Wie Sie die DSGVO mit ECM-Lösungen praxisgerecht einhalten

Leitfaden

www.bitkom.org

bitkom

Herausgeber

Bitkom
Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin
T 030 27576-0
bitkom@bitkom.org
www.bitkom.org

Ansprechpartner

Nils Britze | Bitkom e. V.
T 030 27576-201 | n.britze@bitkom.org

Verantwortliches Bitkom-Gremium

AK ECM-Compliance

Projektleitung

Claudia Göbel | DocuWare GmbH

Inhaltsverzeichnis

Abbildungsverzeichnis

1 Compliance mit der DSGVO ist ein Muss

Die Datenschutz-Grundverordnung (DSGVO) ist ein neues europäisches Regelwerk zum Datenschutz und zu Data Governance. Sie richtet sich nicht nur an alle Unternehmen und Behörden innerhalb der EU, sondern an jede Organisation, die ihre Leistungen an Kunden innerhalb der EU anbietet. Die Verordnung sieht jenseits der gesetzlichen Verarbeitungsmöglichkeiten die aktive Einwilligung des Kunden vor und spricht ihm neue Rechte zu, mit denen er die Übertragung seiner personenbezogenen Informationen kontrollieren und z. B. auch die Löschung von Daten verlangen kann. Bei Nichteinhaltung sieht die Verordnung massive Sanktionen vor. Die Regelungen der DSGVO gelten seit dem 25. Mai 2018 verbindlich in der EU.

Man könnte glauben, dass sich mit der neuen Verordnung nichts Wichtiges ändert. Schließlich hat Europa seit 1995[1] Vorschriften zur Datenhaltung und zum Datenschutz. Die DSGVO ändert und ergänzt die bestehenden Vorschriften jedoch in vielen Punkten. Jede Organisation sollte der DSGVO daher ihre Aufmerksamkeit schenken.

Die sechs DSGVO-Grundsätze

Im Kern dreht sich bei der DSGVO alles um den Schutz personenbezogener oder personenbeziehbare Daten, im Englischen »Personal Data« oder »Personally Identifiable Information« (PII) genannt. Personenbezogene Daten können alle Informationen sein, die es jemandem ermöglichen, direkt oder indirekt eine andere natürliche Person zu identifizieren. Dazu gehören Informationen wie der Name, E-Mail-Adressen, Social-Media-Posts, physische, physiologische oder genetische Informationen, medizinische Daten, der Aufenthaltsort, Bankverbindungen, IP-Adressen und die kulturelle Identität.

Dieser Schutz ist in sechs Grundsätzen verankert, danach müssen personenbezogene Daten

1. rechtmäßig, nach Treu und Glauben und nachvollziehbar verarbeitet werden,
2. für festgelegte, eindeutige und legitime Zwecke erhoben werden,
3. dem Zweck angemessen, erheblich und auf das notwendige Maß beschränkt sein,
4. sachlich richtig und wenn erforderlich auf dem neuesten Stand sein,
5. zeitlich begrenzt nur so lange wie nötig gespeichert werden und
6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit gewährleistet.

Diese allgemeinen DSGVO-Prinzipien müssen Sie nicht nur einhalten. Sie müssen die Einhaltung auch dokumentieren und/oder durch Standardarbeitsanweisungen (Standard Operating Procedures, SOPs) zum Datenschutz nachweisen.

1 Datenschutzrichtlinie 95/46/EG.

Die wichtigsten Fakten

- Die DSGVO ist eine EU-Verordnung: Im Unterschied zur bisherigen EU-Richtlinie zum Datenschutz ist das neue Regelwerk eine Verordnung. Der Verordnungscharakter führt zu Änderungen, da anders als unter der Datenschutzrichtlinie, die DSGVO nicht mehr in den Mitgliedstaaten umgesetzt werden musste. Die Verordnung gilt vielmehr unmittelbar und konnte nur an einigen Stellen von den Mitgliedstaaten national ausgestaltet werden. Die Verordnung trat bereits im Mai 2016 in Kraft und erlangt nun, nach Ablauf einer zweijährigen Umsetzungsfrist, am 25. Mai 2018 verbindliche Geltung.

- Wie jede andere EU-Verordnung kann die DSGVO als eine Art europäisches Gesetz angesehen werden. Sie hat Vorrang vor den nationalen Gesetzen zum Datenschutz und setzt die bisherige Datenschutzrichtlinie außer Kraft.

- Hohe Strafen: Die Sanktionen bei Nichteinhaltung der DSGVO sind immens hoch. Es können Geldbußen bis zu 20 Millionen Euro oder 4 Prozent des weltweiten Jahresumsatzes des letzten Geschäftsjahres verhängt werden, je nachdem, welcher Betrag höher ist (↗ Artikel 83, Absatz 5 und 6).

- Nachweis der Einwilligung des Kunden: Es muss in einigen Fällen eine Einwilligung vom Kunden eingeholt werden. Die Einwilligung kann zum Beispiel auf einen bestimmten Verarbeitungszweck bezogen sein. Der für die Verarbeitung Verantwortliche muss die Einwilligung (Opt-in) nachweisen können. Diese Einwilligung kann darüber hinaus auch widerrufen werden.

- Konformität auch außerhalb der EU: Die DSGVO gilt ausdrücklich auch für Unternehmen außerhalb der EU, die ihre Dienste in der EU anbieten oder Daten von europäischen Bürgern erheben und verarbeiten.

- Personenbezogene Daten können fast alles sein: Unstrukturierte Informationen und Dokumente verwalten zu können – darin liegt der Schlüssel zur Compliance. Die Europäische Kommission hat in ihren FAQ festgestellt: »Personenbezogene Daten sind alle Informationen, die sich auf eine Person beziehen, unabhängig davon, ob sie sich auf ihr privates, berufliches oder öffentliches Leben beziehen.«

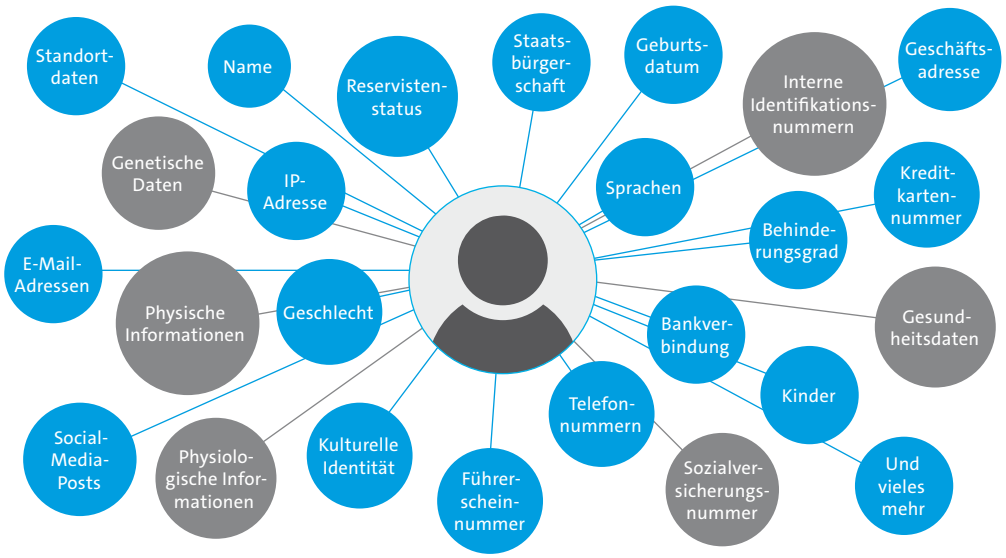

Abbildung 1: Was sind personenbezogene Daten? (Quelle: adaptiert von DocuWare GmbH)

Unternehmen und Behörden müssen in der Lage sein, jeden Ort und jedes Dokument, das personenbezogene Informationen enthält, zu identifizieren und dem Kunden auf Wunsch eine Aufstellung dieser Daten zur Verfügung zu stellen. Ohne ein Enterprise Content Management-System (ECM) ist diese Anforderung unmöglich zu erfüllen.

- Papierdokumente sind eingeschlossen: Die DSGVO gilt nicht nur für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten. Sie bezieht sich auch auf die nicht automatisierte Verarbeitung personenbezogener Daten, die in einem Aktensystem abgelegt sind oder abgelegt werden sollen.

- Erweiterte Haftungsketten: Werden in Ihrem Auftrag personenbezogene Daten bei einem Cloud-Service-Provider oder einem Dokumentenprozess-Outsourcer gespeichert oder verarbeitet, tragen Sie die Verantwortung für dessen Data-Governance-Praxis.

Was sind Sie: Datenverantwortlicher, Auftragsverarbeiter oder beides?

Es gibt fünf Begriffe oder Rollen, die Sie im Zusammenhang mit der DSGVO kennen sollten: betroffene Person, Verantwortlicher, Auftragsverarbeiter, Datenschutzbeauftragter und Datenschutzbehörde.

- Eine betroffene Person, englisch Data Subject, ist eine natürliche Person, zum Beispiel ein Kunde oder ein Mitarbeiter eines Unternehmens oder der Nutzer einer Social-Media-Plattform. Jeder Bürger, jede Bürgerin, der oder die sich im EU-Gebiet aufhält, ist eine betroffene Person im Sinne der DSGVO. Erwägungsgrund 2 legt fest: »Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben.« Die betroffene Person hat diverse Rechte: Sie muss Auskunft darüber erhalten, welche personenbezogenen Daten von ihr gespeichert sind und verarbeitet werden, kann diese berichtigen oder sogar löschen und sie an ein anderes Unternehmen übertragen lassen.

- Der für die Daten Verantwortliche, englisch Data Controller, ist »die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet« (Artikel 4 Nummer 7 DSGVO).

- Der Auftragsverarbeiter, englisch Data Processor, ist »eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet« (Artikel 4 Nummer 8 DSGVO).

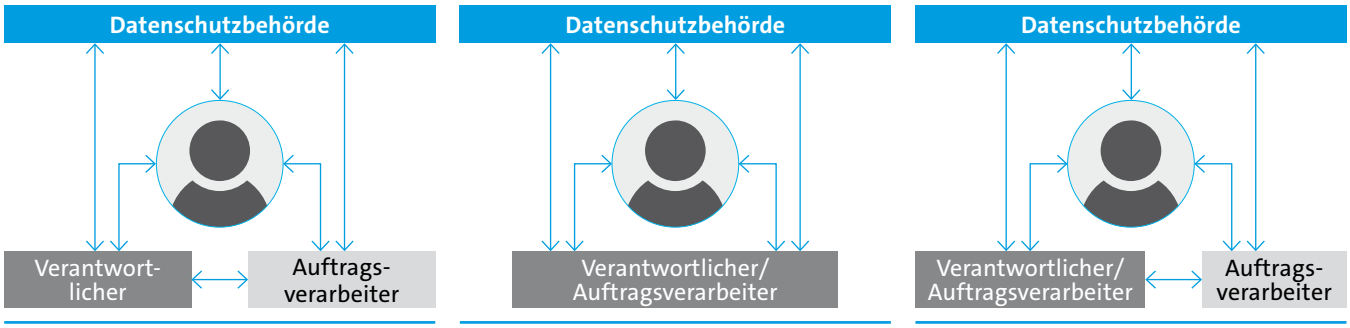

Abbildung 2: Bestimmen Sie die Rolle(n) Ihres Unternehmens anhand von drei Modellen (Quelle: adaptiert von DocuWare GmbH)

Ihr Unternehmen kann Datenverantwortlicher oder Auftragsverarbeiter oder auch beides in einem sein. Ihre Auftraggeber, Kunden, Interessenten und Lieferanten können ebenso Verantwortliche und Auftragsverarbeiter sein. Doch damit nicht genug: Ihre Auftraggeber, Kunden, Interessenten, angestellten und freien Mitarbeiter sind auch alle betroffenen Personen, ebenso wie es die entsprechenden Gruppen bei Ihren Partnern sind.

↗ Artikel 4: Definitionen

Der Datenverantwortliche und der Auftragsverarbeiter müssen von Beginn an sicherheitstechnische Maßnahmen in ihre Produkte und Prozesse einbauen. Falls noch nicht geschehen, haben alle Verantwortlichen und Auftragsverarbeiter nach der DSGVO einen Datenschutzbeauftragten (Data Protection Officer, DPO) zu benennen, wenn ihre Organisation

- eine staatliche Organisation oder Behörde ist,
- hauptsächlich besondere Kategorien von Daten verarbeitet und
- eine umfangreiche regelmäßige und systematische Überwachung vorsieht.

In Deutschland gelten aufgrund der Bestimmungen des BDSG-neu[2] sogar noch strengere Bestimmungen. Auch bisher war im BDSG bereits in § 4 Absatz 1 Buchstabe f geregelt, dass nichtöffentliche Stellen ab zehn Mitarbeitern, die ständig mit automatisierten Datenverarbeitungen beschäftigt sind, einen Datenschutzbeauftragten bestellen mussten.

Nach dem angepassten nationalen Recht gilt nun nach § 38 Absatz 1 BDSG-neu: Ergänzend zu Artikel 37 Absatz 1 Buchstabe b und c der Verordnung (EU) 2016/679 benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen.

↗ Artikel 37: Benennung eines Datenschutzbeauftragten

Jeder EU-Mitgliedstaat muss dafür sorgen, dass eine oder mehrere unabhängige Datenschutzbehörden (Data Protection Authorities, DPAs) die Einhaltung der Vorschriften überwachen.

2 Das BDSG-neu ist das an die DSGVO angepasste Bundesdatenschutzgesetz mit Geltung ab 25. Mai 2018.

Wer kann sich beschweren und wo?

Nach der DSGVO kann nicht nur eine betroffene Person selbst eine Beschwerde einreichen. Die Person kann auch eine gemeinnützige Organisation, z. B. eine Verbraucherschutz-Vereinigung, damit beauftragen, dies in ihrem Namen zu tun.

↗ Artikel 80: Vertretung von betroffenen Personen

Klage wird vor einem Gericht des EU-Mitgliedstaates erhoben, in dem der Verantwortliche oder der Auftragsverarbeiter eine Niederlassung hat (Prinzip des One Stop Shop, OSS). Alternativ können auch die Gerichte des Mitgliedstaats zuständig sein, in dem die klagende betroffene Person ihren gewöhnlichen Aufenthalt hat.

↗ Artikel 79: Recht auf wirksamen gerichtlichen Rechtsbehelf gegen Verantwortliche oder Auftragsverarbeiter

2 Wie ECM-Lösungen Ihnen dabei helfen, die DSGVO einzuhalten

Alle E-Mails, Dateien, Papiere, Notizen oder Dokumente, die persönlich identifizierbare Informationen enthalten, sind personenbezogene Daten. Das heißt, sie müssen alle gemäß DSGVO archiviert, verwaltet, geschützt und kontrolliert werden.

Die DSGVO formuliert die Anforderungen an den Schutz personenbezogener Daten sehr klar. Doch sie äußert sich nicht konkret über die Prozesse und Technologien, die Unternehmen und Behörden einsetzen sollten, um diesen Schutz zu gewährleisten. Und in der Tat ist es unwahrscheinlich, dass ein einziges System alle Aspekte der Verordnung berücksichtigen kann. Um den Vorschriften zu entsprechen, braucht es vielmehr ein koordiniertes technologisches und strategisches Vorgehen.

Eine wichtige Technologie ist ein System zum Dokumentenmanagement oder Enterprise Content Management (ECM): Es digitalisiert nicht nur Papierakten, sondern nutzt auch Metadaten, um die Sicherheit und Governance zu gewährleisten, die zum Schutz von Kundendaten erforderlich sind.

Mit einem ECM steuern Sie, was mit Ihren Dokumenten und Daten geschieht – und mit diesem Ansatz gestalten Sie Ihre Projekte und Prozesse DSGVO-konform. So lassen sich durch ECM-Lösungen beispielweise Archive sehr einfach so einrichten, dass Dokumente nicht heruntergeladen, weitergeleitet oder gedruckt werden können. All das erfordert keine Programmierung und keine Zeile Code, auch keine langwierige Implementierung – es ist einfach als Basisfunktionalität vorhanden.

2.1 Personenbezogene Daten finden und darauf zugreifen

Was passiert, wenn jemand bei Ihnen anfragt, welche personenbezogenen Daten von ihr oder ihm in Ihrem Unternehmen verarbeitet werden? Als Erstes müssen Sie diese **Daten ermitteln**.[3] Da die DSGVO aber auch für **Papierdokumente** gilt, die eine Organisation in strukturierter Aktenhaltung vorhält, ist dies leichter gesagt als getan – falls Sie nämlich noch Prozesse auf Papier verwalten.

3 Zuvor sollte zudem eine Prüfung erfolgen, um sicherzustellen, dass der Anfragende auch berechtigt ist, die Informationen zu erhalten.

Wie ECM Ihre Compliance unterstützt

Mit ECM-Lösungen werden alle Dokumente digitalisiert und in einem sicheren Archiv gespeichert. So können Sie alle persönlichen Daten in Ihren Dokumenten leicht **finden und abrufen**. Dies können E-Mails, Verträge, Rechnungen und vieles mehr sein. ECM automatisiert das Archivieren, Suchen, Finden, Exportieren, Korrigieren und Löschen von persönlich identifizierbaren Informationen.

Das macht diesen Prozess unabhängig von Individuen. Stattdessen wenden ECM-Lösungen die Datenschutz-Richtlinien Ihres Unternehmens oder Ihrer Behörde an. Der automatisierte Ansatz zum Schutz von personenbezogenen Daten bringt Ordnung, Konsistenz und Effizienz in Ihre Ge schäftsprozesse. Er macht Sie schneller und einfacher in der Erfüllung der DSGVO-Anforderungen.

Metadaten spielen eine Schlüsselrolle bei der Einhaltung der DSGVO, und zwar durch das korrekte Klassifizieren, Kategorisieren und Beschreiben persönlich identifizierbarer Informationen. Ein Beispiel wäre die einfache Suche nach Dokumentenarten (wie Verträgen, Rechnungen, Korrespondenz), von denen Sie wissen, dass sie persönlich identifizierbare Informationen enthalten.

ECM-Lösungen automatisieren diesen Klassifizierungsprozess durch maschinelles Lernen und künstliche Intelligenz (KI). Der Service unterstützt so die Compliance und entlastet gleichzeitig Ihr Team von einer komplizierten und langwierigen Dateneingabe.

Nach der Indexierung eines Dokuments können ECM-Lösungen automatisch weitere Maßnahmen einleiten, damit die Informationen garantiert korrekt gehandhabt werden, beispielsweise:

- alle Dateien und Objekte verschlüsseln, die persönlich identifizierbare Informationen enthalten, sowohl während der Übertragung als auch im gespeicherten Zustand,
- Zugriffskontrollen und Berechtigungsmanagement einsetzen, um sicherzustellen, dass nur autorisierte Benutzer auf persönlich identifizierbare Informationen zugreifen können – zum Beispiel können Kundenbetreuer Bestellungen von Klienten einsehen, nicht aber die Mitglieder des Marketing-Teams,
- Aufbewahrungs- und Löschregeln anwenden, um sicherzustellen, dass Daten nicht länger als nötig aufbewahrt werden,
- verhindern, dass Dokumente, die personenbezogene Daten enthalten, versehentlich oder absichtlich per E-Mail verschickt oder anderweitig an Stellen außerhalb der Organisation übertragen werden,
- Änderungen an Dokumenten mit personenbezogenen Informationen nachverfolgen, um zu zeigen, wer was wann geändert hat, und
- Audit-Trails bereitstellen, um nachweisen zu können, dass nur autorisierte Mitarbeiter Zugriff auf personenbezogene Daten von Kunden hatten.

Dieser automatisierte Ansatz zum Schutz personenbezogener Daten bringt Ordnung, Konsistenz und Effizienz in Ihre Compliance-Anstrengungen. Gleichzeitig werden unternehmensweite Datenschutz-Regeln angewendet.

2.2 Personenbezogene Daten exportieren, korrigieren und löschen

Wenn Sie nach personenbezogenen Daten gefragt werden, müssen Sie in der Lage sein, die persönlichen Daten zu exportieren, um sie der anfragenden Person zeigen zu können. In diesem Rahmen kann die Person auch verlangen, ihre Daten in einem »strukturierten, gängigen, maschinenlesbaren und interoperablen Format« an einen anderen Anbieter oder Dienstleister weitergeben zu können.

Dabei sind Sie verpflichtet, eine Kopie der erfragten Daten zur Verfügung zu stellen, und zwar bei der ersten Anfrage kostenlos. Außerdem müssen Sie dies im Regelfall innerhalb eines Monats tun (Artikel 12 Absatz 3 DSGVO).

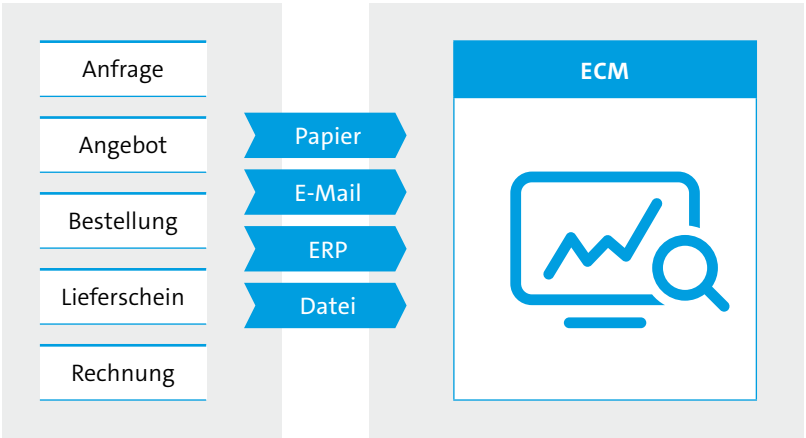

Abbildung 3: ECM erleichtert den Umgang mit personenbezogenen Daten aus verschiedenen Bereichen (Quelle: adaptiert von DocuWare GmbH)

Sollten in Ihrem Unternehmen falsche personenbezogene Daten vorhanden sein, müssen Sie diese auf Verlangen unverzüglich berichtigen. Wenn jemand die Löschung seiner Daten wünscht, müssen Sie dem ebenfalls nachkommen. Dies besagt das neue Recht auf Vergessen-werden. Sie können eine Löschaufforderung nur ablehnen, wenn gesetzliche Verpflichtungen, öffentliches Interesse oder gesetzliche Ansprüche dem entgegenstehen.

Wie ECM Ihre Compliance unterstützt

Jede Anfrage zum Exportieren, Korrigieren oder Löschen von personenbezogenen Daten kann im ECM-System gespeichert werden und kann automatisch einen Workflow auslösen, der speziell auf das Exportieren, Korrigieren oder Löschen der personenbezogenen Daten ausgelegt ist. Die Workflow-Aufgaben können automatisch an den Datenschutzbeauftragten (DPO) verteilt werden, der bei begründeter Anfrage eine Entscheidung dazu trifft.

Mit Modulerweiterung ist die Datenübertragbarkeit gewährleistet. Sie können alle persönlich identifizierbaren Informationen einfach **exportieren und übertragen**.

↗ Artikel 20: Recht auf Datenübertragbarkeit

ECM-Lösungen stellen sicher, dass alle im Viewer vorgenommenen Dokumentänderungen als Overlays zum Dokument gespeichert werden. So können Sie eine Rechnung, die personenbezogene Daten eines Kunden enthält, so exportieren, dass der Freigabestempel und die persönlichen Daten eines Ihrer Mitarbeiter nicht enthalten sind.

Workflow-Aufgaben können gleich dem Datenschutzbeauftragten zugewiesen werden. Die Beauftragten aktualisieren dann entweder selbst die Datenbestände in den verschiedenen Systemen oder sie verteilen die Aufgaben an die zuständigen Kollegen. Der Datenschutzbeauftragte kann leicht auf alle Akten zu der anfragenden Person **zugreifen** und die Dokumente zum Löschen vormerken. Alternativ kann ein ECM-Workflow eine solche Aktion automatisch anstoßen, sobald der Datenschutzbeauftragte bestätigt, dass die Anfrage berechtigt ist.

Um alle relevanten Daten zu **korrigieren**, können die im ECM-System gespeicherten Metadaten im Rahmen dieser Prozesse automatisch oder halbautomatisch aktualisiert werden. Dies stellt eine Konsistenz zwischen den Systemen sicher und trägt zur Einhaltung der DSGVO-Richtlinien bei.

ECM-Systeme können bei Bedarf sowohl **Dokumente als auch Metadaten löschen**. Es kann sogar Anwendungen von Drittanbietern öffnen, was solche Aufgaben stark vereinfacht. Das System kann die betroffene Person automatisch über die Löschung der Daten informieren und einen Zeitplan für die Umsetzung einrichten.

ECM-Lösungen führen eine vollständige **Historie** aller Anfragen zur Berichtigung von Daten. Ist die Korrekturanfrage einer Person nicht gerechtfertigt, kann die ECM-Lösung den Datenschutzbeauftragten unterstützen, indem das System automatisch eine Antwort an die anfragende Person versendet. Darin wird begründet, warum die Anfrage **nicht berechtigt** ist und warum das Unternehmen die persönlichen Daten länger verarbeiten wird. Die Anfragedaten werden für einen erforderlichen Zeitraum aufbewahrt und am Ende automatisch entsorgt.

2.3 Personenbezogene Daten schützen und ihre Weiterverarbeitung verhindern

Ihre Organisation muss in der Lage sein, personenbezogene **Daten vorübergehend oder dauerhaft von einer weiteren Verarbeitung auszuschließen**. Dies kann nötig sein, wenn die Richtigkeit der Daten angezweifelt oder die Verarbeitung als unrechtmäßig angesehen wird oder wenn die betroffene Person einen Ausschluss, aber aus rechtlichen oder historischen Gründen keine Löschung, der Daten wünscht.

↗ Artikel 18: Recht auf Einschränkung der Verarbeitung

Wie ECM Ihre Compliance unterstützt

ECM setzt Regeln zur Datenaufbewahrung und -löschung um, die sicherstellen, dass personenbezogene Daten nicht länger als nötig gespeichert werden. Durch das Einrichten automatischer Aufbewahrungspläne können Sie sehr einfach verhindern, dass Dokumente, die personenbezogene Daten enthalten, versehentlich oder absichtlich per E-Mail verschickt oder anderweitig an Stellen außerhalb des Unternehmens übertragen werden. Dazu ist keinerlei Programmierung erforderlich. Es ist Teil der ECM-Basiskonfiguration, die Administratoren oder Datenschutzbeauftragten von Beginn an zur Verfügung steht.

Darüber hinaus wird jede Änderung an Dokumenten mit personenbezogenen Daten nachverfolgt, um zeigen zu können, wer wann was geändert hat. Mit einer flexiblen und sicheren Rechteverwaltung können nur autorisierte Mitarbeiter auf die personenbezogenen Daten eines Kunden zugreifen. Um nachweisen zu können, dass es keinen unautorisierten Zugriff gab, bietet das System einen Audit-Trail.

So nimmt ECM dem einzelnen Mitarbeiter die Entscheidung in weiten Teilen ab, wie mit personenbezogenen Daten zu verfahren ist. Stattdessen setzt das System zuverlässig die unternehmensweiten Datenschutzbestimmungen um.

2.4 ECM aus der Cloud

Ein besonders hohes Maß an Sicherheit und Vertrauen ist beim Thema »ECM aus der Cloud« erforderlich, also bei IT-Leistungen in den Bereichen Dokumente, Content und Prozesse (z. B. Unterlagen, Akten, Daten, Workflows usw.), die als Service über das Internet bereitgestellt und flexibel genutzt werden können. Hat der ECM-Anbieter ein eigenes Rechenzentrum, ist die Sachlage klar. Aus datenschutzrechtlicher Sicht handelt es bei ECM aus der Cloud um eine Form des Outsourcings im Sinne der Auftragsverarbeitung. Verantwortlich ist der ECM-Kunde, der Daten zur Speicherung und Verarbeitung auf eine externe Cloud auslagert. Auftragsverarbeiter ist in diesem Fall der ECM-Hersteller als Anbieter des Cloud-Services.

Laut DSGVO sind Unternehmen jedoch dazu verpflichtet, auch die Sicherheit derjenigen personenbezogenen Daten zu gewährleisten, deren Speicherung an Dritte ausgelagert wurde. Das können beispielsweise externe Rechenzentren bzw. Cloud-Provider sein, die als Partnerunternehmen des ECM-Anbieters in Erscheinung treten. Die Bereitstellung des ECM-Systems erfolgt hier üblicherweise in Form von »Software as a Service« (SaaS) über das Internet, also über einen Zwischenschritt in Form von öffentlichen, privaten oder hybriden Clouds. Zwar werden Personendaten zu Speicher- und Bearbeitungszwecken auf eine externe Cloud ausgelagert, aber dennoch bleibt der ECM-Kunde (also das Nutzerunternehmen des ECM-Anbieters) endverantwortlich für den DSGVO-konformen Umgang der im Unternehmen verarbeiteten Personendaten.

In diesem Zusammenhang muss sich der ECM-Kunde auch um eine umfassende Dokumentation der Datenverarbeitung in Form eines Verfahrensverzeichnisses kümmern (↗ Artikel 30 DSGVO), was die Beurteilung und Garantie im Falle von Drittlands-Datenübertragungen ebenso mit einschließt (↗ Artikel 49 DSGVO). Der ECM-Anbieter ist zwar hier nicht verantwortlich, sollte diesen Prozess jedoch unterstützen. Im Übrigen sind auch Rechenzentren von den Regularien der DSGVO betroffen, die ihren Unternehmenssitz im Nicht-EU-Ausland haben: Immer dann, wenn Personendaten von EU-Bürgern oder im EU-Raum lebenden Menschen verarbeitet werden, gilt die DSGVO.

Generell sind Cloud-Provider, ECM-Anbieter und ECM-Kunde zu einer umfassenden Zusammenarbeit verpflichtet. Der Cloud-Provider muss für technische und organisatorische Maßnahmen für Datenschutz und Datensicherheit garantieren (ebenso wie der Anbieter). Der ECM-Anbieter muss die Rahmenbedingungen und Prozesse schaffen, die Datenverluste vermeiden oder Missbräuche aufdecken. Und der ECM-Kunde steht als Verantwortlicher in der Pflicht, dies zu überprüfen und Datenverluste, Missbräuche oder Ähnliches unverzüglich anzuzeigen. Das Kundenunternehmen muss zu guter Letzt jederzeit dazu in der Lage sein, Auskunft über den Speicherort sowie die Art und Zweck der Verarbeitung personenbezogener Daten zu geben. Bezogen auf

ECM aus der Cloud bedeutet das: Der Kunde muss sich auch um die ordnungsgemäße und rückstandsfreie Löschung von Personendaten – inklusive möglicher Verweise und Schattenkopien – von den Servern des Rechenzentrums kümmern. Vor Beauftragung sollte der ECM-Kunde demnach die Cloud-Infrastruktur genau prüfen, und zwar unabhängig davon, ob sie dem ECM-Anbieter selbst oder einem beauftragten Dritten gehört. Um sicherzustellen, dass die verschiedenen Verpflichtungen eingehalten werden, muss zudem ein Auftragsverarbeitungsvertrag zwischen dem Verantwortlichen und dem Auftragsverarbeiter abgeschlossen werden.[4]

Die ECM-Software sollte ohnehin DSGVO-konform gestaltet sein. Datenschutz durch Technikgestaltung (Privacy by Design) stellt sicher, dass etwaige Sicherheitsprobleme schon bei der Softwareentwicklung festgestellt werden können und nicht erst im Nachhinein umständlich geschlossen werden müssen. Datenschutzfreundliche Voreinstellungen (Privacy by Default) gewährleisten darüber hinaus, dass nur die Daten erhoben und verarbeitet werden, die für den Zweck der Verarbeitung erforderlich sind.

4 Unter ↗ https://www.bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html kann die Bitkom Mustervertragsanlage zur Auftragsverarbeitung heruntergeladen werden.

3 Entwerfen Sie eine unternehmensweite Compliance-Strategie

Der Einsatz von ECM ist ein großer Schritt in Richtung DSGVO-Compliance. Ihr Unternehmen nutzt jedoch noch andere Software, die personenbezogene Daten verarbeitet, wie zum Beispiel ein CRM, ein Marketingsystem, ein ERP oder andere Anwendungen.

Um den Umgang mit personenbezogenen Daten systemübergreifend zu regeln, legen Sie am besten eine konsistente Strategie fest. So sollten Sie in Ihrem CRM beispielsweise auch in der Lage sein, personenbezogene Daten zu finden, sie zu korrigieren, zu exportieren, zu schützen und zu löschen – und Sie sollten diese Verarbeitungen protokollieren können.

Halten Sie Ihre Aufzeichnungen auf dem neuesten Stand

Ob mit Ihrem ECM-System, einem CRM oder ERP – wenn Sie als Datenverantwortlicher agieren, garantiert Ihr Datenschutzbeauftragter die Einhaltung der DSGVO-Compliance und muss daher Aufzeichnungen mit folgenden Informationen erstellen:

- Ihrem Namen und Ihren Kontaktdaten sowie ggf. gemeinsamen Verantwortlichen, Vertretern und Datenschutzbeauftragten
- Zweck der Verarbeitung
- Beschreibung der Kategorien der betroffenen Personen und der Kategorien personenbezogener Daten;
- Kategorien der Empfänger, einschließlich den Empfängern in Drittländern oder internationalen Organisationen;
- Einzelheiten der Übermittlung personenbezogener Daten in Drittländer (sofern zutreffend);
- Aufbewahrungsfristen für verschiedene Kategorien personenbezogener Daten (soweit möglich)
- Allgemeine Beschreibung der getroffenen Sicherheitsmaßnahmen (soweit möglich).

Wenn Sie einen Datenverarbeiter beauftragen, müssen Sie vertraglich sicherstellen, dass auch dieser alle Kategorien von Verarbeitungstätigkeiten im Auftrag eines Datenverantwortlichen dokumentiert. Dabei stellt das Verarbeitungsverzeichnis[5] als Dokumentationsform das zentrale Instrument des Datenschutzrechts zur Umsetzung der Transparenzpflichten dar.

↗ Artikel 30: Verzeichnis von Verarbeitungstätigkeiten

Der Umfang der Dokumentation umfasst alle Verarbeitungstätigkeiten des Verantwortlichen. Grundsätzlich unterliegt jeder Verantwortliche der Pflicht, ein Verzeichnis von Verarbeitungstätigkeiten zu erstellen und zu führen.

5 Unter dem in Anmerkung 4 genannten Link ist ebenfalls der Bitkom-Praxisleitfaden »Das Verarbeitungsverzeichnis« zu finden.

Weiterführende Informationen

1. Wortlaut der EU-Datenschutz-Gundverordnung (deutsch und englisch, mit Inhaltsverzeichnis und Suchfunktion) ↗ https://dsgvo-gesetz.de/

- Bitkom Praxisleitfäden zur Datenverarbeitung nach der Datenschutz-Grundverordnung (deutsch und englisch)
  ↗ https://www.bitkom.org/Themen/Datenschutz-Sicherheit/Datenschutz/EU-DSGVO/Datenschutzkonforme-Datenverarbeitung.html

- EU-Kommission: DSGVO-Download in allen EU-Sprachen
  ↗ http://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679

- Corrigendum zur DSGVO vom 19. April 2018 in allen EU-Sprachen
  ↗ http://data.consilium.europa.eu/doc/document/ST-8088-2018-INIT/en/pdf

- Bitkom-Informationen zur DSGVO
  ↗ https://www.bitkom.org/Themen/Datenschutz-Sicherheit/DSGVO.html

Danksagung

Der vorliegende Leitfaden ist eine Gemeinschaftspublikation, an der folgende Autoren mitgearbeitet haben:

- Claudia Göbel (DocuWare GmbH)
- Jochen Luckhaus (IQUADRAT AG)
- Jürgen Prummer (d.velop AG)
- Rebekka Weiß (Bitkom e. V.)
- Susanne Dehmel (Bitkom e. V.)
- Thomas Kuckelkorn (BCT Deutschland GmbH)
- Thorsten Brand (Zöller & Partner GmbH)

Besonderer Dank gilt der DocuWare GmbH, die eine erste Version der Gemeinschaftspublikation zur Verfügung gestellt hat. Die Abbildungen basieren auf Inhalten des DocuWare Whitepapers »DSGVO«.

Bitkom vertritt mehr als 2.500 Unternehmen der digitalen Wirtschaft, davon 1.700 Direktmitglieder. Sie erzielen allein mit IT- und Telekommunikationsleistungen jährlich Umsätze von 190 Milliarden Euro, darunter Exporte in Höhe von 50 Milliarden Euro. Die Bitkom-Mitglieder beschäftigen in Deutschland mehr als 2 Millionen Mitarbeiterinnen und Mitarbeiter. Zu den Mitgliedern zählen 1.000 Mittelständler, mehr als 400 Startups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Geräte und Bauteile her, sind im Bereich der digitalen Medien tätig oder in anderer Weise Teil der digitalen Wirtschaft. 80 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, jeweils 8 Prozent kommen aus Europa und den USA, 4 Prozent aus anderen Regionen. Bitkom fördert und treibt die digitale Transformation der deutschen Wirtschaft und setzt sich für eine breite gesellschaftliche Teilhabe an den digitalen Entwicklungen ein. Ziel ist es, Deutschland zu einem weltweit führenden Digitalstandort zu machen.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org