüllten Ausdruck mit Personalnummern. In der Folge hätte ich jeden beliebigen Urlaub der Beteiligten auslesen, gewähren, ändern, versagen oder löschen können.

Patchdosen

Oft befinden sich in Besprechungsräumen Patchdosen für den Netz- bzw. Internetzugang berechtigter Personen. Externe erhalten einen Gastzugang. Dieser muss auf erforderliche Zugriffe begrenzt und zusätzlich gegen Schadsoftware gesichert sein.

Prüfen Sie, ob Patchzugänge vor unbefugten Zugriffen geschützt sind. User-Zugänge bestehen meist aus Vornamen und Namen – im Besprechungsraum liegt oft eine Telefonliste aus. Jetzt fehlt noch das Passwort. Mit Erfahrung und etwas Glück können Profis rasch ins Netz gelangen. Patchdosen sind daher zusätzlich zu sichern.

Wenn Whiteboards doch immer weiß wären …

Whiteboards gehören wie Flipcharts zur Standardausstattung vieler Besprechungsräume. Nach dem Ende der →

Besprechung sind sie zu reinigen. Das gilt erst recht, wenn sich personenbezogene Daten auf den Tafeln befinden.

Smartboards

Immer öfter kommen in Besprechungsräumen Smartboards zum Einsatz. Smartboards sind eine Kombination aus Tafel bzw. Whiteboard und großem Computerbildschirm, auf dem die Mitarbeiter mit geeigneten Stiften auch schreiben können. Notierte Inhalte lassen sich zusammen mit der Projektion abspeichern und per Mail an die Besprechungsteilnehmer versenden. Das bringt Risiken mit sich:

- Versendete Dateien können vertrauliche Informationen enthalten, die so in die Hände Unbefugter gelangen.
- Außerdem speichern Smartboards temporäre Dateien ab, die spätere Anwender wieder öffnen können. Das kann zu Datenschutzverletzungen führen.

Der Telkostern als Wanze

Telkosterne unterstützen Telefonkonferenzen, da sie die Sprachqualität verbessern. Sie haben in der Telefonanlage eine eigene Durchwahlnummer. Damit können sich Personen von außen in eine Telefonkonferenz einwählen. Diese Einwahl lässt sich bei einigen Geräten ohne Rufton vornehmen, um laufende Konferenzen nicht zu stören. So könnten sich Unbefugte unbemerkt in laufende Besprechungen einwählen und jedes Wort mithören. Klären Sie, ob ein solches Einwählen möglich ist. Wenn ja, lassen Sie diese Funktion außer Kraft setzen.

ACHTUNG!

Flipcharts sind in Besprechungsräumen Standard. Zu oft lassen Mitarbeiter beschriebene Blätter unbedacht auf dem Flipchart. Vom Passwort über Planzahlen des Unternehmens bis hin zu vertraulichen Projektdetails findet sich hier vieles. Mithilfe eines Mobiltelefons lassen sich leicht Daten fotografieren und weitergeben. Daher beschriebene Blätter immer entfernen!

To dos für die Mitarbeiter

Checkpunkt	erledigt
Reservierungswege einhalten	☐
benötigte Technik melden	☐
verantwortliche Person für die Besprechung festlegen und melden	☐
Smartboards: Dateien löschen, auch temporäre Dateien, Vorsicht beim Versenden von Mails mit vertraulichen Informationen	☐
Flipchart-Bögen mitnehmen und sicher entsorgen	☐
Whiteboards reinigen	☐
Veranstaltungsrechner abmelden und ausschalten, bei kurzen Pausen Bildschirm sperren	☐
USB-Sticks entfernen	☐
Papierkörbe kontrollieren	☐
Schredder nutzen	☐
Endkontrolle auf möglicherweise vergessene Unterlagen mit personenbezogenen Daten vornehmen (Checkliste ausfüllen)	☐
Besprechungsräume immer abschließen	☐

Regeln für Besprechungsräume. Je nach Einrichtung der Besprechungsräume regeln Sie mindestens die in der Checkliste genannten Punkte. Abonnenten finden die Checkliste unter www.datenschutz-praxis.de/praxishilfen.

Papierkörbe in Besprechungsräumen

Unterlagen sind am Ende des Meetings zu entfernen, um Fundstücke wie eingangs beschrieben zu vermeiden. Teilnehmer von Besprechungen sind oft so eng getaktet, dass sie von einem Meeting ins nächste hetzen. Werden Unterlagen ausgeteilt, entsorgen die Mitarbeiter sie oft noch rasch vor dem nächsten Meeting. So wird der Papierkorb zum Fundort für vertrauliche Informationen. Daher ist nach dem Ende eines Meetings alles systematisch zu entfernen. Das gilt auch für Notizen.

Reihen gleichartiger Besprechungen

Finden ähnliche Besprechungen mehrfach hintereinander statt, sinkt die Aufmerksamkeit, was herumliegende Unterlagen angeht, je länger die Gespräche dauern.

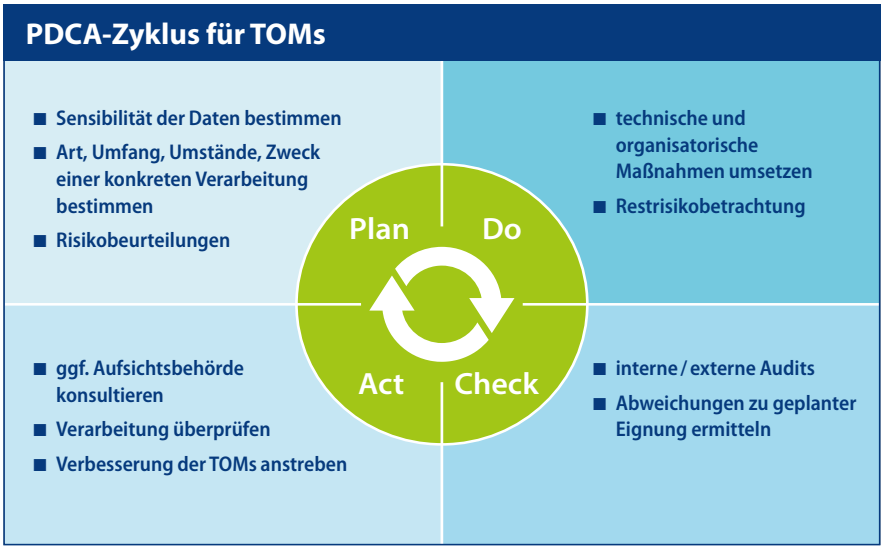
Besonders bei Bewerbungsgesprächen kommt es immer wieder vor, dass Bewerber im Raum Hinweise auf andere Bewerber vorfinden. Das wirkt unprofessionell und ist ein klarer Verstoß gegen Datenschutzvorgaben. Nach jeder Vorstellungsrunde ist der Raum darauf zu untersuchen, dass keine Hinweise auf vorherige Gespräche vorhanden sind.

Besprechungsräume = Archiv?

In Anwaltskanzleien oder bei Steuerberatern stehen in Besprechungsräumen oft Aktenschränke. Da schon der Name eines Mandanten unter das Privatgeheimnis fällt, dürfen die Rückenschilder von Akten in solchen Räumen keine eindeutigen personenbezogenen Daten enthalten. Daher sind sie entweder mit neutralen Nummern zu versehen, oder die Schränke müssen undurchsichtige Türen haben und bei Besprechungen mit Externen verschlossen sein.

Und wie für alle Besprechungsräume gilt natürlich auch hier: Es dürfen keine Unterlagen offen herumliegen. Flipcharts, Whiteboards und Bildschirme dürfen keine Hinweise auf Mandate oder andere personenbezogene Daten geben.

Eberhard Häcker ist externer Datenschutzbeauftragter, der in seinem Datenschutzalltag schon viel erlebt hat.



Das Prinzip der stetigen Verbesserung (PDCA-Zyklus) sorgt für geeignete technische und organisatorische Maßnahmen

Technische und organisatorische Maßnahmen

Tipps zur Auswahl von TOMs

Die Datenschutz-Grundverordnung (DSGVO) stärkt den technischen Datenschutz. Sie bleibt aber vage, was konkrete Maßnahmen angeht. Wir stellen Möglichkeiten vor, diese Lücke zu füllen.

Die vermeintlich einfachen Kontrollpflichten der Anlage des § 9 Bundesdatenschutzgesetz (BDSG) verführen bisher dazu, sie als rein formale Punkte zu verstehen. In generische Checklisten umgesetzt, ermöglicht das zwar eine einfache Anwendung für „jedermann". Es führt aber dazu, dass die technischen und organisatorischen Maßnahmen (TOMs) mitunter zwei wichtige Anforderungen nicht erfüllen:

1. Wirksamkeit

Die technischen und organisatorischen Maßnahmen müssen, umgangssprachlich gesagt, auch etwas „bringen", d.h. sie sollen dazu beitragen, die datenschutzrechtlichen Anforderungen umzusetzen. Negativbeispiele sind etwa

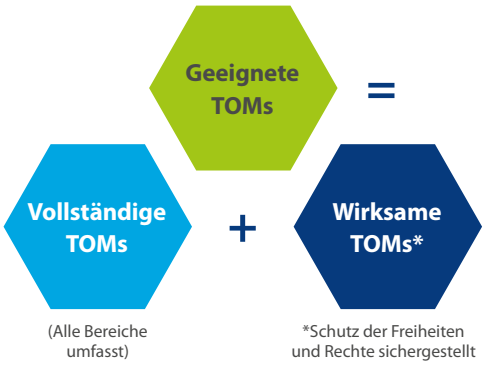
- die schlichte Nennung von Firewalls zum Schutz gegen externe Angreifer (bringen bei Web-Hacking-Angriffen nichts),
- Hashverfahren als vermeintlich geeignete Anonymisierungsverfahren (sind sie meist nicht) oder
- die pauschale Nennung von Rollen-Rechte-Konzepten (erst die korrekte Umsetzung bringt den Schutz).

Auch hängen die TOMs vom Anwendungsszenario ab. Eine Aktenvernichtung benötigt andere Maßnahmen als der Betrieb eines Cloud-Service oder einer smarten Anwendung wie Pay-as-you-drive-Tarife von Versicherungen.

2. Vollständigkeit

Schutzmaßnahmen müssen das komplette Spektrum von Risikoquellen – beispielsweise Hacker, ungeschulte Mitarbeiter, eine übereifrige Marketing-Abteilung, die Verarbeitung an sich, … – auf allen relevanten technischen und organisatorischen Ebenen der Verarbeitungsprozesse umfassen. So mag mitunter zwar das Hosting einer Webanwendung in einem Rechenzentrum bezüglich der Perimetersicherheit, der Zugangskontrolle sowie der Versorgung mit Strom sehr gut umgesetzt sein. Die Webanwendung kann aber mangels geregeltem Patch-Management und aufgrund von Fehlkonfigurationen für jedermann „offen wie ein Scheunentor" sein.

Zielsetzung bei der Ausgestaltung der TOMs nach der DSGVO muss daher sein, geeignete technische u nd organisatorische Maßnahmen auszuwählen, die sich auf folgende Formel bringen lassen:



Keine Chance ohne Managementsystem

Spätestens bei der Frage, wie man als Verantwortlicher die Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO erfüllt, kommt man um ein Managementsystem nicht herum. Es basiert auf dem Prinzip der stetigen Verbesserung. Es lässt sich mit dem sogenannten PCDA-Zyklus (Plan – Do – Check – Act) abbilden und umfasst auch die Maßnahmenauswahl. →

PRAXIS-TIPP

Ein Tipp für kleine Unternehmen: Das Verarbeitungsverzeichnis (passt auf wenige Seiten Papier) regelmäßig vom Datenschutzexperten prüfen lassen, aktualisieren und das kurz dokumentieren – dann ist schon viel mit wenig Aufwand erreicht.

Das bedeutet, dass die Auswahl von TOMs keine einmalige Sache ist. Die Maßnahmen müssen regelmäßig über Audits geprüft und mit dem Fokus „geeignet" bewertet werden.

Keine Checklisten, aber Kataloge

Die Frage, ob es denn Checklisten für TOMs unter der DSGVO gibt, muss weiterhin mit einem klaren Nein beantwortet werden. Allerdings können und sollen Verantwortliche Kataloge mit Maßnahmen verwenden – sie müssen aber auch dann die Eignung der Maßnahmen passend zur jeweiligen Verarbeitungstätigkeit nachweisen. Im Folgenden einige Beispiele:

ISO-27000-Familie

Der Standard ISO 27001 setzt ein Informationssicherheitsmanagementsystem (ISMS) um. Passend dazu gibt es einen Katalog mit Best-Practice-Empfehlungen in der ISO 27002. Er beschreibt in 14 Abschnitten 113 Sicherheitsmaßnahmen (Security Controls). Zu beachten ist, dass die ISO-Standards sehr dokumentenorientiert sind, die TOMs aber nicht nur auf dem Papier stehen dürfen. Die Maßnahmen legen den Fokus auf Informationssicherheit und berücksichtigen, allein verwendet, ggf. den technischen Datenschutz nur unzureichend.

ISO 29151

Datenschutz ist mehr als nur Informationssicherheit. Das bedeutet, dass zum einen der Fokus der Risikobetrachtung auf den Freiheiten und Rechten des Betroffenen liegt. Zum anderen muss der Verantwortliche weitere Grundsätze wie z.B. Datenminimierung realisieren. Der Standard ISO 29151 geht diesen Weg in zweierlei Weise: Er konkretisiert den Katalog der Security Controls aus der ISO 27002 auf den Datenschutz und erweitert ihn um Maßnahmen (Privacy Controls), deren Ursprung in der ISO 29100 zu finden sind. Trotz dieses geschärften Blickwinkels ist auch bei diesem Standard auf geeignete Maßnahmen zu achten.

IT-Grundschutzkataloge

Die umfangreichen IT-Grundschutzkataloge lassen sich wie bisher verwenden, um das Risiko unbefugter oder unrechtmäßiger Verarbeitungen (z.B. für Art. 32 DSGVO) einzudämmen. Sie sind damit vergleichbar zur ISO 27002 einzusetzen.

Standard-Datenschutzmodell

Das Modell, das momentan einige deutsche Aufsichtsbehörden entwickeln und evaluieren, soll in Zukunft ebenfalls einen umfangreichen Maßnahmenkatalog erhalten. Es soll sich in die IT-Grundschutzmethode einfügen und sie um den Blickwinkel des Datenschutzes erweitern.

NIST

Auch in den USA gibt es den technischen Datenschutz, wie ein Blick in verschiedene Dokumente der NIST (National Institute of Standards and Technology) offenbart. Aktuelle Dokumente zeigen, dass datenschutzspezifische Schutzziele langsam den Weg in diese Standards finden.

Ergebnis

Checklisten, die den Anspruch haben, alle TOMs für alle Verarbeitungstätigkeiten geeignet umzusetzen, wird es bei der Datenschutz-Grundverordnung nicht geben. Vorstellbar sind allenfalls Checklisten in Bereichen, die stark homogene Verarbeitungsvorgänge und IT-Systeme haben, wie Arztpraxen, Office-IT oder Aktenvernichtung. Bei allen anderen müssen Verantwortliche basierend auf dem Risiko der Verarbeitung aus Maßnahmenkatalogen, die sowohl Security Controls – Blickwinkel: unbefugte Verarbeitung oder unbefugter Zugriff – als auch Privacy Controls – Blickwinkel: rechtmäßige Verarbeitung – enthalten, wirksame und geeignete TOMs auswählen.

Andreas Sachs ist Referatsleiter Technischer Datenschutz und IT-Sicherheit beim Bayerischen Landesamt für Datenschutzaufsicht.

ONLINE-TIPP

- *BSI: Kryptographische Verfahren: Empfehlungen und Schlüssellängen, 2017, www.bsi.bund.de*
- *Enisa: Algorithms, key size and parameters report, 2014, www.enisa.europa.eu*
- *ISO27002: Beziehbar unter www.iso.org/standard/54533.html*
- *ISO29151: Beziehbar unter www.iso.org/standard/62726.html*
- *IT-Grundschutz: detaillierte Informationen unter www.bsi.bund.de*
- *Standard-Datenschutzmodell (Version 1.0): http://ogy.de/sdm*

Pseudonymisierung & Verschlüsselung

Wirksame technische Konzepte

Die Grundverordnung nennt ausdrücklich zwei technische Konzepte, die zu den wirksamsten des Datenschutzes gehören – sofern sie richtig eingesetzt werden:

Pseudonymisierung

Unter Pseudonymisierung versteht man das Ersetzen eines identifizierenden personenbezogenen Datums (z.B. Name, E-Mail-Adresse, Versichertennummer) mit einem neuen Wert (dem Pseudonym), sodass nur bestimmte Stellen/Personen des Verantwortlichen diese beiden Werte in einer Abbildungstabelle (z.B. Excel, Datenbank) zusammenbringen können.

Verschlüsselung

Kryptografische Verfahren umfassen symmetrische Verschlüsselung (z.B. AES), asymmetrische Verschlüsselung (z.B. RSA) und Hashverfahren (z.B. SHA-512). Sie haben nach der DSGVO wie heute schon dem Stand der Technik zu entsprechen.

Foto: Microsoft AG

Microsoft will mit den neuen Einstellungsmöglichkeiten Anwender nicht überfordern. Daher hat es viele Optionen gestrichen oder gebündelt.

Windows 10

Datenschutz im Creators Update verstehen

Mit dem Creators Update, auch als Redstone 2 bekannt, hat Microsoft die neue Version von Windows 10 veröffentlicht. Wie bei jeder Version nimmt Microsoft Datenschutz-Anpassungen vor. Was ist neu?

Mit der Aktualisierung ändert Microsoft deutlich die Einstellungsmöglichkeiten für den Datenschutz. Das heißt, nach der Installation des Updates sollten Administratoren in der Einstellungs-App zum Bereich Datenschutz wechseln. Hier sind neue Einstellungen und andere Optionen zu sehen. Die Express-Einstellungen wurden zusammengefasst und über Schieberegler zur Verfügung gestellt. Es gibt in Windows 10 Version 1703 – so heißt es nun offiziell nach dem Update – also keine Schaltfläche für die Express-Einstellungen mehr.

Weniger Einstellungsmöglichkeiten, aber gebündelter

Microsoft stellt nun generell deutlich weniger Einstellungsmöglichkeiten zur Verfügung, um den Datenschutz zu verbessern. Allerdings weist es darauf hin, dass die verschiedenen Einstellungen nur zusammengefasst wurden: Mit wenigen Klicks lassen sich also mehr Datensammel-Aktionen auf einmal deaktivieren.

Windows 10 Version 1703 verfügt über angepasste Datenschutzeinstellungen

Datenkrake Cortana

Werden Rechner mit Windows 10 Version 1703 neu installiert, ist während der Installation Cortana automatisch aktiviert. Cortana ermöglicht zwar eine sprachgesteuerte Installation. Allerdings ist der Sprachassistent dann auch im Rahmen des Betriebs von Windows 10 aktiv.

Außerdem will der Assistent die Verwendung eines Online-Kontos oder die Aktivierung von Cortana innerhalb des Betriebssystems aufdringlich erzwingen.

Ist Cortana aktiviert, zeigt der Assistent auch Informationen an, wenn ein Anwender seinen PC gesperrt hat. Das Verhalten lässt sich, wie andere Einstellungen von Cortana, über Gruppenrichtlinien steuern. Dazu stellt Microsoft eine neue Version der ADMX-(Administrative-Templates-) Dateien zur Verfügung. Damit lassen sich die Einstellungen nach der Installation anpassen (http://ogy.de/admx-dateien).

Datenschutz während der Installation steuern

Im Rahmen der Installation hat Microsoft nicht nur die Anbindung von Cortana geändert, sondern auch die Steuerungsmöglichkeiten des Datenschutzes. Standardmäßig sind in Windows 10 Version 1703 nahezu alle Sammelaktionen aktiviert. Anwender müssen sie erst manuell deaktivieren.

Sind die Datensammelfunktionen deaktiviert, reduziert sich die Übertragung laut Microsoft auf notwendige Protokolle zur Fehleranalyse. Allerdings lassen sich alle Funktionen nur zuverlässig abstellen, wenn Administratoren mühsam den Netzwerkverkehr von Windows 10 überwachen und die Server bei Microsoft in der Firewall blockieren.

Windows Hello for Business

Mit Windows 10 Version 1703 können Unternehmen Kennwörter durch eine →

Zwei-Wege-Authentifizierung ersetzen, die sich auch über Azure Active Directory nutzen lässt. Hier ist für den Datenschutz zu steuern,

- wo die Funktion Daten speichert,
- welche Anwender die Funktion nutzen,
- wie die Anmeldung abgesichert wird.

Die Anmeldung an Azure Active Directory kann durch Sicherheitsrichtlinien gesteuert werden.

PRAXIS-TIPP

Deaktivieren Administratoren oder Anwender die Datensammelfunktionen während der Installation, zeigt Windows 10 gelbe Warnmeldungen an. So entsteht der Eindruck, dass die aktivierten Datensammlungen notwendig sind, damit das Betriebssystem fehlerfrei funktioniert. Lassen Sie sich dadurch nicht irritieren.

Windows Defender Advanced Threat Protection (ATP)

Der Clouddienst Windows Defender Advanced Threat Protection (ATP) soll für mehr Sicherheit in Windows-10-Netzwerken sorgen. Dazu wird auf den Arbeitsstationen ein Dienst installiert, der mit Sensoren Informationen zur Verwendung des Betriebssystems in die Cloud überträgt.

Die Sensoren waren bereits in der Vorgängerversion Windows 10 Version 1607 (Anniversary Update, Redstone 1) aktiv. Allerdings hat Microsoft die Zusammenarbeit von Windows 10 Version 1703 und Windows Defender Advanced Threat Protection (ATP) deutlich erweitert. Es gibt zahlreiche neue Sensoren und Daten, die in die Cloud übertragen und durch Administratoren ausgewertet werden können.

Die Funktion baut generell auf Windows Defender auf, unterstützt aber auch die Virenscanner anderer Hersteller. Bevor der Cloud-Dienst zum Einsatz kommt, spielt es also eine wichtige Rolle, die einzelnen Sensoren sowie die Möglichkeiten der Datenüberwachung zu prüfen.

Mobile Überwachung in Windows 10

Windows 10 Version 1703 bietet weitaus mehr Möglichkeiten, mobile Arbeitsstationen und Tablets zentral zu steuern. Die neue Version bietet Funktionen, die durch Mobile-Device-Management-(MDM-)Lösungen auslesbar sind.

Darüber hinaus lassen sich zahlreiche weitere solcher Sensoren einbinden, etwa um Office zentral zu steuern und zu überwachen. Administratoren können beliebige Richtlinien und Überwachungsfunktionen aktivieren, die dann an die MDM-Lösung geschickt werden.

ONLINE-TIPP

In einem eigenen Blog-Beitrag informiert Microsoft genauer darüber, wie es um den Datenschutz in Windows 10 bestellt ist: http://ogy.de/privacy-journey.
Alle Daten, die Windows 10 Version 1703 sammelt, listet Microsoft in der TechNet auf: http://ogy.de/diagnostic-data

Hier spielt der Datenschutz natürlich eine wichtige Rolle, da nicht ganz klar ist, welche Daten gesammelt werden und wo das geschieht. Fakt ist nur, dass Windows 10 Version 1703 auch dann in der Lage ist, diese Daten zu senden, wenn keinerlei Zusatzsoftware installiert wird. Denn die Überwachungs- und Steuerungsfunktionen gehören zu den Bordmitteln in Windows 10 Version 1703.

Fazit: Kein Datenschutzpreis in Sicht

Auch mit Windows 10 Version 1703 wird Microsoft sicherlich keinen Preis für den Datenschutz gewinnen. Die neue Version sammelt weiterhin massiv Daten und erlaubt keine komplette Blockierung der Datenübertragungen. Zwar hat Microsoft die Optionen vereinfacht. Doch die Datensammlungen sind nur wenig transparent, und nicht alle Übertragungen lassen sich auch garantiert abstellen.

Schlussendlich müssen Unternehmen auf Zusatztools zurückgreifen und Datenverbindungen in der Firewall blockieren.

Thomas Joos ist freiberuflicher Autor und Journalist mit über 20 Jahren Berufserfahrung als IT-Consultant und Trainer. Schwerpunktmäßig beschäftigt er sich mit Microsoft-Produkten und der Sicherheit in Netzwerken.

Windows 10 sammelt fleißig weiter

Datensparsamkeit? Fehlanzeige!

Microsoft hat zwar versprochen, dass sich Windows 10 bei der Aktualisierung an die Datenschutzeinstellungen hält, die der Anwender vor der Installation gesetzt hat. Allerdings lässt sich das nur schwer nachverfolgen. Nach wie vor sammelt Windows 10 viele Daten:

- aus dem Browser
- aus der App-Nutzung
- aus der Spracherkennung
- von Cortana
- Daten zur Hardware des Rechners
- Ortungsdaten
- Verbindungsinformationen u.v.m.

Hören Anwender Musik mit Windows 10, werden diese Informationen ebenfalls genutzt und übertragen; das gilt auch für andere Mediendateien wie Filme. Verwenden Anwender Cortana aktiv, überträgt Windows 10 Version 1703 noch mehr Daten, etwa Suchanfragen. Sie werden übrigens auch gemessen und übertragen, wenn Edge im Einsatz ist, der Nachfolger des Internet Explorer.

Fotos: iStock.com/MarioGuti; Jorisvo/iStock/Thinkstock

Zum Schluss ging alles erstaunlich schnell: Am 12. Mai 2017 hat der Bundesrat den Gesetzentwurf für das „Datenschutz-Anpassungs- und -Umsetzungsgesetz EU (DSAnpUG-EU)" binnen weniger Minuten gebilligt.

Das „BDSG-neu"

Ein Blick auf wesentliche Änderungen

Der Artikel 1 des nun verabschiedeten Datenschutz-Anpassungs- und -Umsetzungsgesetzes enthält die Neufassung des Bundesdatenschutzgesetzes (BDSG-neu). Welche seiner Regelungen haben besondere Bedeutung für die Privatwirtschaft? Und wo verstößt der nationale Gesetzgeber möglicherweise gegen die DSGVO?

Die Datenschutz-Grundverordnung (EU) 2016/679, kurz meist DSGVO genannt, gilt in allen Mitgliedstaaten der EU unmittelbar. Das ist bei sämtlichen EU-Verordnungen so, wie sich aus Art. 288 Abs. 2 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) ergibt: „Die Verordnung hat allgemeine Geltung. Sie ist in allen ihren Teilen verbindlich und gilt unmittelbar in jedem Mitgliedstaat."

„Öffnungsklauseln" = „spezifischere Vorschriften"

Nationale Regelungen, wie sie der deutsche Gesetzgeber nunmehr im BDSG-neu getroffen hat, sind daneben normalerweise nicht zulässig. Etwas anderes gilt dann, wenn die DSGVO es ausdrücklich erlaubt. Dies geschieht durch entsprechende Formulierungen in einzelnen Bestimmungen. Sie werden in Deutschland meist als „Öffnungsklauseln" bezeichnet.

Einige Kritiker halten diesen Begriff für unglücklich gewählt. Ihre Begründung: Er erweckt den Eindruck, als könne der nationale Gesetzgeber in solchen Fällen völlig frei handeln, obwohl das fast nie zutrifft. Häufig erlaubt die DSGVO lediglich, dass er „spezifischere Vorschriften" vorsehen kann (so etwa in Art. 88 Abs. 1 DSGVO, der die „Datenverarbeitung im Beschäftigungskontext" regelt).

„Kollisionsregelung" im BDSG-neu

Es bedarf nur geringer Fantasie, dass im Einzelfall sehr schnell Streit darüber entstehen kann, ob eine bestimmte nationale Regelung noch als eine derartige „spezifischere Vorschrift" anzusehen ist oder ob der nationale Gesetzgeber seinen Handlungsspielraum überschritten hat.

Dieses Problem versucht das BDSG-neu dadurch zu lösen, dass es eine Art „Kollisionsregelung" trifft. Sie ist in § 1 Abs. 5 BDSG-neu enthalten und lautet: „Die Vorschriften dieses Gesetzes finden keine Anwendung, soweit das Recht der Europäischen Union, im Besonderen die Verordnung (EU) 2016/679 in der jeweiligen Fassung, unmittelbar gilt." Damit versucht der Gesetzgeber sicherzustellen, dass Regelungen des BDSG-neu nicht unzulässig in die DSGVO eingreifen.

WICHTIG

Dem Praktiker gibt diese „Kollisionregelung" allerdings Steine statt Brot. Das BDSG-neu mutet ihm zu, in Zweifelsfällen zu prüfen, ob eine bestimmte Auslegung des BDSG-neu mit dem Inhalt der DSGVO kollidiert. Sollte dies der Fall sein, darf man das BDSG-neu nicht anwenden, sondern muss der entsprechenden Regelung der DSGVO den Vorrang geben. Es liegt auf der Hand, dass der typische Praktiker eine solche Prüfung schlicht nicht leisten kann. Er muss davon ausgehen, dass das BDSG-neu nur solche Regelungen enthält, die mit der DSGVO zu vereinbaren sind. Alles andere wird er den Aufsichtsbehörden und den Gerichten überlassen.

Diese Situation trägt erhebliche Unsicherheit in den Datenschutzalltag der →

Unternehmen. Denn gerade bei wichtigen Fragen wird es anfangs unterschiedliche Meinungen dazu geben, ob einzelne Bestimmungen des BDSG-neu mit der DSGVO in Einklang stehen oder nicht.

Beispiel Beschäftigtendatenschutz

Ein gutes Beispiel für solche Zweifel bietet der neue § 26 BDSG, der laut Überschrift die „Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses" regelt. Bereits die Abweichung von der Überschrift des Art. 88 DSGVO („Datenverarbeitung im Beschäftigungskontext") wirft die Frage auf, ob § 26 BDSG-neu spezifische Regelungen für jede Art von Datenverarbeitung im Beschäftigungskontext treffen will oder ob die „Beschäftigungsverhältnisse" lediglich eine Teilmenge des „Beschäftigungskontextes" bilden.

Diese Unsicherheit wird noch dadurch verstärkt, dass § 26 Abs. 8 BDSG-neu eigenständig definiert, welche Personen als „Beschäftigte im Sinne dieses Gesetzes" anzusehen sind. Die DSGVO erwähnt den Begriff „Beschäftigte" zwar an mehreren Stellen. Beispiele hierfür bilden Art. 47 DSGVO („Verbindliche interne Datenschutzvorschriften") und Erwägungsgrund 155 (Einwilligung des Beschäftigten). Sie enthält aber keine Definition des Begriffs.

Ob man daraus ableiten kann, dass der jeweilige nationale Gesetzgeber selbst festlegen kann, wen er als Beschäftigten ansieht, ist äußerst umstritten. Falls man diese Frage bejaht, könnte es dazu kommen, dass in allen 28 Mitgliedstaaten jeweils unterschiedliche Definitionen dieses Begriffs erfolgen. Es liegt auf der Hand, dass dies mit der unmittelbaren und allgemeinen Geltung der DSGVO nicht zu vereinbaren wäre.

Insgesamt gesehen bleibt somit gerade bei der wichtigen Frage des Datenschutzes bei Beschäftigungsverhältnissen offen, ob der Bundesgesetzgeber über den Spielraum hinausgegangen ist, den ihm die DSGVO insoweit gibt.

Besonderer Schutz für DSBs

Wie steht es um den Kündigungsschutz?

Schwierig wird es bei der Frage, ob das BDSG-neu für den Datenschutzbeauftragten einen besonderen Kündigungsschutz vorsehen darf. Dies hat das BDSG-neu in Form einer relativ schwer lesbaren Verweiskette getan: § 38 Abs. 2 Halbsatz 1 BDSG-neu verweist auf § 6 Abs. 4 Satz 2 BDSG-neu, der einen besonderen Kündigungsschutz vorsieht (Stichwort: „Kündigung nur aus wichtigem Grund").

Das Problem: Ausdrücklich zum Kündigungsschutz sagt die DSGVO zwar nichts. Sie enthält jedoch in Art. 38 Abs. 3 Satz 2 folgende Regelung: „Der Datenschutzbeauftragte darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden." Es ist umstritten, ob aus dem Verbot der Abberufung auch ein besonderer Kündigungsschutz für den Datenschutzbeauftragten abzuleiten ist oder gerade nicht.

- Träfe die erste Interpretation zu, würde eine entsprechende nationale Regelung die DSGVO in unnötiger (und auch unzulässiger) Weise wiederholen.
- Träfe dagegen die zweite Interpretation zu, stellt sich die Frage, ob der nationale Gesetzgeber einen besonderen Kündigungsschutz festlegen darf, den die DSGVO nicht vorsieht.

Schwierige Kompetenzfragen

Die Angelegenheit wird noch komplizierter, wenn man die Frage stellt, ob der Kündigungsschutz des Datenschutzbeauftragten überhaupt zu den Themen gehört, die die DSGVO regeln kann, oder ob es sich dabei um eine rein arbeitsrechtliche Frage handelt, die überhaupt nicht zum Thema „Datenschutz" gehört. Ob ein Datenschutzbeauftragter einen besonderen Kündigungsschutz genießt oder nicht, wird bei dieser schwierigen Gemengelage abschließend erst der Europäische Gerichtshof klären können. Dabei kann es Jahre dauern, bis ein derartiger Fall zu ihm gelangt.

Bestellung eines Datenschutzbeauftragten

Bei anderen Regelungen herrscht größere Klarheit. So steht außer Frage, dass der nationale Gesetzgeber ergänzende Regelungen dazu treffen kann, wann nicht-öffentliche Stellen (und damit insbesondere Unternehmen der Privatwirtschaft) einen Datenschutzbeauftragten benennen müssen. Das hat das BDSG-neu in § 38 Abs. 1 getan. Diese Regelung tritt neben Art. 37 Abs. 1 DSGVO.

Soweit Unternehmen bereits von dieser Bestimmung erfasst werden – etwa weil sich ihre Kerntätigkeit auf Gesundheitsdaten bezieht, siehe Art. 37 Abs. 1 Buchst. c DSGVO –, spielt § 38 Abs. 1 BDSG daneben keinerlei Rolle. Wichtig ist die Regelung dagegen für Unternehmen, für die Art 37 Abs. 1 DSGVO nicht gilt, und das sind zahlenmäßig relativ viele. Für sie ergibt sich die Pflicht zur Bestellung eines Datenschutzbeauftragten erst aus dem BDSG-neu.

Ergänzende Bußgeldtatbestände

Einige wichtige Ergänzungen zur DSGVO enthält das BDSG-neu im Bereich der Sanktionen. Die DSGVO selbst sieht in Art. 83 Abs. 4 und Abs. 5 eine Reihe von Bußgeldtatbeständen vor. Zusätzlich gibt sie jedoch den Mitgliedstaaten den Auftrag, Sanktionen für Verstöße festzulegen, die in ihr selbst nicht geregelt sind (siehe Art. 84 Abs. 1 DSGVO). Das hat das BDSG-neu

in § 43 für sehr spezielle Fälle getan, nämlich für Verstöße im Zusammenhang mit Verbraucherkrediten (§ 30 BDSG-neu).

Wichtige neue Strafvorschriften

Deutlich wichtiger sind die Strafvorschriften in § 42 BDSG-neu. Die Europäische Union hat normalerweise keine Befugnis, Strafvorschriften vorzusehen. Deshalb hält Erwägungsgrund 149 Satz 1 fest, dass es Sache der Mitgliedstaaten ist, strafrechtliche Sanktionen festzulegen.

PRAXIS-TIPP

Die Strafvorschriften in § 42 BDSG-neu können erhebliche praktische Bedeutung erlangen. Sie greifen beispielsweise dann ein, wenn es um Daten einer „großen Zahl von Personen" geht, die in gewerbsmäßiger Weise unzulässig an einen Dritten übermittelt werden. Dafür ist eine Freiheitsstrafe bis zu drei Jahren vorgesehen (siehe § 42 Abs. 1 BDSG-neu). Was genau unter einer „großen Zahl von Personen" zu verstehen ist, definiert das BDSG-neu nicht. Das werden Gerichte entscheiden.

Keine Bußgelder gegenüber Behörden und öffentlichen Stellen

Jeder Mitgliedstaat kann selbst festlegen, ob gegenüber Behörden und öffentlichen Stellen Bußgelder verhängt werden können (siehe Art. 83 Abs. 7 DSGVO). § 43 Abs. 3 BDSG-neu schließt diese Möglichkeit vom Grundsatz her aus. Dabei ist allerdings eine wichtige Ausnahme zu beachten, bei der auch gegen eine öffentliche Stelle eine Geldbuße verhängt werden kann. Sie betrifft sogenannte „Wettbewerbsunternehmen".

Besonderheiten für Wettbewerbsunternehmen

Welche öffentlichen Stellen zu den Wettbewerbsunternehmen zählen, ist in § 2 Abs. 5 BDSG-neu geregelt. Für sie schließt § 43 Abs. 3 BDSG Bußgelder nicht aus. Er verweist nämlich für die Definition der öffentlichen Stellen lediglich auf die „gewöhnlichen" öffentlichen Stellen, die in § 2 Abs. 1 BDSG-neu definiert sind. Das hat große Bedeutung beispielsweise für Krankenhäuser. Sie sind in der Regel Unternehmen, die im Wettbewerb stehen. Damit sind gegen sie auch dann Bußgelder möglich, wenn sie von der Rechtsform her öffentliche Stellen sind.

Fazit: Neue Auslegungsfragen

Die Grundverordnung enthält manche Unklarheiten. Optimisten hatten gehofft, dass das BDSG-neu hier zumindest in manchen Punkten weiterhilft. Letztlich ist das Gegenteil eingetreten. Das BDSG-neu führt zu neuen Auslegungsfragen.

Dr. Eugen Ehmann ist Regierungsvizepräsident von Mittelfranken (Bayern) und Mitherausgeber eines neuen Kommentars zur Grundverordnung.

Drucksachen statt Bundesgesetzblatt

Bei Redaktionsschluss (15.05.2017) war das DSAnpUG-EU noch nicht im Bundesgesetzblatt veröffentlicht. Wer seinen genauen Inhalt feststellen will, muss deshalb einstweilen auf die entsprechenden Drucksachen von Bundestag und Bundesrat zurückgreifen. Das sind v.a.:

- **Bundestags-Drucksache 18/11325 vom 24. Februar 2017 (Gesetzentwurf der Bundesregierung)**
- **Bundesrats-Drucksache 332/17 vom 28. April 2017 (Änderung des Bundestags am ursprünglichen Gesetzentwurf der Bundesregierung).**

Beibehalten wurde die schwer verständliche Gliederungsstruktur des DSAnpUG-EU. Sie ist erläutert in Datenschutz PRAXIS 01/17, Seite 1.

IMPRESSUM

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

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

Geschäftsführer:
Stephan Behrens, Michael Bruns, Werner Pehland

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

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

Erscheinungsweise:
Zwölfmal pro Jahr

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

Abonnementpreis:
12 Ausgaben 189,00 €
(zzgl. MwSt. und Versandkosten)
Einzelheft 17 €
(zzgl. MwSt. und Versandkosten)

Druck:
Geiselmann Printkommunikation GmbH
Leonhardstraße 23, 88471 Laupheim

Layout & Satz:
punktneun | Grafikdesign & Webdesign
München

Bestell-Nr.:
09100-4042

ISSN-Nr.:
1614-6867

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

Eine (fast) wahre Geschichte

Folgenabschätzung für die Keksdose

Reinigungskräfte finden bei ihrer Arbeit im Großraumbüro im Benjamini einen Gegenstand, Größe ca. 2 x 2 cm. Der Vorgesetzte erkennt eine Webcam mit Funkübertragung. Wer hat die Kamera angebracht?

Die Gerüchteküche beginnt zu brodeln, das Thema eskaliert immer weiter. Der Betriebsrat wird aktiv: „Wieso werden im Großraumbüro die Kolleginnen und Kollegen ausspioniert?" Die Geschäftsführung versichert glaubhaft, keine Ahnung zu haben.

Der Datenschutzbeauftragte wird einbezogen. Müssen wir die Aufsichtsbehörde informieren? Sind Spione am Werk? Der DSB schreitet schließlich zusammen mit der Reinigungskraft zur Tatortbesichtigung.

Was war geschehen?

Kollege Hungerhaken hat eine Keksdose mit hochwertigen Keksen für das 11-Uhr-Loch an seinem Arbeitsplatz stehen. Zu seinem Ärger stellt er fest, dass der Inhalt der Keksdose schneller abnimmt, als er selbst Kekse isst. Irgendwer futtert offenkundig mit. Bloß wer?

Sein Gegenüber schlägt ihm vor, eine kleine Funkwebcam aufzuhängen, um den dreisten Keksdieb zu fassen. Bevor das jedoch gelingt, wird die Kamera entdeckt.

Die Auflösung

Der Datenschutzbeauftragte stellt fest, dass es sich bei der Keksdose und bei der Webcam um private Gegenstände handelt. Da weder die Geschäftsleitung eingebunden war noch eine offizielle Videoüberwachung vorlag, beschließt der DSB, dies als rein private Datenverarbeitung einzuordnen. Die fällt ja bekanntlich nicht unter das Datenschutzrecht.

Aus seinem Budget kauft der DSB mit Genehmigung der Geschäftsführung eine neue Keksdose, nimmt vor Ort eine Datenschutz-Unterweisung zur erlaubten und nicht erlaubten Videoüberwachung vor und lässt die Dose dabei herumgehen. Die Folgen für die Keksdose lassen sich leicht abschätzen: Sie wird immer leerer.

Übrigens: Der Übeltäter war der Auszubildende, der sich schließlich beim – schweigepflichtigen – DSB meldete. Kollege Hungerhaken hatte dem immer hungrigen jungen Mann einst erlaubt, sich bei seinen Keksen zu bedienen. Und: Die Funk-Webcam hat zu keiner Zeit funktioniert.

Eberhard Häcker wird an dieser Stelle zukünftig regelmäßig über bemerkenswerte Fälle aus seinem reichen Erfahrungsschatz als externer DSB berichten.

IN DER NÄCHSTEN AUSGABE

Identitätsdiebstahl

„Mit meinem Geburtstagsdatum kann niemand etwas anfangen" – auch schon einmal gehört? Weit gefehlt!

Tools zur Grundverordnung

Wir stellen spezielle Tools vor, die dabei helfen, bestehende Lücken in der Umsetzung der DSGVO zu schließen.

So lesen Sie ein EuGH-Urteil

Der Europäische Gerichtshof wird entscheiden, wie die DSGVO auszulegen ist. Seine Urteile sind also für Sie wichtig.