DocuWare

White Paper
DSGVO

Dieses Dokument wurde erstellt mit AuthorIT™, Total Document Creation (http://www.author-it.com).

Disclaimer

Dieses Dokument wurde mit größter Sorgfalt zusammengestellt und die Informationen darin sind Quellen entnommen, die als zuverlässig gelten. Dennoch kann keine Haftung übernommen werden für die Richtigkeit, Vollständigkeit und Aktualität der Informationen. Aus den in diesem Dokument aufgenommenen Informationen können keine Ansprüche hergeleitet werden. Die DocuWare GmbH behält sich das Recht vor, jegliche Informationen, die in diesem Dokument enthalten sind, ohne vorherige Ankündigung zu verändern.

DocuWare GmbH
Therese-Giehse-Platz 2
82110 Germering
www.docuware.com (http://www.docuware.com)

DocuWare

Inhalt

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 europäischen Unternehmen und Behörden, sondern an jede Organisation, die in Europa oder mit europäischen Kunden Geschäfte macht. Die Verordnung sieht eine aktive Einwilligung des Kunden vor und spricht ihm neue Rechte zu, mit denen er die Übertragung seiner personenbezogenen Informationen kontrollieren kann. Bei Nichteinhaltung sieht die Verordnung massive Sanktionen vor. All dies tritt am 25. Mai 2018 in Kraft.

Man könnte glauben, dass sich mit der neuen Verordnung nichts Wichtiges ändert. Schließlich hat Europa seit 1995 Vorschriften zur Datenhaltung und zum Datenschutz. Die DSGVO besitzt auf der EU-Agenda allerdings höchste Priorität und jede Organisation muss ihr Aufmerksamkeit schenken.

Die sechs DSGVO-Grundsätze

Im Kern dreht sich bei der DSGVO alles um den Schutz personenbezogener Daten, im Englischen "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, Cookies 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 dies auch dokumentieren und/oder durch Standardarbeitsanweisungen (Standard Operating Procedures, SOPs) zum Datenschutz nachweisen.

Die wichtigsten Fakten

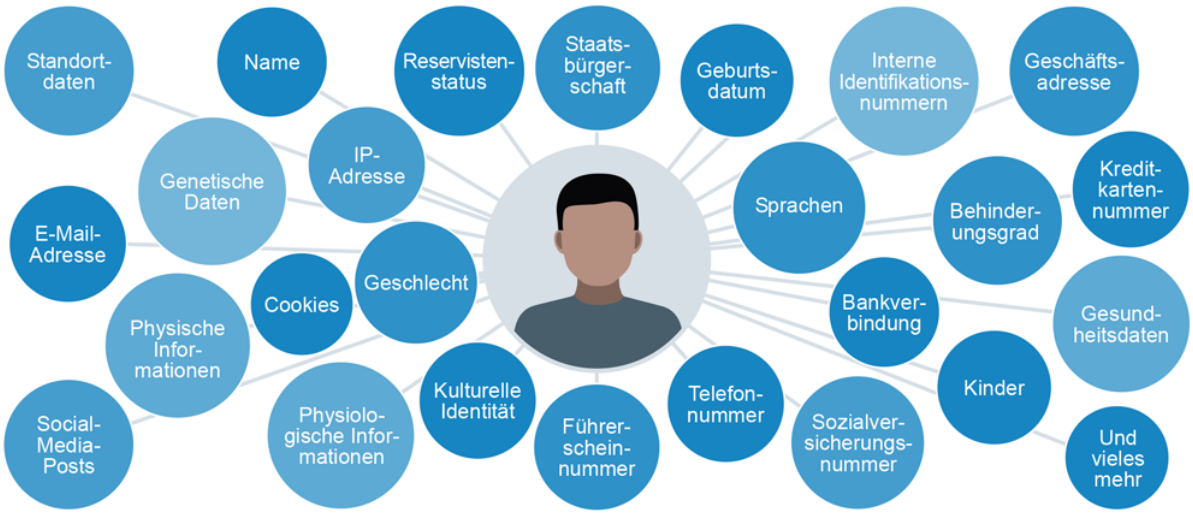
1 **Die DSGVO ist eine EU-Verordnung, die alles andere außer Kraft setzt:** Im Unterschied zur bisherigen EU-Richtlinie zum Datenschutz ist das neue Regelwerk eine EU-Verordnung. Das bedeutet, sie tritt nach einer zweijährigen Übergangszeit am 25. Mai 2018 sofort in Kraft tritt. Anders als bei einer Richtlinie sind dafür keine Vorschriften zur Umsetzung in nationales Recht nötig. Wie jede andere EU-Verordnung kann die DSGVO als eine Art europäisches Gesetz angesehen werden. Sie hat Vorrang vor den nationalen Gesetzen und allen bisherigen EU-Richtlinien.

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

3 **Explizite Einwilligung des Kunden:** Es muss ein ausdrückliches Einverständnis erteilt werden, und zwar sowohl mit der Datenerhebung als auch mit dem Zweck, für den diese Daten verwendet werden (DSGVO Artikel https://dsgvo-gesetz.de/art-83-dsgvo/ 7 https://dsgvo-gesetz.de/art-7-dsgvo/; definiert in Artikel 4 https://dsgvo-gesetz.de/art-4-dsgvo/). Zusätzlich muss der für die Verarbeitung Verantwortliche die Einwilligung (Opt-in) nachweisen können. Diese Einwilligung kann darüber hinaus widerrufen werden.

4 **Konformität auch außerhalb der EU:** Die alten Ausstiegsklauseln für außereuropäische Unternehmen gelten nicht mehr. Viele Nicht-EU-Firmen beriefen sich lange auf das Safe-Harbor-Abkommen, um die früheren EU-Datenschutzregeln einzuhalten. Die Europäische Kommission hatte im Juli 2000 entschieden, dass US-Unternehmen, die Safe Harbor beitreten und dessen Grundsätze einhalten, personenbezogene Daten aus der EU in die USA übertragen dürfen. Jedoch hob der Europäische Gerichtshof die Safe-Harbor-Datenschutz-Grundsätze am 24. Oktober 2015 auf. Anlass dafür war die Beschwerde eines Kunden, der seine Facebook-Daten als nicht ausreichend geschützt ansah.

5 **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."



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 ist diese Anforderung unmöglich zu erfüllen.

6 **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. Artikel 2: Sachlicher Anwendungsbereich

7 **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, (Daten-)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. Die Definition der betroffenen Person kann mit dem rechtlichen Konzept des Eigentümers, in diesem Fall der Daten, verglichen werden. Jeder Bürger, jede Bürgerin, der oder die sich im EU-Gebiet aufhält, ist eine betroffene Person: "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".
- Der Auftragsverarbeiter, englisch Data Processor, ist "eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet".

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 betroffene Personen, ebenso wie es die entsprechenden Gruppen bei Ihren Partnern sind.

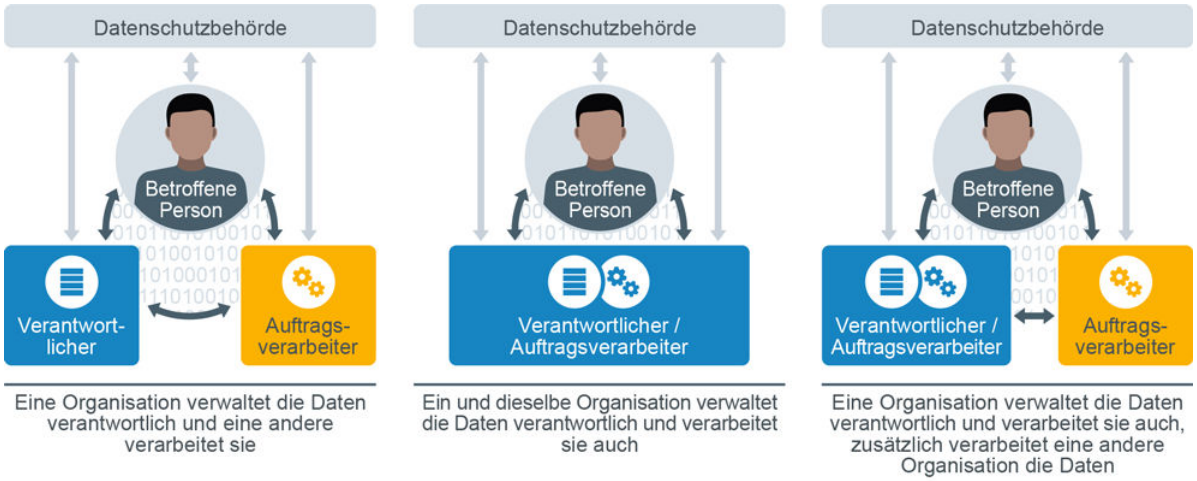
Artikel 4: Definitionen

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 einen Datenschutzbeauftragten (Data Protection Officer, DPO) zu benennen, der auch dann haftet, wenn die Organisation

- personenbezogene Daten von mehr als 5000 Datensubjekten pro Jahr verarbeitet,
- eine staatliche Organisation oder Behörde ist,
- hauptsächlich besondere Kategorien von Daten verarbeitet und
- eine umfangreiche regelmäßige und systematische Überwachung vorsieht.

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.



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 DocuWare Ihnen dabei hilft, 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 Dokumentenmanagement-System: Es digitalisiert nicht nur Papierakten, sondern nutzt auch Metadaten, um die Sicherheit und Governance zu gewährleisten, die zum Schutz von Kundendaten erforderlich sind.

Mit DocuWare steuern Sie, was mit Ihren Dokumenten und Daten geschieht - und mit diesem Ansatz unterstützt DocuWare direkt Ihre Projekte zur DSGVO-Compliance. So lassen sich in DocuWare 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**. Da die DSGVO aber auch für **Papierdokumente** gilt, die in einer Organisation vorgehalten werden, ist dies leichter gesagt als getan - falls Sie nämlich noch Prozesse auf Papier verwalten.

Wie DocuWare Ihre Compliance unterstützt

Mit DocuWare 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. DocuWare automatisiert das Archivieren, Suchen, Finden, Exportieren, Korrigieren und Löschen von persönlich identifizierbaren Informationen.

Das macht diesen Prozess unabhängig von Individuen. Stattdessen wendet DocuWare die Datenschutz-Richtlinien Ihres Unternehmens oder Ihrer Behörde an. Der automatisierte Ansatz zum Schutz von personenbezogenen Daten bringt Ordnung, Konsistenz und Effizienz in Ihre Geschäftsprozesse. 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.

DocuWare Intelligent Indexing automatisiert 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 kann DocuWare 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 "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 innerhalb von 30 Tagen tun.

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 Vergessenwerden. Sie können eine Löschaufforderung nur ablehnen, wenn gesetzliche Verpflichtungen, öffentliches Interesse oder gesetzliche Ansprüche dem entgegenstehen.

Wie DocuWare Ihre Compliance unterstützt

Jede Anfrage zum Exportieren, Korrigieren oder Löschen von personenbezogenen Daten kann in DocuWare 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 dem Modul DocuWare Request ist die Datenübertragbarkeit gewährleistet. Sie können alle persönlich identifizierbaren Informationen einfach **exportieren und übertragen**.

Artikel 20: Recht auf Datenübertragbarkeit

Der DocuWare Viewer stellt 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 den 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 DocuWare Workflow eine solche Aktion automatisch anstoßen, sobald der Datenschutzbeauftragte bestätigt, dass die Anfrage berechtigt ist.

Um alle relevanten Daten zu **korrigieren**, können die in DocuWare 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.

DocuWare kann 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.

DocuWare führt eine vollständige **Historie** aller Anfragen zur Berichtigung von Daten. Ist die Korrekturanfrage einer Person nicht gerechtfertigt, kann DocuWare 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 DocuWare Ihre Compliance unterstützt

DocuWare 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 DocuWare-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 DocuWare 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.

3 Entwerfen Sie eine unternehmensweite Compliance-Strategie

Der Einsatz eines Dokumentenmanagement-Systems wie DocuWare 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 Dokumentenmanagement-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.

Artikel 30: Verzeichnis von Verarbeitungstätigkeiten

Führen Sie außerdem eine Risikobewertung nach Artikel 35 durch. Der Bitkom-Leitfaden Risk Assessment & Datenschutz-Folgenabschätzung unterstützt Sie dabei.

Weiterführende Informationen

- Wortlaut der EU-Datenschutz-Grundverordnung (deutsch und englisch, mit Inhaltsverzeichnis und Suchfunktion)
- E-Book „Datenschutz und Sicherheit – Die DSGVO ist nur die Spitze des Eisbergs“ des Branchenverbandes AIIM International
- To-do-Liste DSGVO von Rechtsanwalt Rolf Becker
- EU-Kommission: DSGVO-Download in allen EU-Sprachen