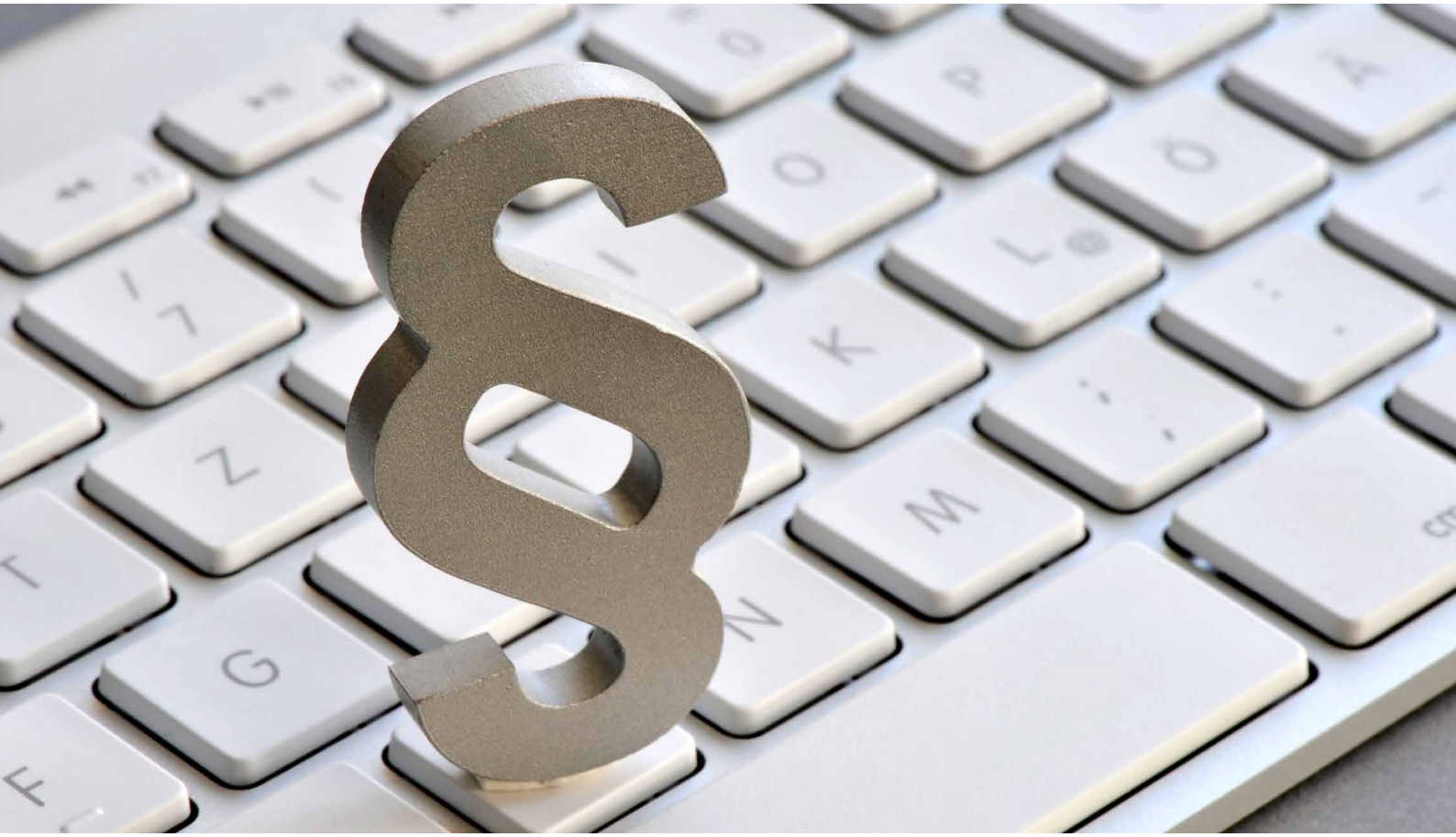
CEYONIQ Technology
A KYOCERA GROUP COMPANY

Whitepaper

Datenschutz braucht ECM:

Die fünf größten Herausforderungen der DSGVO und wie sie zu meistern sind



DSGVO & ECM

1 Einführung: Datenschutz ist Pflicht

Die EU-Datenschutzgrundverordnung (DSGVO) ist in aller Munde. Dass mit dem neuen Gesetz viel Arbeit auf Unternehmen und Behörden zukommt, dürfte niemanden mehr überraschen. Umso erstaunlicher ist es, dass laut des „2017 Veritas GDPR reports“ noch immer 39 Prozent aller Organisationen überhaupt nicht wissen, welche personenbezogenen Daten sie verarbeiten und wo diese liegen.

42 Prozent glauben zudem, dass ihre derzeitige Technologie für eine Umsetzung der DSGVO-Vorschriften nicht ausreichend geeignet ist. Es verwundert daher nicht, dass laut einer Studie von IDC 44 Prozent der befragten Organisationen noch keine konkreten Maßnahmen zur Erfüllung der DSGVO ergriffen haben.

Viel Zeit bleibt dabei nicht mehr, denn ab dem 25.05.2018 ist die Verordnung für alle Organisationen verbindlich; mit weiteren Gnadenfristen sollte nicht gerechnet werden. Umso besorgniserregender, dass laut einer aktuellen Studie der Marktforscher von Gartner über die Hälfte der Unternehmen weltweit die neuen Bestimmungen zum Stichtag nicht einhalten können.

Doch was passiert eigentlich, wenn Unternehmen und öffentliche Stellen künftig nicht DSGVO-konform arbeiten? Wie aus den Jahresberichten der Landesdatenschutzbeauftragten hervorgeht, werden Unternehmen, die als Datenschutz-Ignoranten entlarvt werden, auch jetzt schon hart bestraft. Die bisher überschaubaren Bußgelder werden sich zukünftig auch für geringe Verstöße sehr wahrscheinlich vervielfachen.

Die neue Höchststrafe beträgt mit einer Höhe von 20 Millionen Euro immerhin mehr als das 66-fache der bisherigen Geldbußen. Für Konzernunternehmen wird es besonders brisant, denn hier werden bis zu vier Prozent des jährlichen Gesamtumsatzes fällig.

Bei vielen Entscheidern herrscht derzeit noch große Unsicherheit, denn der Umfang der DSGVO kann zunächst überfordern. Wir zeigen Ihnen deshalb, welche die fünf größten Herausforderungen im Zuge der DSGVO sind und wie Enterprise-Content-Management-Lösungen (ECM) bei der Umsetzung der Verordnung unterstützen können. Die Devise ist klar: Unternehmen müssen handeln.

2 DSGVO: Drei weit verbreitete Irrtümer

Trotz der erheblichen Sanktionen, die mit der DSGVO auf Unternehmen zukommen können, zeigt die Praxis, dass viele Organisationen gar nicht wissen, dass die Verordnung auch für sie relevant ist. Das liegt vor allem an mangelndem Hintergrundwissen und unzureichendem Bewusstsein darüber, dass auch die eigene Datenverarbeitung regelmäßig hinterfragt werden sollte. Prinzipiell gilt: Die DSGVO muss in jedem Unternehmen und jeder Behörde umgesetzt werden. Dennoch halten sich die folgenden drei Irrtümer hartnäckig.

Irrtum 1: Unser Unternehmen verarbeitet keine personenbezogenen Daten!

Die Annahme, dass Unternehmen keine personenbezogenen Daten verarbeiten würden, ist in der Regel falsch. Die DSGVO gilt für alle in der EU befindlichen natürlichen Personen, deren Daten durch Unternehmen und Behörden verarbeitet werden. Personenbezogene Daten sind dabei alle Daten, die irgendeine Information zu diesen Personen liefern. Damit betrifft die DSGVO nicht nur Kundendaten, sondern auch Angaben zu eigenen Mitarbeitern, den Mitarbeitern von Partnerunternehmen, Lieferanten und Dienstleistern sowie sämtlichen anderen externen Personen. Große Unsicherheit herrscht zudem bei der Frage, ob berufliche Kontaktdaten sowie Angaben zur Firmenzugehörigkeit und der Position im Unternehmen überhaupt datenschutzrelevant sind. Die Antwort lautet eindeutig: ja. Daten, die einer lebendigen Person unmittelbar zuordenbar sind, haben Personenbezug.

Das bedeutet in der Praxis, dass alle Angaben zu einzelnen Mitarbeitern wie Name, personalisierte E-Mail und die Telefondurchwahl als personenbezogene Daten gelten. Allgemeine Firmeninformationen wie die zentrale Rufnummer sind hingegen vom Datenschutz ausgenommen. Weiterhin betrifft die DSGVO ausnahmslos jede Information, die sich in irgendeiner Form auf natürliche Personen bezieht, sei dies der Name, eine personalisierte E-Mailadresse, das Datum des letzten Arztbesuchs, IT-seitig erstellte Logfiles oder die private Bankverbindung.

Zusammenfassend lässt sich sagen, dass der Kreis der Daten, die für die DSGVO relevant sind, größer als häufig angenommen ist. Betrachten Sie Ihre Datenbestände deshalb sorgfältig und hinterfragen Sie deren Datenschutzrelevanz mit äußerster Vorsicht.

Irrtum 2: Unser Unternehmen ist viel zu klein für Datenschutz!

Die DSGVO schützt natürliche Personen bei jeder Datenverarbeitung, die in Zusammenhang mit dem Erwerb einer Ware oder der Erbringung einer Dienstleistung, entgeltlich wie unentgeltlich, steht. Eine Mindestgröße, die Firmen haben müssen, damit die Datenschutzgesetze für sie gelten, gibt es dabei nicht. Nach Art. 3 Abs. 7 DSGVO gilt jede juristische Person als sogenannter Verantwortlicher, „die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet". Damit fallen prinzipiell jedes Unternehmen, jede Behörde und auch zahlreiche sonstige Organisationen in den Anwendungsbereich der DSGVO, denn wie bereits festgestellt wurde: Organisationen, die keine personenbezogenen Daten verarbeiten, gibt es so gut wie nicht.

Irrtum 3: Unser Unternehmen hat schon immer datenschutzkonform gearbeitet, damit müssen wir uns um die DSGVO nicht weiter kümmern!

Die Vorschriften, die das Bundesdatenschutzgesetz in der Vergangenheit gemacht hat, waren zweifelsohne bereits sehr streng. Doch vor allem im Bereich der Dokumentations- und Nachweispflichten haben sich die Anforderungen erhöht. In Zukunft muss lückenlos nachgewiesen werden können, dass geltende Datenschutzbestimmungen eingehalten werden.

Für Unternehmen und Behörden, die ihren Datenschutz gut im Griff haben, bedeutet dies vor allem Schreibarbeit – denn die Dokumentation der Umsetzung der neuen Anforderungen dürfte sich aufwendig gestalten. Dies betrifft nicht nur offensichtliche Dinge wie die Führung des Verarbeitungsverzeichnisses, auch das Vorhandensein von datenschutzrelevanten Steuerprozessen sollte genau dokumentiert sein.

Auch an anderen Stellen steckt der Teufel im Detail: Bisher dürften nur die wenigsten Unternehmen ihre technischorganisatorischen Maßnahmen nachweisbar risikoorientiert vergeben haben. Auch der Prozess der Datenschutz-Vorabkontrolle wird mit der Einführung des neuen Instruments der Datenschutzfolgenabschätzung noch einmal verkompliziert. Die konkrete Umsetzung von Betroffenenrechten gestaltet sich künftig ebenfalls anders. Jeder, der die Anforderungen des BDSG im Datenschutz bisher nicht weit übertroffen hat, sollte dringend aktiv werden!

3 Von der Planung zur Umsetzung: Die fünf größten Herausforderungen der DSGVO

Ohne sorgfältige Planung kann ein DSGVO-Projekt nicht gelingen. Um Kapazitäten zu bündeln und zielgerichtet vorgehen zu können, empfiehlt es sich, die neuen Vorschriften in verschiedene Themenblöcke einzuteilen und entsprechend zu bearbeiten. Unterschätzen Sie dabei die Einzelaufwände nicht, denn durch DSGVO-Projekte treten oftmals Probleme zutage, die schon lange schwelen, aber nie ausreichend Beachtung gefunden haben. Dieses Kapitel beschreibt die fünf größten Herausforderungen, die bei der Umsetzung der DSGVO auf Unternehmen zukommen.

Herausforderung 1: Die Datenverarbeitung muss für Betroffene transparent sein

Der Dreh- und Angelpunkt der Verordnung ist die transparente Datenverarbeitung, die durchaus als Grundlage für die Umsetzung aller weiteren Vorschriften gesehen werden kann. Transparenz hat dabei zwei Gesichtspunkte: Zum einen muss die gesamte Datenverarbeitung des Unternehmens so dokumentiert sein, dass sie von außen nachvollziehbar ist. Zum anderen müssen sämtliche Informationen und Auskünfte, die nach diversen Artikeln der DSGVO zu erteilen sind, so erbracht werden, dass Betroffene sie verstehen, vollumfänglich informiert sind und eine angemessene Entscheidungsgrundlage dazu haben, was mit ihren Daten passieren soll. Ohne Transparenz ist Datenschutz nicht möglich.

Vor allem die Bereitstellung von Informationen zur Datenverarbeitung an die Betroffenen dürfte zunächst einigen Mehraufwand verursachen. Wie können Sie also sicherstellen, dass Sie Ihrer Informationspflicht überall dort nachkommen, wo es notwendig ist? Artikel 12 der Verordnung definiert dazu die genauen Vorfälle, in denen Informationen an Betroffene auszuhändigen sind:

- Datenerhebung (durch Verantwortliche oder Dritte): Die Vorschrift, dass Betroffene zu informieren sind, wenn ihre Daten erstmalig erhoben werden, ist bereits im BDSG-alt enthalten. Neu ist jedoch der erhebliche Umfang, in dem Betroffene zu informieren sind (s. DSGVO Art. 13, 14). Wichtig ist deshalb zu prüfen, wie und in welchem Umfang bisher informiert wurde und welche Informationen künftig noch beizubringen sind. Auch für Verarbeitungstätigkeiten, über die nach BDSG alt bereits informiert wurde, sind fehlende Informationen nachzuliefern!

- Geltendmachung von Betroffenenrechten: Betroffene, die ihre Rechte nach den Art. 15 bis 22 geltend machen wollen, müssen bei einer entsprechenden Anfrage vollumfänglich und verständlich darüber informiert werden, was mit ihren Daten geschieht. Verantwortliche dürfen dafür keine Gebühr verlangen und müssen den Anfragen binnen eines Monats nachkommen.

- Information der Betroffenen bei Datenschutzverstößen: Damit Betroffene bei Datenschutzverstößen, die maßgeblich ihre Rechte und Freiheiten gefährden, gegebenenfalls selbst intervenieren können, müssen sie nach Art. 34 über entsprechende Vorfälle vollumfänglich informiert werden. Zudem muss jeder Verstoß binnen 72 Stunden an die zuständige Aufsichtsbehörde gemeldet werden.

Betroffene nur zu informieren, reicht jedoch noch nicht aus, um die Transparenzpflichten vollumfänglich zu erfüllen. Auch die Art und Weise, wie Informationen zur Verfügung gestellt werden, ist ausschlaggebend. Folgende Kriterien müssen dabei erfüllt sein:

- Präzise Formulierungen: Alle Angaben sollten so genau wie möglich sein und möglichst wenig Interpretationsspielraum lassen.

- Leichte Zugänglichkeit der Information: Betroffene sollten jederzeit ohne größere Hürden die Möglichkeiten haben, die entsprechenden Informationen abzurufen. Dazu können Auskünfte je nach Vorgang beispielsweise schriftlich oder online zur Verfügung gestellt werden.

- Verständliche, einfache Sprache: Nur, wer versteht, was er liest, kann auch informierte Entscheidungen treffen. Verzichten Sie daher auf umständliche Formulierungen und „Juristendeutsch".

Die erforderlichen Informationen können Verantwortliche jedoch nur dann liefern, wenn die eigene Datenverarbeitung auf Prozessebene umfangreich dokumentiert ist. Nach BDSG-alt war dies optional, mit der DSGVO wird es nach Art. 30 zur Pflicht. Wer sich diese Mühe bereits in der Vergangenheit gemacht hat, wird nun belohnt, denn dann ist der Anpassungsaufwand des Verzeichnisses der Verarbeitungstätigkeiten (VVT) überschaubar. Alle anderen sollten dringend damit beginnen, ihre internen Prozesse zu dokumentieren. Ausschlaggebend für die Definition eines Verfahrens ist dabei der jeweilige Zweck der Datenverarbeitung.

Zu den einzelnen Verfahren ist zudem zu erfassen, welche Datenarten welcher Personengruppen verarbeitet werden. Dasselbe gilt für die Empfängergruppen, an die Daten weitergeleitet werden. Weiterhin ist zu notieren, ob Daten in ein Drittland (außerhalb der EU) übertragen werden und wie hierbei ein angemessenes Datenschutzniveau geschaffen wird (z. B. über Standardvertragsklauseln). Für die einzelnen Daten sind zudem die sich aus anderen Gesetzen ergebenden Löschfristen und geeignete technischorganisatorische Sicherheitsmaßnahmen festzuhalten.

Herausforderung 2: Lösch- und Aufbewahrungsfristen müssen eingehalten werden

Mit dem „Recht auf Vergessenwerden" (DSGVO Artikel 17) zementiert die EU eine Löschpflicht für personenbezogene Daten, wenn der jeweilige Verarbeitungszweck erloschen ist. Dies ist beispielsweise der Fall, wenn ein Kunde einen Werbewiderspruch einlegt oder eine Geschäftsbeziehung beendet. Maßgeblich für die Notwendigkeit der Datenhaltung ist damit also ausschließlich der Zweck, zu dem sie ursprünglich erfasst wurden. Diese Vorschrift gab es auch bereits im BDSG-alt, neu ist jedoch, dass eine unterbliebene Datenlöschung nun mit einem Bußgeld geahndet werden kann. Der Pflicht zur Datenlöschung stehen jedoch zahlreiche Aufbewahrungsfristen gegenüber, die eine Vernichtung bis zum Ende der jeweiligen Frist verbieten. Diese ergeben sich aus anderen Rechtsvorschriften, wie beispielsweise der Abgabenordnung oder dem Handelsgesetzbuch.

Empfehlenswert ist deshalb, zunächst die Aufbewahrungsfristen für jedes Verfahren zu ermitteln. Dies sollte in Abstimmung mit den Fachabteilungen und, wenn möglich, einem Wirtschaftsprüfer, Steuerberater o.ä. stattfinden. Bestimmte personenbezogene Daten, wie beispielsweise Name und Anschrift eines Kunden, werden jedoch mit hoher Wahrscheinlichkeit in unterschiedlichen Verfahren mit unterschiedlichen Aufbewahrungsfristen verwendet. Es ist daher ratsam zu dokumentieren, an welchen Orten die Daten jedes Verfahrens gespeichert sind, um diese später zielgerichtet löschen zu können. Daten, die in mehreren Verfahren mit unterschiedlichen Aufbewahrungsfristen verwendet werden, können so lange aufgehoben werden, wie es die längste Frist vorsieht.

Während des Ablaufs der Aufbewahrungsfrist (und damit nach Erlöschen der Zweckbestimmung) ist der Zugriff auf die betreffenden Daten so zu begrenzen, dass sie nicht mehr verarbeitet werden können, es sei denn, es tritt ein triftiger Grund wie eine Wirtschaftsprüfung auf. Dies kann entweder durch den Entzug von Nutzerberechtigungen geschehen oder durch das Setzen von Sperrkennzeichen bzw. die Verwahrung von Papierakten in einem abgeschlossenen Archiv mit entsprechender Zutrittskontrolle. Auch Daten, die für ein Verfahren noch benötigt, für ein anderes jedoch nur noch aufbewahrt werden, sind

so zu schützen, dass nur den Personen Zugriff gewährt wird, die am noch laufenden Verfahren arbeiten. Kommt es während der Aufbewahrungsfrist dazu, dass Daten noch einmal benötigt werden, ist die Frist für diesen Zeitraum zu pausieren. Die verschiedenen Datenkategorien, Aufbewahrungsfristen und Speicherorte sollten in einem zentralen Löschkonzept dokumentiert werden, ebenso wie die Vorgehensweise, nach der gelöscht wird. Eine genaue Anleitung für die Erstellung eines Löschkonzepts bietet die DIN 66398.

Herausforderung 3: Ohne Datenschutzmanagementsystem keine Datensicherheit

Schon das BDSG-alt schrieb technischorganisatorische Maßnahmen (TOMs) vor, die für ein angemessenes Sicherheitsniveau sorgen sollen. In der DSGVO ist im Artikel 32 beschrieben, dass TOMs künftig risikobasiert zu vergeben sind und gewährleisten sollen, dass die Vertraulichkeit, Integrität und Verfügbarkeit von Daten geschützt wird. Diese Anforderungen sind bereits als Schutzziele der Informationssicherheit bekannt. Zudem ist dafür Sorge zu tragen, dass Systeme im Notfall schnell wiederhergestellt werden können und belastbar sind. Bevor TOMs festgelegt werden, ist zunächst eine Risikobewertung aller Verfahren durchzuführen. Diese kann vergleichbar nach der Methodik einschlägiger ISO-Normen (z. B. ISO/ IEC 27001) aufgebaut werden. Als Kriterien für die Bewertung des tatsächlichen Risikos darf dabei neben der Eintrittswahrscheinlichkeit jedoch nicht der mögliche Schaden aus Unternehmenssicht, sondern die Gefährdung der Rechte und Freiheiten betroffener Personen herangezogen werden. Dies soll gewährleisten, dass wirtschaftliche Interessen nicht dem Schutz Betroffener entgegenstehen.

Auf Basis dieser Risikobewertung sind im Anschluss entsprechende TOMs zu vergeben. Das BDSG-neu hat in §64 hierzu neue Referenzmaßnahmen veröffentlicht. Unabhängig vom Ergebnis der Risikobewertung müssen bestehende TOMs also auf jeden Fall überarbeitet werden. Die DSGVO selbst äußert

sich kaum zu konkreten Maßnahmen und nennt lediglich an einigen Stellen Pseudonymisierung, Anonymisierung und Verschlüsselung als sinnvollen Schutz. Eine enge Zusammenarbeit mit der IT und dem Informationssicherheitsbeauftragten ist bei der Vergabe von TOMs deshalb dringend anzuraten.

Damit nachgewiesen werden kann, dass die ausgewählten Maßnahmen wirkungsvoll sind, sind diese regelmäßig zu überprüfen und zu bewerten. Auch dieser Prozess orientiert sich stark an der Vorgehensweise bekannter Managementsysteme. Die DSGVO empfiehlt deshalb, ein Datenschutzmanagementsystem einzuführen. Dieses ist zwar keine Pflicht, ergibt sich jedoch fast schon zwangsweise aus den genannten Anforderungen und kann nach Art. 83 sogar bußgeldmindernd wirken, wenn es zu einem Datenschutzverstoß kommt.

Herausforderung 4: Privacy by design und privacy by default gewährleisten

Das Konzept hinter privacy by design und privacy by default (datenschutzfreundliche Voreinstellungen und Datenschutz durch Technikgestaltung) steht im logischen Einklang mit den restlichen Vorschriften der DSGVO. Die Anforderungen des Artikels sollten dabei sowohl aus Sicht der Betroffenen als auch aus Sicht des Verantwortlichen betrachtet und entsprechend umgesetzt werden.

Aus Betroffenensicht bedeuten die Vorschriften vor allem, dass überall, wo Datenschutzeinstellungen in Prozessen und Software möglich sind, diese im Standard bereits mit maximaler Einstellung zur Verfügung gestellt werden müssen, ohne dabei jedoch den Verarbeitungszweck oder die Sicherheit zu gefährden. Dies gilt auch dann, wenn die Betroffenen selbst die Möglichkeiten haben, Datenschutzeinstellungen zu ändern, wie beispielsweise bei der Nutzung sozialer Netzwerke. Prinzipiell sollte Software bevorzugt werden, die derartige Einstellungen zulässt.

Aus Sicht der Verantwortlichen ergeben sich dabei jedoch noch eine ganze Reihe weiterer Aspekte, die zu beachten sind. So müssen datenschutzrechtliche Aspekte künftig bereits nachweislich bei der Planung von Prozessen und Software betrachtet und entsprechend umgesetzt werden. Konkret gehören dazu vor allem die Datenschutzgrundsätze nach Art. 5, die Betroffenenrechte nach Kapitel III sowie Maßnahmen für die Datensicherheit nach Art. 32 und BDSG-neu §64. Dabei ist dies nicht nur bei Neueinführungen zu beachten, sondern sollte auch fester Teil des Change Managements sein. Die frühzeitige Einbeziehung des Datenschutzbeauftragten in die Prozessplanung und Softwareauswahl ist deshalb anzuraten.

Herausforderung 5: Auftragsverarbeiter müssen mehr Verantwortung übernehmen

Auftragsverarbeitung (AV, zuvor Auftragsdatenverarbeitung) liegt dann vor, wenn ein Dienstleister nach Weisung eines Auftraggebers dessen Daten verarbeitet, ohne dabei selbst über die Art und Weise der Datenverarbeitung entscheiden zu können. Damit für die Weitergabe von Daten, die hier stattfindet, nicht zusätzlich die Einwilligung aller Betroffenen eingeholt werden muss, wurde bereits 2009 das Konstrukt der Auftragsverarbeitung geschaffen. Der Dienstleister zählt damit als verlängerter Arm des Verantwortlichen, die Rechtsgrundlage hierfür bildet ein entsprechender Vertrag.

Als Teil des Verantwortlichen waren Auftragnehmer im AV-Verhältnis bisher davon befreit, die Zulässigkeit der ihnen übertragenen Aufgaben prüfen zu müssen. Auch der Abschluss entsprechender Verträge als Rechtsgrundlage oblag bisher immer dem Auftraggeber. Auftragnehmer wurden für Verfehlungen ihrer Auftraggeber damit datenschutzrechtlich nicht belangt. Sogar für Fehler, die Auftragnehmern während der Datenverarbeitung unterlaufen können, wurden die Auftraggeber zur Rechenschaft gezogen. Diese waren deshalb wiederrum dazu verpflichtet, ihre Auftragnehmer regelmäßig hinsichtlich der Einhaltung des Datenschutzes und entsprechender Sicherheitsbestimmungen zu überprüfen.

Künftig nimmt die DSGVO Auftragsverarbeiter stärker in die Pflicht. Dazu werden Dienstleistern unter anderem zusätzliche Dokumentationspflichten auferlegt. Neben dem regulären Verzeichnis der Verarbeitungstätigkeiten (VVT) müssen sie zudem ein gesondertes VVT für die Tätigkeiten führen, die sie im Rahmen der AV erledigen. Dieses Verzeichnis weist zwar einen reduzierten Umfang auf, dürfte für Auftragnehmer aber gänzlich neu sein und damit viel Mehrarbeit bedeuten, denn oftmals ist gar nicht klar, an welchen Stellen überhaupt AV-Verhältnisse bestehen. Zudem sollten alle Weisungen, die der Auftraggeber hinsichtlich der Datenverarbeitung erteilt, sicher aufbewahrt werden.

Weiterhin treffen den Auftragsverarbeiter künftig einige Prüf- und Sorgfaltspflichten. So ist er dafür verantwortlich, sich zu vergewissern, dass der Auftraggeber die Datenverarbeitung nur in rechtlich einwandfreiem Rahmen anweist. Dazu gehört, dass auch im AV-Verhältnis eine Rechtsgrundlage wie beispielsweise die Einwilligung der Betroffenen für die eigentliche Verarbeitung vorliegen muss und den Informationspflichten ausreichend nachgekommen wurde. Dies ist beispielsweise durch entsprechende Klauseln im AV-Vertrag möglich. Für dessen Abschluss ist der Auftragnehmer mit der DSGVO im Übrigen genauso verantwortlich wie der Auftraggeber, denn schließlich ist auch die Verarbeitung im Auftrag ohne entsprechende Ermächtigung nicht datenschutzkonform.

Verantwortliche sollten deshalb umgehend prüfen, in welchen Fällen sie Auftragnehmer im Rahmen eines AV-Verhältnisses beschäftigen und wo sie unter Umständen selbst Auftragnehmer sind. Nicht immer sind diese Fälle ganz eindeutig, mehrere Aufsichtsbehörden haben hierzu jedoch entsprechende Orientierungshilfen veröffentlicht. Im nächsten Schritt sollten fehlende AV-Verträge abgeschlossen und bestehende Verträge auf die DSGVO angepasst werden. Auftragnehmer sollten sich zudem einmal eingehend mit der Rechtmäßigkeit der ihnen übertragenen Aufgaben auseinandersetzen, Auftraggeber hingegen sollten darauf achten, dass sie ihre Auftragnehmer regelmäßig nachweislich überprüfen.

DSGVO & ECM

4 Wie ECM-Systeme bei der Umsetzung der DSGVO unterstützen

Grundvoraussetzung für die Erfüllung der Bestimmungen der DSGVO ist vor allem eines: eine übersichtliche und strukturierte Datenhaltung. Ein nicht unerheblicher Teil davon besteht aus Dokumenten, die digital wie in Papierform im Unternehmen benötigt werden und meist auch in beiden Varianten vorhanden sind. Daraus ergeben sich jedoch einige Probleme, denn ohne einheitliche Dokumentenlenkung können die Bestimmungen der DSGVO nur schwer überwacht werden. Das größte Problem für Unternehmen, die noch kein Enterprise-Content-Management-System (ECM) einsetzen, dürfte künftig die Einhaltung der gesetzlichen Löschfristen darstellen.

Gerade wenn Dokumente mehrfach im Unternehmen vorhanden sind oder wahllos auf Fileservern abgelegt werden, ist es kaum möglich, alle Exemplare eines Dokuments ausfindig zu machen und zu vernichten. Dokumente, die hingegen strukturiert und revisionssicher abgelegt werden, müssen bis auf wenige Ausnahmen nicht mehr auf Papier vorgehalten werden. Damit entfällt vor allem die doppelte Datenhaltung und der Such- und Löschaufwand reduziert sich deutlich. Zudem sollte jedes ECM auch die Möglichkeit bieten, umfassende Löschregeln zu vergeben, die bei Bedarf pausiert werden können. Dies birgt gleich mehrere Vorteile: Einerseits werden Mitarbeiter dadurch von Arbeiten entlastet, die nicht zum Kerngeschäft des Unternehmens gehören. Andererseits stellt das ECM direkt eine komfortable Möglichkeit zur Verfügung, um nicht nur sicheres Löschen, sondern auch die geforderte Zugriffsbegrenzung während der Aufbewahrungsfrist sicherzustellen.

Ähnlich zur Thematik der Datenlöschung verhält es sich mit der Aussagefähigkeit bei Auskunftsersuchen Betroffener. Während beispielsweise die Vorhaltung von Kontakt- und Identifikationsdaten relativ leicht überprüft werden kann, ist eine Überprüfung personenbezogener Daten, die in strukturierten Dokumenten vorhanden sind, schon wesentlich schwieriger. Versuchen Unternehmen also, das Auskunftsersuchen wahrheitsgemäß zu beantworten, droht ihnen ein erheblicher Aufwand beim Zusammentragen der abgefragten Informationen.

ECM-Systeme mit umfassenden Suchfunktionen erleichtern das Auffinden von Dokumenten mit personenbezogenen Informationen deutlich. Nicht zuletzt kann ein ECM-System auch erheblich zur Steigerung der Datensicherheit abgelegter Dokumente beitragen. Durch die versionierte Dokumentablage ist stets nachvollziehbar, wer zu welchem Zeitpunkt Änderungen an Dokumenten vorgenommen hat. Die in §64 geforderte Eingabekontrolle ist damit gegeben. Zudem sorgen flexible Rechte- und Rollenkonzepte dafür, dass nur die Personen Zugriff auf Dokumente haben, die diese auch wirklich für ihre Arbeit benötigen. Die Vertraulichkeit von Dokumenten bleibt somit ebenfalls gewahrt. Zuverlässige Backup-Konzepte sichern überdies die ständige Verfügbarkeit Ihrer Dokumente.

5 Fazit

Sabine Köhler
Consultant für Datenschutz und
Expertin für die DSGVO
Ceyoniq Technology GmbH

Die Aufwände, die mit der DSGVO entstehen, dürfen nicht unterschätzt werden. Ein DSGVO-Projekt gelingt nur, wenn das notwendige Know-how innerhalb der Organisation vorhanden ist. Vor einer Projektierung sind Schulungen und Coachings deshalb dringend anzuraten. Stellenweise kann es notwendig sein, erhöhte Personalressourcen zur Verfügung zu stellen. Gerade die Dokumentation der Datenverarbeitung erweist sich häufig als aufwendig.

Auch entsprechendes Budget sollte zur Verfügung gestellt werden, denn bestehende Softwarelösungen sind ab Mai 2018 unter Umständen nicht mehr gesetzeskonform einsetzbar.

Sie benötigen Unterstützung? Die Ceyoniq Technology bietet ein umfangreiches Beratungsportfolio für die DSGVO. Neben Mitarbeiterschulungen und Anforderungsanalysen nach individuellen Kundenvorgaben begleiten wir Sie auf Wunsch auch bei der Umsetzung Ihres DSGVO-Projekts oder der Einführung eines Datenschutzmanagementsystems. Unsere Berater verfügen dazu über weitrechende Expertise zu allen Fragen des Datenschutzes und einschlägigen Sicherheitsnormen wie der ISO/ IEC 27001.

CEYONIQ Technology

A KYOCERA GROUP COMPANY

Ceyoniq Technology GmbH
Boulevard 9
33613 Bielefeld

Telefon: +49 521 9318- 1000
Telefax: +49 521 9318- 1111
E-Mail: info@ceyoniq.com

www.ceyoniq.com

/ceyoniq @ceyoniq

Stand: 01/2018
Änderungen vorbehalten

TÜV InterCert SAAR SYSTEMCERTIFIED EN ISO 9001:2015