VERLAG des wissenschaftlichen Instituts der Steuerberater GmbH

Merkblatt 9 | 2017

Nr. 1811.1

Datenschutz im Unternehmen

Inhalt

1. Vorbemerkung

Seit 25.05.2016 ist die **EU-Datenschutz-Grundverordnung (DS-GVO)** in Kraft. Noch befinden wir uns in einer zweijährigen Übergangszeit, die den Unternehmen die Gelegenheit geben soll, ihre Prozesse an die neuen Gegebenheiten anzupassen. Im Gegensatz zur bisherigen Datenschutz-Richtlinie aus dem Jahr 1995, die erst nach der Umsetzung in nationales Recht auch national Anwendung fand, gilt die DS-GVO unmittelbar in allen Mitgliedstaaten ab dem 25.05.2018.

Bereits das Bundesdatenschutzgesetz in der bisherigen Form legt einem Unternehmen umfangreiche Pflichten im Bereich Datenschutz auf. Es gilt, das **„Grundrecht auf informationelle Selbstbestimmung“** sicher zu stellen und die **Daten der Betroffenen** (Kunden, Mitarbeiter, Mitglieder, Geschäftspartner etc.) **vor Missbrauch zu schützen.** Unternehmen mit mehr als neun Mitarbeitern, die ständig personenbezogene Daten verarbeiten, haben deshalb die Pflicht, einen Datenschutzbeauftragten (DSB) zu bestellen. Zu diesem Personenkreis gehören neben der Geschäftsleitung u. a. Mitarbeiter aus den Bereichen Personal, Marketing, Vertrieb und IT. Diese Bestellpflicht gilt in gleicher Weise für Vereine und Organisationen, in denen mehr als neun Personen beispielsweise Zugriff auf Daten von Mitgliedern oder Angehörigen der jeweiligen Organisation haben. Verarbeiten in einem Unternehmen weniger als zehn Mitarbeiter regelmäßig personenbezogene Daten, liegt die Umsetzung sämtlicher datenschutzrelevanter Themen in den Händen der Geschäftsleitung.

Aus Gründen der besseren Lesbarkeit, wird im folgenden Text in der Regel vom „Unternehmen“ oder vom „Verantwortlichen“ gesprochen, wobei hiermit natürlich auch Vereine, Verbände und sonstige Organisationen adressiert sind. Dieses Merkblatt soll kleine und mittlere Unternehmen und Vereine informieren, damit diese ihre Organisation und Prozesse rechtzeitig an die neue Rechtslage anpassen können.

2. Datenschutzrelevante Themen

Die Themen im Datenschutzmanagement reichen vom datenschutzkonformen Internetauftritt über die Kontrolle der Dienstleister, die Beschreibung und Bewertung sämtlicher datenschutzrelevanter

Prozesse im Unternehmen bis hin zur Sensibilisierung der Mitarbeiter. Es gab und gibt viel zu tun für den DSB, denn Datenschutz wird oft vernachlässigt. Das Gefährdungspotenzial steigt jedoch durch die moderne Technik stetig an (jederzeitige Verfügbarkeit von Daten, leichtes Erstellen von Profilen und Querverbindungen etc.).

3. Die DS-GVO und das Bundesdatenschutzgesetz (BDSG)

Seit 25.05.2016 hat sich die Datenschutzwelt grundlegend geändert. Die DS-GVO wird weitreichende Auswirkungen auf nahezu alle Unternehmen in Europa haben. Ab 25.05.2018 sind in Deutschland sowohl deren Vorgaben, als auch die Vorgaben des BDSG-neu zu beachten. Dieses Gesetz wurde am 05.07.2017 mit dem „Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU)“ im Bundesgesetzblatt veröffentlicht und wird auch weiterhin die Bezeichnung „Bundesdatenschutzgesetz“ (BDSG) innehaben. Alle Entscheidungsträger sollten sich der Auswirkungen der DS-GVO bewusst sein und wissen, was diese für den Alltag in ihrem Unternehmen bedeutet.

Betrachten wir zunächst die Vorgaben aus Europa.

Die DS-GVO

- regelt das Recht auf **Schutz personenbezogener Daten** als **Grundrecht** innerhalb der EU,
- vereinheitlicht weitgehend die derzeit bestehenden 28 nationalen Gesetze innerhalb der EU,
- **erhöht die Sanktionen** drastisch (bis zu 10/20 Mio. € bzw. 2/4 % des weltweiten Jahresumsatzes),
- wird durch die Aufsichtsbehörden voraussichtlich wesentlich **strenger sanktioniert** als das bisher der Fall war,
- beinhaltet eine **Meldepflicht** innerhalb von **72 Stunden** und eine **Beweislastumkehr**,
- setzt wesentlich mehr an Dokumentation voraus als das BDSG-alt,
- bringt neue Aspekte wie **privacy by design & default, Rechenschaftspflicht, Risikobewertung**,
- **tritt mit 25.05.2018 EU-weit in Kraft.**

Das BDSG-neu regelt die Punkte, welche die DS-GVO im Rahmen sog. Öffnungsklauseln den Mitgliedsstaaten überlässt, unter anderem die **Bestellung eines DSB,** wenn in der Regel **mindestens zehn Personen ständig personenbezogene Daten verarbeiten.** Im Zweifel gehen stets die Regelungen der DS-GVO denen des BDSG vor.

Soweit zu einigen Eckdaten. Mit Gelten der DS-GVO gibt es jedoch noch zahlreiche weitere und teils neue Aspekte zu beachten. Zwar entfällt die Pflicht, wie bislang gefordert ein sog. „Jedermannverzeichnis“ vorzuhalten, doch muss das Unternehmen bei jeder Erhebung personenbezogener Daten dem Betroffenen nun umfangreiche Informationen zur Verfügung stellen. Dies reicht von den Datenkategorien, die im Unternehmen verarbeitet werden, über Informationen zur Geschäftsleitung und zum DSB bis hin zum Widerspruchsrecht und zur Datenschutzaufsichtsbehörde, bei der sich der Betroffene beschweren könnte, wenn er einen rechtswidrigen Umgang mit seinen Daten befürchtet.

Waren Datenpannen bislang an Aufsichtsbehörde und Betroffene zu melden, wenn sensible Daten, wie z. B. Gesundheitsdaten oder Bank-/Kreditkartendaten natürlicher Personen betroffen waren, so gilt die Meldepflicht zukünftig für nahezu alle personenbezogenen Daten, wobei die Meldefrist auf 72 Stunden verkürzt wurde.

Das Verfahrensverzeichnis, zukünftig „Verzeichnis der Verarbeitungstätigkeiten“, in dem jeder einzelne personenbezogene Daten verarbeitende Prozess im Unternehmen beschrieben ist, ist um eine Risikobewertung zu ergänzen. Ggf. ist zudem noch eine sog. „Datenschutz-Folgenabschätzung“ erforderlich.

Die Schulung und Sensibilisierung der Mitarbeiter bleibt auch weiterhin unerlässlich.

Auf den DSB kommt künftig zusätzlich noch eine verstärkte Überwachungspflicht hinsichtlich der Einhaltung der Regelungen aus DS-GVO, BDSG-neu und interner Richtlinien zu.

Das Unternehmen unterliegt nun einer „Rechenschaftspflicht“ und muss im Falle einer Datenschutz- oder Datensicherheitspanne sowie einer Kontrolle durch die Aufsichtsbehörde nachweisen können, welche Maßnahmen implementiert wurden, um Pannen zu verhindern. Hierdurch kommen auch weitere Anforderungen bzgl. der Dokumentation der IT-Infrastuktur und der IT-Sicherheitsmaßnahmen auf das Unternehmen zu. Sollte dennoch etwas passieren, sieht die DS-GVO empfindliche Bußgelder bis zu 20 Millionen € oder 4 % des weltweiten Jahresumsatzes vor.

Fasst man die Grundsätze der DS-GVO zusammen, so handelt es sich um:

- Rechtmäßigkeit der Datenverarbeitung,
- Verarbeitung nach Treu und Glauben und Transparenz,
- Zweckbindung,
- Datensparsamkeit und Speicherbegrenzung,
- Richtigkeit und Aktualität,
- Integrität und Vertraulichkeit sowie
- unabhängige Kontrolle.

Auf die Punkte Rechtmäßigkeit der Verarbeitung und die individuellen Datenschutzrechte wird an dieser Stelle besonders eingegangen.

4. Grundsätze der DS-GVO und des BDSG-neu

4.1 Rechtmäßigkeit der Verarbeitung

4.1.1 Einwilligung

Die DS-GVO rückt die **Einwilligung der Betroffenen** stärker in den Fokus, als das BDSG-alt. Immer dann, wenn keine Rechtsgrundlage vorhanden ist, muss der Betroffene seine Einwilligung ausdrücklich erklären. Der Betroffene muss stets in der Lage sein, seine Einwilligung zu verweigern oder zu widerrufen, ohne dabei Nachteile zu erleiden. Auf Betreiben des Europäischen Parlaments wurde zusätzlich ein sog. **„Kopplungsverbot"** mit in die DS-GVO aufgenommen. Dies soll verhindern, dass Betroffene Angebote im Internet nur dann nutzen können, wenn sie hierbei Daten von sich preisgeben, die für die Nutzung des entsprechenden Dienstes nicht erforderlich sind. Die Wirksamkeit einer Einwilligung hängt zudem davon ab, dass der Betroffene sie **„informiert"** erteilt. Aus diesem Grund muss im Zuge der Einwilligung darüber informiert werden, wer der **Verantwortliche** ist und zu welchem **Zweck** die Einwilligung erfolgt. Werden im Zuge einer solchen Einwilligung erstmals personenbezogene Daten von Betroffenen erhoben, so gilt es noch weitere Angaben zu machen, auf die wir unter 4.2.1 (Information) eingehen werden. Die Einwilligung selbst muss in **leichter und verständlicher Sprache** verfasst sein. Die Schriftform ist im Grunde nicht gefordert, der Verantwortliche muss aber im Zuge seiner Rechenschaftspflicht nachweisen können, dass eine Einwilligung vorliegt. Neben dem bereits etablierten Verfahren „Double-Opt-In" bei Einwilligungen in den Newsletter-Bezug gibt es jedoch derzeit im Grunde keine Alternativen zur Schriftform.

Für die Einwilligung von Kindern gelten spezielle Regelungen, wobei die DS-GVO hier eine Altersgrenze von 16 Jahren vorsieht. Diese Grenze kann von den Mitgliedsstaaten auf bis zu 13 Jahre herabgesenkt werden, wovon Deutschland allerdings keinen Gebrauch gemacht hat. Dies bezieht sich jedoch nicht auf Einwilligungen im beruflichen oder gewerblichen Bereich, sondern auf Einwilligungen bei einem **Angebot von Diensten der Informationsgesellschaft**, z. B. soziale Netzwerke, Chats oder Online-Foren. Bei der Einholung der Einwilligung eines Kindes muss der Verantwortliche zudem nachweisen, dass er als **Diensteanbieter „angemessene Anstrengungen"** unternommen hat, um sich der Einwilligung durch den Träger der elterlichen Verantwortung zu vergewissern. Es ist zu erwarten, dass sich in der Praxis noch viele Fragen stellen werden, insbesondere wann ein Diensteanbieter beispielsweise „angemessene Anstrengungen" unternommen hat.

Bereits erteilte Einwilligungen gelten fort, wenn sie DS-GVO-konform erteilt wurden.

Praxistipp: Unternehmen sind gut beraten, ihre Prozesse bzgl. des Einholens von Einwilligungen zu überprüfen; insbesondere im Zusammenhang mit Mailings, Newslettern, Gewinnspielen und Messeauftritten. Vergessen Sie nicht, die Anmeldung zum Newsletter-Bezug datenschutzkonform zu gestalten („Double-Opt-In"-Verfahren). Beim „Double-Opt-In" muss die Eintragung in eine Newsletter-Abonnentenliste in einem zweiten Schritt (deshalb Double) bestätigt werden. Hierzu wird in der Regel eine E-Mail-Nachricht mit Bitte um Bestätigung an die eingetragene E-Mail-Adresse gesendet. Die Registrierung beim „Double-Opt-in" erfolgt erst dann, wenn sie mit dieser E-Mail bestätigt wird. Dieses Verfahren hat sich mittlerweile im E-Mail-Marketing in Deutschland durchgesetzt. Denken Sie auch an Datenerhebungen im Rahmen von Tracking der Besucher des Internetauftritts oder Mitschnitten von Chats oder Hotlineanrufen! Als Tracking bezeichnet man die Technik mit der das Nutzerverhalten im Internet analysiert werden kann. Dafür gibt es spezielle Tracking-Tools, wie z. B. Google Analytics. In der Regel nutzt man hierfür Cookies oder Zählpixel. Neuerdings bedient man sich aber auch Ultraschalltönen, die von Smartphones empfangen werden können. Oftmals haben deren Besitzer beim Download einer (meist kostenlosen) App die Datenschutzhinweise gar nicht gelesen, in denen der Zugriff der App auf Mikrofon und Nutzerverhalten erlaubt wurde.

4.1.2 Weitere Verarbeitungsgrundlagen

Die DS-GVO erlaubt Datenverarbeitungen, die auf der **Erfüllung eines Vertrages** oder eines **vorvertraglichen Schuldverhältnisses** beruhen. Entscheidend hierbei ist, dass die Erhebung der Daten für die Erfüllung des Vertrages erforderlich ist. Die Erhebung weiterer Daten auf Grundlage einer Einwilligung dürfte vor dem Hintergrund des oben bereits erwähnten „Kopplungsverbotes" problematisch werden. Es gibt jedoch Spielräume zur Gestaltung von Vertragsverhältnissen, in denen Nutzer mit ihren Daten bezahlen, was gerade bei kostenlosen Apps oftmals der Fall ist. Hier setzt die DS-GVO zwar enge Grenzen, es sind jedoch Modelle denkbar, in denen man „Bezahl-Alternativen" anbietet. Bei der Gestaltung solcher Modelle sind Unternehmen jedoch stets gut beraten, sich Unterstützung durch externe Fachleute und ggf. auch juristische Beratung einzuholen.

Im **Beschäftigungskontext** kommen verstärkt die Regelungen des BDSG-neu zum Tragen, da die DS-GVO hier eine Öffnungsklausel vorsieht. Beim Einholen von Einwilligungen im Beschäftigungskontext, ein Klassiker ist die **Einwilligung in die Veröffentlichung eines Mitarbeiterfotos** auf der Homepage, ist besondere Sorgfalt geboten. Hier wird die Freiwilligkeit der Einwilligung aufgrund des **wirtschaftlichen Abhängigkeitsverhältnisses** oftmals in Frage gestellt. Vor diesem Hintergrund ist es wichtig, die Einwilligungen datenschutzkonform und für den Mitarbeiter transparent zu gestalten und ihm ein Widerrufsrecht einzuräumen. Gerade für die Beendigung des Arbeitsverhältnisses sollten entsprechende Regelungen bezüglich der Entfernung der Bilder von der Homepage getroffen werden. Einwilligungen für die Veröffentlichung von Mitarbeiterbildern in sozialen Netzwerken sind etwas komplizierter zu gestalten, aber durch den DSB mit Sicherheit zu regeln. Hier

müssen weitergehende Vereinbarungen getroffen werden. An dieser Stelle sei auch angemerkt, dass eine **Social Media Guideline** heutzutage fast unvermeidbar ist, wenn man von den Mitarbeitern einerseits Engagement in sozialen Netzwerken in beruflichem Interesse erwartet, andererseits aber auch im Privatleben eine gewisse **„Netikette"** einfordert.

Im Grunde muss für jede Verarbeitung personenbezogener Daten eine Rechtsgrundlage vorhanden sein. Auch die DS-GVO setzt somit die Tradition des sog. **„Verbots mit Erlaubnisvorbehalt"** fort, sprich die Verarbeitung personenbezogener Daten ist grundsätzlich verboten, es sei denn, es gibt eine Rechtsgrundlage, welche diese gestattet.

Viele Unternehmen stützen die Verarbeitung personenbezogener Daten auf das sog. **„berechtigte Interesse"**, sprich sie treffen eine Interessenabwägung zwischen den Belangen des Unternehmens und den Interessen der Betroffenen. Im Grunde kommt es hierbei darauf an, dass der Betroffene aufgrund seiner Beziehung zum Verantwortlichen mit der Verarbeitung seiner Daten rechnen kann. Auch die Bekämpfung von Betrug kann beispielsweise ein solches berechtigtes Interesse darstellen. Bei der Bewertung solcher Prozesse sollte in jedem Fall der DSB oder ein externer Experte zu Rate gezogen werden. Für eine **Weiterverarbeitung** von personenbezogenen Daten muss stets hinterfragt werden, ob die Verarbeitung noch für den ursprünglichen Zweck erfolgt.

Praxistipp: Überprüfen Sie alle Prozesse, in denen personenbezogene Daten verarbeitet werden, auf die jeweilige Rechtsgrundlage. Sind weitere Einwilligungen erforderlich? Brauchen Sie eine Social Media Guideline?

4.1.3 Sensible Daten

Die DS-GVO sieht für bestimmte Daten besondere Regelungen vor. Betrachten wir zunächst die „besonderen Kategorien personenbezogener Daten", die wir noch aus dem BDSG-alt kennen. Hierzu gehören Gesundheitsdaten, rassische und ethnische Herkunft, Gewerkschaftszugehörigkeit, Sexualleben und sexuelle Orientierung, weltanschauliche Überzeugung und politische Meinung. Auch die Verarbeitung von personenbezogenen Daten über strafrechtliche Verfolgung und Straftaten unterliegen besonderen Auflagen. Gerade die „besonderen Kategorien personenbezogener Daten" kommen im Grunde in jeder Personalabteilung vor, je nach Branche oder Geschäftsmodell aber auch in Kunden- oder Interessentendatenbanken.

Praxistipp: Prozesse, in denen solche Datenbestände vorhanden sind, sind im Verzeichnis der Verarbeitungstätigkeiten eindeutig zu kennzeichnen. Diese Prozesse müssen einem besonderen Schutz unterliegen. Ggf. muss für diese Prozesse eine Datenschutz-Folgenabschätzung durchgeführt werden.

4.1.4 Risikobewertung und Datenschutz-Folgenabschätzung

Jeder Prozess im Unternehmen, in dem personenbezogene Daten verarbeitet werden, ist hinsichtlich des damit verbundenen Risikos für den Betroffenen zu bewerten. Das Risiko für das Unternehmen (Bußgeld oder Kosten für IT-Experten nach Befall mit Schadsoftware) spielt dabei keine Rolle. Es geht einzig und allein darum, welche Konsequenzen für den Betroffenen zu befürchten sind, wenn seine Daten offenbart werden. Potenzielle Schäden können physischer, materieller oder immaterieller Art sein. Die DS-GVO benennt hier beispielhaft Diskriminierung, Identitätsdiebstahl, finanzielle Verluste, Rufschädigung, Verlust der Vertraulichkeit oder einen Verstoß gegen das Berufsgeheimnis. Die Risikobewertung betrachtet hierbei die Eintrittswahrscheinlichkeit sowie die Schwere des Risikos. Die ermittelten Risiken müssen dann durch geeignete Abhilfemaßnahmen (insbesondere durch technisch-organisatorische Maßnahmen) eingedämmt werden. Führt eine Datenverarbeitung dennoch weiter zu einem hohen Risiko für den Betroffenen, so hat das Unternehmen eine sog. Datenschutz-Folgenabschätzung vorzunehmen. Hierbei ist stets der Rat des DSB einzuholen, sofern ein solcher benannt wurde.

Eine solche Bewertung wird weder die Geschäftsleitung noch der DSB alleine bewerkstelligen können, sondern es wird ein Team verschiedenster Mitarbeiter (IT-Sicherheit, Compliance, ggf. auch Vertreter von Dienstleistern) erforderlich sein. Die DS-GVO sieht vor, dass die Datenschutzaufsichtsbehörden eine Liste der Verarbeitungsvorgänge veröffentlichen, bei denen eine solche Datenschutz-Folgenabschätzung erforderlich ist.

Praxistipp: Verschaffen Sie sich möglichst schnell und umfassend einen Überblick über alle Prozesse im Unternehmen, in denen personenbezogene Daten verarbeitet werden! Stellen Sie für jeden Prozess die Schutzmaßnahmen dar. Mehr dazu beim Verzeichnis der Verarbeitungstätigkeiten.

4.2 Individuelle Datenschutzrechte

4.2.1 Information

Der Verantwortliche hat den Betroffenen bei jeder Datenverarbeitung von sich aus aktiv zu informieren. Der Betroffene muss auch wissen, was passiert, wenn er seine Daten nicht preisgibt. Zur den erforderlichen Informationen gehören der Zweck der Datenverarbeitung, die Kontaktdaten des Verantwortlichen, die Kontaktdaten des DSB (sofern vorhanden), ggf. die berechtigten Interessen, auf deren Grundlage die Datenverarbeitung erfolgt, die Empfänger oder Kategorien von Empfängern und (falls geplant) eine Übermittlung in Drittstaaten (außerhalb der EU/des EWR). Hinzu kommt die Dauer der Datenspeicherung, das Recht auf Auskunft und Widerruf und das Bestehen eines Beschwerderechts bei der Aufsichtsbehörde. Falls im Zuge der Datenverarbeitung

eine automatisierte Entscheidungsfindung stattfindet, so ist der Betroffene auch über die involvierte Logik und die Tragweite bzw. die Auswirkungen dieser Entscheidung zu informieren. Beabsichtigt ein Unternehmen beispielsweise, im Zuge einer Veranstaltung ein Gewinnspiel durchzuführen, so wird es nicht umhinkommen, im Rahmen der Einwilligung diese Informationen zur Verfügung zu stellen.

Praxistipp: Prüfen Sie, an welchen Stellen im Unternehmen personenbezogene Daten erhoben werden – Personalfragebogen bei Einstellung, Kundendaten bei Verträgen, Gewinnspiele bei Messen, Aufnahme von Interessenten oder Tracking im Rahmen des Internetauftritts usw. Tragen Sie die erforderlichen Informationen zusammen, um Ihre Datenschutzerklärungen nach den Vorgaben der DS-GVO zu gestalten!

4.2.2 Auskunft

Ein Betroffener kann jederzeit Auskunft darüber verlangen, ob ein Unternehmen Daten zu seiner Person verarbeitet. Ist dies der Fall, so hat der Betroffene ein Recht zu erfahren, welche Kategorien von Daten zu welchem Zweck verarbeitet werden, an wen diese weitergeleitet werden und wie lange sie gespeichert werden. Er ist darüber in Kenntnis zu setzen, dass er ein Recht auf Berichtigung und Löschung bzw. Einschränkung der Verarbeitung dieser Daten hat. Des Weiteren ist er darauf hinzuweisen, dass er ein Recht zur Beschwerde bei einer Aufsichtsbehörde hat. Falls die Daten nicht beim Betroffenen selbst erhoben wurden, ist ihm Auskunft über deren Herkunft zu geben. Ebenfalls hat er wie bei der Information (vgl. 4.2.1) das Recht, über evtl. automatisierte Entscheidungsfindungen informiert zu werden. Werden durch den Verantwortlichen Daten des Betroffenen in ein Drittland oder an internationale Organisationen übermittelt, so ist er über die in diesem Zusammenhang bestehenden Garantien bei der Übermittlung zu informieren. Gerade bei internationalen Verbänden (Sportverbände oder gemeinnützige Organisationen) ist eine solche Übermittlung regelmäßig der Fall. Dem Betroffenen ist auf Verlangen auch eine kostenfreie Kopie dieser Daten auszuhändigen. Die Auskunft ist dem Betroffenen unverzüglich zu erteilen, spätestens jedoch innerhalb eines Monats.

Praxistipp: Überprüfen Sie, ob Sie in der Lage sind, in den datenverarbeitenden Prozessen in Ihrem Unternehmen die Daten einer Person schnell und umfassend zu ermitteln. Legen Sie fest, wer im Unternehmen für Auskunftsanfragen von Betroffenen zuständig ist und informieren Sie Ihre Mitarbeiter über diese Vorgaben, sodass diese bei Anfragen professionell reagieren.

4.2.3 Berichtigung und Löschung („Recht auf Vergessenwerden")

Ein Betroffener hat das Recht, die Berichtigung oder Vervollständigung seiner Daten zu verlangen, wenn diese unrichtig oder unvollständig im Unternehmen gespeichert wurden.

Wenn die Daten eines Betroffenen im Unternehmen nicht mehr erforderlich sind und es keine weitere Rechtsgrundlage für die Speicherung mehr gibt (was z. B. bei steuerrelevanten Daten in der Regel für zehn Jahre der Fall ist), so sind diese zu löschen. Dies ist auch beim Widerruf einer Einwilligung der Fall oder wenn Daten unrechtmäßig verarbeitet wurden.

Dieses Recht kann mitunter in der Umsetzung komplex sein, so etwa wenn bereits weitere Stellen auf Veröffentlichungen des Verantwortlichen verwiesen oder verlinkt haben. Auch wenn Datenbestände revisionssicher archiviert wurden oder in Backups enthalten sind, ist eine Löschung in der Praxis nahezu ausgeschlossen, bzw. die Kosten stünden in keinem Verhältnis zum Nutzen. In diesen Situationen tritt an die Stelle der Löschung die Einschränkung der Verarbeitung, im BDSG-alt als Sperrung bezeichnet.

Oftmals vernachlässigt wird das Thema „Bewerbungen". Abgelehnte Bewerber haben ein „Recht auf Vergessenwerden", es sei denn das Unternehmen hat eine Einwilligung für die weitere Speicherung eingeholt. Eine Speicherung von drei bis vier Monaten erscheint vor dem Hintergrund der zweimonatigen Verjährungsfrist im Allgemeinen Gleichbehandlungsgesetz (AGG) vertretbar.

Praxistipp: Überprüfen Sie regelmäßig die Rechtsgrundlagen für die Speicherung personenbezogener Daten im Unternehmen!

4.2.4 Recht auf Datenübertragbarkeit

Ursprünglich für soziale Netzwerke gedacht, gilt das Recht auf Datenübertragbarkeit nunmehr für alle Daten, die ein Verantwortlicher gespeichert hat. Der Betroffene hat das Recht, seine Daten in einem strukturierten, gängigen und maschinenlesbaren Format zu erhalten. Diese Daten können dann wiederum einem anderen Verantwortlichen zur Verfügung gestellt werden. Der Betroffene hat auch das Recht darauf, dass diese Übertragung unmittelbar zwischen zwei Verantwortlichen erfolgt. Fraglich ist, inwieweit dies mit den bislang marktüblichen Systemen realisierbar ist.

Praxistipp: Fragen Sie beim Hersteller Ihrer Softwarelösungen an, ob bereits Möglichkeiten vorhanden sind, um die Personenstammdaten und ggf. weitere Daten der Betroffenen in einem maschinenlesbaren Format zu exportieren.

4.2.5 Widerspruch

Ein Betroffener hat das Recht, der Speicherung seiner Daten zu widersprechen. Dies gilt jedoch nur, wenn keine anderen Gründe wie zum Beispiel gesetzliche Aufbewahrungsfristen oder Interessen Dritter der Löschung widersprechen. Gerade im Bereich Marketing gibt es hierzu bereits zahlreiche Regelungen, die es zu beachten gilt. So macht beispielsweise auch das Gesetz gegen den unlauteren Wettbewerb (UWG) Auflagen hinsichtlich der werblichen Ansprache. Daraus resultiert u. a. die unter 4.1.1 bereits angesprochene Forderung, bei der An-

meldung zum Newsletter-Bezug das „Double-Opt-In"-Verfahren zu nutzen.

Praxistipp: Überprüfen Sie die Notwendigkeit der in Ihrem Internetauftritt eingebundenen Tracking-Funktionen. Werden diese Auswertungen im Unternehmen genutzt? Sind diese Anwendungen in der Lage, ein „Do Not Track"-Signal des Nutzers umzusetzen?

5. Pflichten des Verantwortlichen

Viele der Pflichten eines Verantwortlichen ergeben sich aus den oben dargestellten individuellen Rechten. Hinzu kommen jedoch noch weitere Aspekte, unter anderem die Bestellung eines DSB. Diesem Thema wurde jedoch ein eigenes Kapitel gewidmet.

5.1 Privacy by Design und Privacy by Default

Mit der DS-GVO haben zwei neue Schlagworte Einzug gehalten: „Privacy by Design" (Datenschutz durch Technikgestaltung) und „Privacy by Default" (datenschutzfreundliche Voreinstellungen). Die eingesetzten Lösungen müssen u.a. grundsätzlich dazu geeignet sein, mit ihnen datenschutzkonform zu arbeiten.

Für Unternehmer heißt das, dass sie bei Investitionen in Lösungen und Technik, mit denen personenbezogene Daten verarbeitet werden, vom Hersteller eine Aussage dazu einfordern müssen, wie mit personenbezogenen Daten in diesen Lösungen umgegangen wird. Im Grunde ein neues Kriterium als Entscheidungsgrundlage.

Onlineangebote dürfen etwa keine überflüssigen Datenfelder enthalten. Voreinstellungen müssen so getroffen werden, dass z.B. Profile nicht automatisch veröffentlicht werden, oder eine Anwendung nicht automatisch Daten überträgt. Der Betroffene muss aktiv über die Nutzung der Daten bestimmen und nicht erst im Nachhinein reagieren können.

„Privacy by Design" und „Privacy by Default" waren im Grunde auch schon im BDSG-alt verankert. Die DS-GVO verleiht dieser Forderung jedoch eine neue Qualität.

Praxistipp: Überprüfen Sie Ihre Anwendungen und Unterlagen auf die Einhaltung dieser neuen Anforderungen!

Einige Beispiele: Werden Logins nach mehreren Fehleingaben gesperrt? Wird die Komplexität der Passwörter technisch erzwungen? Gibt es bei Online-Zugriffen auf sensible Daten eine Mehrfachauthentifizierung? Beinhalten Ihre Formulare unnötige Datenfelder?

5.2 Rechenschaftspflicht

Ab 25.05.2018 ist der Verantwortliche in der Nachweispflicht, die DS-GVO spricht hier von einer „Rechenschaftspflicht". Es gilt zu dokumentieren, welche Maßnahmen unternommen wurden, um den Anforderungen der DS-GVO gerecht zu werden. Erleidet ein Betroffener einen Schaden, so ist es Sache des Unternehmens nachzuweisen, dass es alle (wirtschaftlich vertretbaren) Anstrengungen unternommen hat, um diesen Schaden zu verhindern. In Zusammenhang mit der durch die DS-GVO vorgegebenen Beweislastumkehr, führt dies im Unternehmen zu einem erhöhten Dokumentationsaufwand.

5.3 Meldung von Datenpannen

Auch bisher waren Datenschutzpannen unter bestimmten Umständen an die Aufsichtsbehörde zu melden und den Betroffenen mitzuteilen. In der Regel war dies der Fall, wenn besondere Arten personenbezogener Daten, Berufsgeheimnisdaten oder Bank-/Kreditkartendaten natürlicher Personen betroffenen waren und ein schwerwiegender Schaden für die Betroffenen drohte. In der Vergangenheit führte dies in manchen Fällen gar zu Veröffentlichungen in der Presse.

Die DS-GVO senkt diese Schwelle jedoch ab. In Zukunft sind alle Datenschutzpannen an die Aufsichtsbehörde zu melden, es sei denn, dass diese Panne voraussichtlich nicht zu einem Risiko für den Betroffenen führt. Eine Benachrichtigung der betroffenen Personen muss dagegen nur dann erfolgen, wenn ein hohes Risiko für deren Rechte und Freiheiten besteht.

Während die Meldung bislang „unverzüglich"(sprich „ohne schuldhaftes Zögern") zu erfolgen hatte, was durchaus zwei Wochen dauern konnte, verkürzt die DS-GVO die maximale Zeitspanne extrem. **Die Meldung hat ab 25.05.2018 innerhalb von 72 Stunden nach Bekanntwerden der Panne zu erfolgen!**

Praxistipp: Stellen Sie sicher, dass die Meldewege in Ihrem Unternehmen funktionieren! Die Geschäftsleitung und der DSB müssen über Datenschutz- und Datensicherheitspannen umgehend informiert werden!

5.4 Verstöße (Bußgeld)

Während das BDSG-alt bislang maximale Bußgeldsummen von 50.000 €/300.000 € vorsah, sind Verstöße gegen die Vorgaben der DS-GVO mit Bußgeldern bis zu 10 Mio. €/20 Mio. € oder 2 % bzw. 4 % des weltweiten Jahresumsatzes bewehrt. Auch die Bußgeldtatbestände wurden erweitert. Diese sind zu umfangreich, um sie an dieser Stelle alle aufzuführen (siehe Artikel 83 und 84 DS-GVO). Nahezu alle in diesem Artikel angesprochenen Vorgaben sind bei Verstoß bußgeldbewehrt. Eines sollte jedoch herausgestellt werden: Nach der DS-GVO stellt der Verstoß gegen die Pflicht zur Ergreifung geeigneter und angemessener technischer und organisatorischer Maßnahmen zum Schutz personenbezogener Daten eine Ordnungswidrigkeit dar, was im BDSG-alt nicht explizit der Fall war.

Diese Bußgeldtatbestände stellen zwar ein Risiko für das Unternehmen dar, spielen aber keine Rolle für die Bewertung der Prozessrisiken im Unterneh-

men. Hierfür ist allein die Frage ausschlaggebend, welches Risiko bzw. welcher Schaden für den Betroffenen entstehen könnte.

6. Der Datenschutzbeauftragte (DSB)

Nach DS-GVO sind Unternehmen dann zur Bestellung eines DSB verpflichtet, wenn eine Kerntätigkeit mit umfangreicher oder systematischer Überwachung von Personen oder eine Kerntätigkeit mit umfangreicher Verarbeitung besonderer Kategorien von Daten vorliegt. Das BDSG-neu behält jedoch aufgrund einer Öffnungsklausel in der DS-GVO die bisherige Regelung, sodass diese drei Fallgruppen in Deutschland kaum eine Rolle spielen werden.

Unternehmen, in denen zehn oder mehr Personen regelmäßig personenbezogene Daten verarbeiten, haben die Pflicht einen DSB zu bestellen!

Gelingen kann die Einführung und Umsetzung eines Datenschutz-Managementsystems jedoch nur, wenn dieser DSB auch über die entsprechenden Kompetenzen verfügt.

6.1 Fachkompetenz

Hierzu gehört eine qualifizierte Ausbildung in zumindest einer der Kategorien Organisation und Prozesse, Informations- und Kommunikationstechnologie (IuK) oder Recht, dazu solide Grundkompetenzen in den beiden anderen Kategorien. Neben einer mindestens zweijährigen Berufserfahrung in den genannten Bereichen muss diese Person eine anerkannte Qualifikation zum DSB nachweisen.

6.2 Datenschutzrechtliche Grundkompetenzen

Im Zuge seiner Ausbildung erhält ein angehender DSB Grundkompetenzen im Datenschutzrecht. Darüber hinaus benötigt er Kenntnis der datenschutzrelevanten Vorschriften seiner Branche, was bei einer Person aus dem Unternehmen gegeben sein sollte. Auch Kenntnis des Allgemeinen Persönlichkeitsrechts und der Grundrechtecharta der EU mit Datenschutzbezug gehören zu seiner Ausbildung, ebenso Grundlagen des europäischen und des deutschen Datenschutzrechts, Rechtsgrundlagen der Verarbeitung personenbezogener Daten und datenschutzrechtliche Anforderungen beim Einsatz von IuK.

6.3 IuK-Grundkompetenzen

Um den datenschutzrechtlichen Anforderungen beim Einsatz der IuK zu genügen, muss ein DSB technisches Verständnis (Sachverhalte der Informationstechnologien) mitbringen. Die Organisation der IuK, die Strukturen von IT-Systemen, IT-Applikationen und IT-Prozessen sollten ihm bekannt sein. Ebenso sollte er über Kenntnisse im Informationssicherheitsmanagement verfügen. Nur mit diesen Fähigkeiten wird er in der Lage sein, Risiken für betroffene Personen, die aus IT-Systemen, IT-Applikationen und IT-Prozessen resultieren, zu erkennen.

6.4 Weitere Kompetenzen

Ein DSB versteht die Unternehmensprozesse und Managementsysteme, kennt Methoden zur Risikoanalyse sowie zu Audit- und Prüfverfahren. Er verfügt über persönliche Integrität, Beratungskompetenz, methodische und didaktische Kompetenz und kann seinen eigenen Status durchsetzen.

6.5 Externer versus interner DSB

Die Funktion des DSB kann sowohl von unternehmensinternen, als auch von externen Personen übernommen werden. Der Vorteil des internen DSB ist, dass dieser das Unternehmen kennt und in den internen Ablauf eingebunden ist. Nachteilig kann sich jedoch auswirken, dass neben der Unkündbarkeit des bestellten (zukünftig „benannten“) DSB dessen Tätigkeit nicht zeitlich begrenzt werden kann, da er weisungsfrei ist und sein Zeitaufwand zu Lasten seiner eigentlichen Tätigkeit geht. Ganz nebenbei besteht zudem die Gefahr der „Betriebsblindheit“. Es gilt darüber hinaus Interessenkollisionen zu vermeiden. So darf die Funktion des DSB nicht durch den EDV-Leiter, den Personalleiter oder die Geschäftsleitung wahrgenommen werden. Als zusätzlichen Kostenaufwand gilt es auch erforderliche Schulungen, Weiterbildungen, ein eigenes Büro, einen eigenen PC etc. einzukalkulieren.

Ein externer DSB hingegen hat eine neutrale Stellung und Unabhängigkeit, wodurch Interessenkonflikte vermieden werden. Er verfügt bereits über entsprechende Fachkenntnisse. Die Nachteile, dass der externe DSB anfangs das Unternehmen nicht kennt und nicht ohne weiteres in den internen Ablauf eingebunden ist, sind durch entsprechende Branchenkenntnisse gut zu kompensieren.

Egal jedoch, ob sich ein interner oder externer DSB, oder in kleinen Betrieben die Geschäftsleitung selbst um das Thema kümmert, ist es allerhöchste Zeit, sich auf die neuen Anforderungen vorzubereiten.

6.6 Rolle des Datenschutzbeauftragten (DSB)

Der DSB ist bei der Erfüllung seiner Aufgaben weisungsfrei, er darf deswegen weder abberufen noch benachteiligt werden. Er berichtet unmittelbar der Geschäftsleitung. Den Betroffenen gegenüber ist er allerdings zur Geheimhaltung verpflichtet.

Der DSB hat folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten,
- Überwachung der Einhaltung der Datenschutzvorschriften und der Sensibilisierung und Schulung der Mitarbeiter und der diesbezüglichen Überprüfungen,

- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung,
- Zusammenarbeit mit der Aufsichtsbehörde,
- Anlaufstelle für die Aufsichtsbehörde.

Hinzu kommt noch die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß DS-GVO im Zusammenhang stehenden Fragen.

Im Vergleich zum alten Recht verschieben sich hier die Zuständigkeiten in Richtung Geschäftsleitung. Dem DSB kommt zunehmend eine Überwachungsfunktion und eine Beratungsfunktion zu.

Praxistipp: Überprüfen Sie, ob Ihr DSB über die erforderlichen Kompetenzen verfügt! Sollte noch kein DSB bestellt sein, überprüfen Sie die Notwendigkeit einer Bestellung! Bewerten Sie Vor- und Nachteile einer externen oder internen Lösung!

Bei der Ermittlung der Anzahl der in der Regel mindestens zehn Personen, die ständig personenbezogene Daten verarbeiten, sind alle „Köpfe" zu zählen: Geschäftsleitung, Beschäftigte, freie Mitarbeiter, Praktikanten, Auszubildende.

6.7 Meldung an die Aufsichtsbehörde

Ab 25.05.2018 ist jeder Verantwortliche verpflichtet, die Kontaktdaten seines DSB an die zuständige Datenschutzaufsichtsbehörde zu melden. Erste Aufsichtsbehörden haben bereits kundgetan, dass sie hierzu Onlinemeldeverfahren einrichten wollen. Aufgrund der föderalen Struktur der Datenschutzaufsicht in Deutschland ist die hierfür zuständige Behörde im nicht-öffentlichen Bereich der jeweilige Landesbeauftragte für den Datenschutz bzw. in Bayern das Bayerische Landesamt für Datenschutzaufsicht.

7. Auftragsverarbeitung

Von Auftragsdatenverarbeitung spricht man, wenn sich der Verantwortliche einer Stelle bedient, die für ihn im Auftrag und weisungsabhängig personenbezogene Daten erhebt, verarbeitet oder nutzt (z. B. Rechenzentrum, IT-Dienstleister, Aktenvernichtungsunternehmen oder Datenerfassungsbüros). Die Verantwortung und Haftung für den Umgang mit den personenbezogenen Daten bleibt weiterhin beim Auftraggeber.

Das BDSG-alt sieht vor, dass im Falle einer Auftragsdatenverarbeitung nach § 11 BDSG der Auftragnehmer sorgfältig auszuwählen ist und der Auftrag schriftlich zu erteilen ist. Hierbei ist im Einzelnen schriftlich festzulegen:

- der Gegenstand und die Dauer des Auftrags,
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Zur sorgfältigen Auswahl gehört u. a. die Überprüfung der technisch-organisatorischen Maßnahmen beim Auftragnehmer. Dies kann durch ein Vor-Ort-Audit, durch Vorlage von Auditberichten/Zertifizierungen oder durch Selbstauskunft erfolgen.

Mit der DS-GVO ändert sich zunächst die Begrifflichkeit, man spricht ab 25.05.2018 von Auftragsverarbeitung und Auftragsverarbeitern.

Neu ist, dass der Auftragsverarbeiter bei Vertragsschluss die beauftragten Subunternehmer explizit benennen muss. Gerade im Onlinebereich und bei Service- und Wartungsarbeiten geben viele Dienstleister Aufträge an Subdienstleister weiter. Hier ist bis zum letzten Glied der Kette eine vertragliche Regelung erforderlich. Der Wechsel eines Subunternehmers ist durch den Auftraggeber schriftlich zu genehmigen. In der Praxis werden sich vermutlich Lösungen etablieren, in denen der Auftragsverarbeiter einen Wechsel schriftlich anzeigt und dem Auftraggeber ein Sonderkündigungsrecht einräumt.

Das BDSG-alt sieht auch die Fernwartung von EDV-Systemen als Auftragsverarbeitung. Hierzu lässt sich die DS-GVO nicht explizit aus. Es ist aber davon auszugehen, dass dieser Umstand im Falle der Fernwartung von EDV-Systemen, in denen personenbezogene Daten verarbeitet werden, auch weiterhin als Auftragsverarbeitung angesehen wird.

Haftete bislang allein der Auftraggeber für Verstöße des Auftragsverarbeiters, so weitet die DS-GVO die Haftung in bestimmten Situationen auch auf den Auftragsverarbeiter aus.

Der Auftragsverarbeiter muss zukünftig ein Verzeichnis seiner Auftraggeber vorhalten, mehr dazu unter Punkt 9.

Praxistipp für Auftraggeber: Überprüfen Sie, ob mit allen Dienstleistern, die personenbezogene Daten verarbeiten, entsprechende Verträge geschlossen wurden! Passen Sie Ihre Verträge auf die neue Rechtslage an!

Zusätzlicher Tipp für Auftragsverarbeiter: Überprüfen Sie die Verträge mit Ihren Subunternehmern! Etablieren Sie ein Verfahren bei Wechsel der Subunternehmer! Erstellen Sie das Verzeichnis Ihrer Auftraggeber!

8. Technisch-organisatorische Maßnahmen

Im BDSG-alt sind die technisch-organisatorischen Maßnahmen in sog. „Acht Gebote" gegliedert: Zutrittskontrolle, Zugangskontrolle, Zugriffskontrolle, Weitergabekontrolle, Eingabekontrolle, Auftragskontrolle, Verfügbarkeitskontrolle und Trennungskontrolle. Ergänzend sind Vorgaben zur Verschlüsselung zu beachten.

Die DS-GVO spricht in diesem Zusammenhang von „Sicherheit der Verarbeitung" und benennt u. a. die klassischen Schutzziele der IT-Sicherheit. Neu ist der Begriff der „Belastbarkeit" der Dienste und Systeme. Im Vordergrund steht die Risikobewertung. Die DS-GVO fordert, dass die Maßnahmen, die zum Schutz von personenbezogenen Daten getroffen werden, unter Berücksichtigung des Risikos ausgewählt werden. Hierbei ist zu beachten, dass die Betroffenen bei der Risikobewertung in den Mittelpunkt zu stellen sind.

Auch für die technisch-organisatorischen Maßnahmen besteht eine „Rechenschaftspflicht". Der Verantwortliche muss nachweisen können, dass die Sicherheit der Verarbeitung gewährleistet ist. Damit werden interne Richtlinien und externe Zertifizierungen noch weiter an Bedeutung gewinnen. In diesem Zusammenhang gilt es, noch weitere Informationen der Aufsichtsbehörden abzuwarten, da gem. DS-GVO zukünftig nur noch akkreditierte Zertifizierungsstellen externe Zertifizierungen vornehmen dürfen.

Praxistipp: Etablieren Sie ein Verfahren zur regelmäßigen Überprüfung der Wirksamkeit der technisch-organisatorischen Maßnahmen! Legen Sie konkrete Vorgaben für die Risikobewertung Ihrer Prozesse fest!

9. Verzeichnis der Verarbeitungstätigkeiten

Das BDSG-alt fordert vom Unternehmen ein Verzeichnis aller Prozesse, in denen personenbezogene Daten verarbeitet werden. Die DS-GVO fordert dies grundsätzlich nur von Unternehmen, die mehr als 250 Mitarbeiter beschäftigen. Das Verzeichnis ist jedoch nach DS-GVO auch zu erstellen, wenn z. B. besondere Arten personenbezogener Daten verarbeitet werden. Dies ist im Grunde in einer Personalabteilung immer der Fall.

Um das „Recht auf Vergessenwerden" umzusetzen, muss das Unternehmen wissen, welche Daten in welchen Prozessen vorhanden sind. Auch dies wird ohne das Verzeichnis nur schwerlich gelingen.

Hinzu kommt die Forderung, die Risiken der Prozesse zu bewerten. Auch dies setzt Kenntnis aller Prozesse voraus.

Im Verzeichnis der Verarbeitungstätigkeiten sind zahlreiche Angaben aufzunehmen, die auch bislang gefordert waren. Neu hinzu kommt die Angabe des DSB, es entfällt die Angabe des Leiters der Datenverarbeitung.

Neu ist, dass Auftragsverarbeiter ebenfalls ein Verzeichnis zu führen haben. In diesem sind Name und Kontaktdaten des Auftragsverarbeiters und jedes Verantwortlichen, in dessen Auftrag er tätig ist, aufzuführen. Der DSB des Auftraggebers ist ebenso zu nennen, wie die Kategorien von Verarbeitungen, die im Auftrag jedes Auftraggebers durchgeführt werden. Hinzu kommen ggf. Angaben zu Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation.

Praxistipp: Überprüfen Sie, ob Sie alle Prozesse erfasst haben, in denen personenbezogene Daten verarbeitet werden!

Zusätzlicher Praxistipp für Auftragsverarbeiter: Erstellen Sie bereits jetzt das geforderte Verzeichnis! Verschaffen Sie sich einen Überblick, welche Daten Sie für wen verarbeiten!

10. Sonderfall Videoüberwachung

Das BDSG-alt macht im Gegensatz zur DS-GVO konkrete Vorgaben zur Videoüberwachung. Das BDSG-neu übernimmt in Teilen die Regelungen des BDSG-alt, weitet aber die Zulässigkeit der Videoüberwachung gerade für den Bereich öffentlicher Plätze und des öffentlichen Personennahverkehrs aus. Diese Regelungen wurden bereits als Änderung des BDSG in Kraft gesetzt.

Für Unternehmen ändert sich im Grunde nicht viel. Ist die Überprüfung der Videoüberwachung bislang durch den DSB vorab durchzuführen, so sollte auch weiterhin der DSB zu Rate gezogen werden. In vielen Fällen dürfte dies aufgrund der Notwendigkeit einer Datenschutz-Folgenabschätzung ohnehin erforderlich sein. Es ist davon auszugehen, dass hier noch weitere Konkretisierungen durch den EU-Datenschutz-Ausschuss erfolgen werden.

Praxistipp: Überprüfen Sie den Prozess der Videoüberwachung! Sind alle Beobachtungsbereiche ausgeschildert? Sind die Schilder zu erkennen, bevor der Beobachtungsbereich betreten wird? Ist auf den Schildern der Verantwortliche für die Videoüberwachung benannt?

11. Datenschutz-Managementsystem

Das Datenschutz-Managementsystem wird zukünftig durch neue Anforderungen eine andere Qualität haben. Wir haben mehrere Themen wie Rechenschaftspflicht, Meldung von Datenpannen, Risikobewertung oder Datenschutz-Folgenabschätzung bereits angesprochen. Dokumentation und Versionierung werden eine wesentlich stärkere Rolle spielen als bisher. Im Folgenden werden stichpunktartig einige Punkte und Unterlagen angeführt, die in einem Unternehmen auf jeden Fall vorhanden sein sollten:

- Bestellung eines DSB (Bestellungsurkunde, falls erforderlich)
- Datenschutzleitlinie und Datenschutzhandbuch/ Datenschutzkonzept
  - Verantwortlichkeiten im Unternehmen
  - Stellenbeschreibung DSB
  - Kategorisierung personenbezogener Daten
  - Risikobewertung und Datenschutz-Folgenabschätzung
  - Verhalten am Telefon
  - Clean Desk Policy
  - etc...
- Richtlinie zur Nutzung der EDV, ggf. IT-Sicherheitskonzept
- Checklisten zur Auswahl von technischen und organisatorischen Maßnahmen
- Regelung der Privatnutzung von Internet, E-Mail und Telefon
- Liste der Dienstleister und Verträge zur Auftragsverarbeitung
- Verzeichnis der Verarbeitungstätigkeiten als Verantwortlicher
- Ggf. Verzeichnis der Verarbeitungstätigkeiten als Auftragsverarbeiter
- Protokollierungs-, Archivierungs- und Löschkonzepte
- Datensicherungskonzept
- Notfallplan
- Nachweis der Schulung der Mitarbeiter
- Dokumentation interner und externer Audits, ggf. Zertifizierungen
- Datenschutzhinweise für sämtliche Datenerhebungen (auch Internetauftritt!)
- Sowie zahlreiche weitere Unterlagen in Abhängigkeit von Branche, Rechtsform oder Geschäftsmodell...

12. Fazit

Der Umfang dieses Merkblatts erlaubt es nicht, auf spezielle Fragestellung einzugehen, wie Auftragsverarbeitung außerhalb der EU, Binding Corporate Rules, Codes of Conduct und vieles mehr. Auch mussten viele Aspekte im Detail offenbleiben. Dies war jedoch auch nicht die Zielstellung. Fazit ist, dass die Anforderungen an das Datenschutz-Managementsystem einer Organisation bereits in den vergangenen Jahren aufgrund zunehmender technischer Komplexität und zahlreicher neuer Anforderungen gestiegen sind. Mit dem 25.05.2018 verschärfen sich die rechtlich-organisatorischen Anforderungen und die Bußgeldsummen werden drastisch erhöht. Datenschutz wird aber auch mehr und mehr zum Image- und Compliance-Thema. Eine Zertifizierung nach ISO 9001/2015 ohne Umsetzung der datenschutzrechtlichen Anforderungen ist künftig kaum noch möglich.

Gehen Sie das Thema Datenschutz jetzt aktiv an!
Lassen Sie sich von Ihrem Verband, IHK, HWK oder anderen externen Datenschutzbeauftragten beraten !

Dirk Munker, Dipl.-Staatsw. (Univ.), Datenschutz-Auditor (TÜV)