windream GmbH – Whitepaper

Das ECM-System windream im Kontext der EU-Datenschutzgrund-verordnung

windream GmbH, Bochum

windream GmbH
Wasserstr.219
44799 Bochum

Wichtige Hinweise

Alle Informationen und technischen Angaben dieser Beschreibung wurden von den Autoren mit größter Sorgfalt zusammengetragen. Sie können jedoch weder Garantie noch juristische Verantwortung oder irgendeine Haftung für Folgen, die auf fehlerhafte Angaben zurückgehen, übernehmen.

Wir weisen darauf hin, dass die in dieser Beschreibung verwendeten Soft- und Hardwarebezeichnungen und Markennamen der jeweiligen Firmen im Allgemeinen einem Warenzeichen-, Marken- oder Patentrechtschutz unterliegen.

Stand: 04/2018

Inhalt

Das ECM-System windream im Kontext der EU-Datenschutzgrundverordnung (EU-DSGVO)

Management Summary

Zusammenfassung des Inhalts dieses Dokuments

Von den Anforderungen der EU-DSGVO sind faktisch alle Unternehmen betroffen. Bei Datenschutzverletzungen drohen hohe Bußgelder.

Um die Hürden der Verordnung elegant zu meistern, unterstützt das ECM-System windream alle Anwender, die sich mit der EU-DSGVO beschäftigen müssen. Im Rahmen konkreter Anwendungsfälle zeigt dieses Dokument auf, wie windream die Anwender unterstützt, und zwar auch dann, wenn sich Unternehmen bisher entweder noch gar nicht oder nur rudimentär mit den neuen Datenschutzbestimmungen auseinandergesetzt haben.

In diesem Kontext kommt es darauf an, ein System einzusetzen, das so intuitiv bedienbar ist, dass der Anwender seine Arbeit wie gewohnt weiterführen kann und sich nicht auf eine neue Arbeitsweise einstellen muss. Genau diesen Aspekt erfüllt windream exakt.

Einführung

Die EU-Datenschutzgrundverordnung (EU-DSGVO) ist eine Verordnung der Europäischen Union, mit der die gesetzlichen Regelungen zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Die Verordnung tritt am 25. Mai 2018 in Kraft und wird damit das bisher geltende Bundesdatenschutzgesetz (BDSG) ablösen. Die EU-DSGVO wird ab diesem Termin für alle Mitgliedsstaaten der Europäischen Union verbindlich sein. Zweck der Verordnung ist es, erstmals den Schutz personenbezogener Daten innerhalb der gesamten Europäischen Union auf eine für alle Mitgliedsstaaten einheitliche gesetzliche Basis zu stellen.

Das Bundesdatenschutzgesetz „neu“

Im Kontext der neuen EU-DSGVO wurde das bisher geltende Bundesdatenschutzgesetz an die EU-DSGVO angepasst. Der Grund besteht darin, dass die EU-Verordnung rund 50 so genannte Öffnungsklauseln nennt. Diese Klauseln ermöglichen es den EU-Mitgliedsstaaten, ihre eigene Datenschutzgesetzgebung an die EU-Verordnung anzupassen bzw. zu ergänzen, sofern diese Ergänzungen nicht im Widerspruch zu den Inhalten der Verordnung stehen. In Deutschland bestehen diese Ergänzungen in einer überarbeiteten Fassung des Bundesdatenschutzgesetzes, dem so genannten BDSG-neu (offizielle Bezeichnung: *Gesetz zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680* bzw. *Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU*) vom 30. Juni 2017.

Auswirkungen auf die geltende Rechtsprechung

Zum aktuellen Zeitpunkt ist es schwierig zu prognostizieren, ob es mit Inkrafttreten der EU-DSGVO in Deutschland eine veränderte Rechtsprechung im Bereich des Datenschutzes geben wird, da die EU-DSGVO ja neu und somit das BDSG erst noch ablösen wird. Selbstverständlich wird und muss eine zukünftige Rechtsprechung aber immer auf der Basis der EU-DSGVO erfolgen.

Es gilt somit festzuhalten, dass die Rechtsprechung bis jetzt nach dem BDSG erfolgte. Rechtsexperten gehen davon aus, dass die aktuelle Rechtsprechung (nicht die Gesetzgebung!) auch weiterhin zunächst auf dieser Basis erfolgen wird und zukünftige gerichtliche Urteile, die auf der gesetzlichen Basis der EU-DSGVO ausgesprochen werden, in ihrer Begründung häufig auf bereits gefällte Urteile nach dem BDSG verweisen.

Eine Kommentierung der EU-DSGVO gibt es bisher (noch) nicht

Da die EU-DSGVO erst am 25. Mai 2018 in Kraft tritt, gibt es zum jetzigen Zeitpunkt noch keinerlei Interpretationen oder Kommentierungen der Verordnung, obwohl Gesetzeskommentare in der juristischen Praxis überaus wichtig sind. Erst nach Inkrafttreten der EU-Verordnung wird sich eine Rechtsprechung herausbilden, die präzisere und konkrete Interpretationen der EU-DSGVO zulassen wird.

Hinweis: Eine sehr wichtige Tatsache darf an dieser Stelle nicht unerwähnt bleiben:

Wie schon das BDSG, so gelten die Bestimmungen der neuen EU-DSGVO nur, wenn nicht andere Gesetze oder Vorschriften der Verordnung entgegenstehen (zum Beispiel finanz- und steuerrechtliche Bestimmungen wie die GoBD in Deutschland).

Auswirkungen auf Unternehmen

Dass die neue EU-Datenschutzgrundverordnung Ende Mai 2018 wirksam wird, sollte mittlerweile in jedem Unternehmen bekannt sein. Nach den Ergebnissen der Umfragen verschiedenster Analysten ist jedoch immer noch davon auszugehen, dass sich bisher noch längst nicht alle Unternehmen adäquat auf die neue Verordnung vorbereitet haben, obwohl so gut wie alle unmittelbar davon betroffen sind. Ein Grund dafür ist sicherlich, dass eine allgemeine Unsicherheit darüber besteht, wie bzw. mit welchen Mitteln eine Umsetzung der Verordnung gesetzeskonform realisiert werden kann. Genau dieser Unsicherheit wollen wir mit dem vorliegenden Dokument so weit wie möglich entgegenwirken und zeigen auf, dass windream die Anwender konsequent bei der Umsetzung der neuen Bestimmungen unterstützt.

ECM-Systeme bieten Hilfestellung

Es wird häufig übersehen, dass längst moderne, IT-gestützte Systeme wie windream existieren, die nicht nur den betrieblichen Datenschutzbeauftragten, sondern generell alle Anwender in Unternehmen dabei unterstützen, die Anforderungen der Verordnung umzusetzen. Um den geforderten Schutz personenbezogener Daten zu gewährleisten, bietet ein ECM-System wie windream eine wertvolle Hilfe.

Mit dem vorliegenden „Whitepaper“ wollen wir über die wichtigsten Anforderungen der neuen EU-DSGVO informieren und aufzeigen, wie ein ECM-System wie windream dazu beitragen kann, die gesetzlichen Anforderungen zu erfüllen.

Dokumentationspflichten im Fokus

Allein die Tatsache, dass die Verordnung eine umfassende, nachvollziehbare Dokumentation aller Prozesse verlangt, die im Zusammenhang mit personenbezogenen Daten stehen, führt dazu, dass der Einsatz eines spezialisierten Systems zur Informationsverwaltung im Vordergrund aller Aktivitäten stehen muss. Hier kann „Enterprise Content Management“ (ECM) mit windream seine Stärken voll ausspielen. Und zwar insbesondere dann, wenn zum Beispiel Aspekte wie eingeschränkte Zugriffsberechtigungen durch ein restriktives Rechtekonzept, die lückenlose Nachvollziehbarkeit dokumentbezogener Prozesse oder auch die adäquate Sperrung bzw. Löschung personenbezogener Informationen wichtig werden. All diese Aspekte sind unmittelbar mit den Anforderungen der EU-DSGVO verknüpft.

Im Folgenden werden einige Beispiele erläutert, die – ganz konkret – in direktem Zusammenhang mit den einzelnen Artikeln der EU-DSGVO stehen und die – ebenfalls ganz konkret – aufzeigen, wie das ECM-

System windream Unternehmen bei der Umsetzung der Grundverordnung unterstützt.

Vollständige Übersicht über Verarbeitungstätigkeiten

Artikel 30 der EU-DSGVO fordert eine umfassende Übersicht und Beschreibung aller Verarbeitungstätigkeiten, die im Zusammenhang mit personenbezogenen Daten stehen. Diese Anforderung ist nicht neu, auch das bis Ende Mai 2018 noch geltende Bundesdatenschutzgesetz fordert eine derartige Übersicht. Aber: Artikel 30 präzisiert die Inhalte, zum Beispiel Namen und Kontaktdaten des Verantwortlichen im Unternehmen, die Zwecke der Verarbeitung, eine Beschreibung der Kategorien betroffener Personen und Daten, die Kategorien von Empfängern und vieles mehr.

Datenkategorien, Dokument-Historien und Änderungsnachweise

Zur Erfassung und Dokumentation dieser Prozesse lässt sich windream ideal verwenden. Das betrifft nicht nur die Verwaltung der Prozessbeschreibungen an sich, sondern auch eine mögliche Indexierung der prozessbeschreibenden Dokumente nach den in der Verordnung exakt definierten Datenkategorien.

Sofern Änderungen oder Erweiterungen der bestehenden Dokumente notwendig sein sollten, die Verarbeitungstätigkeiten im Sinne des Artikel 30 beschreiben, so lassen sich auch diese Änderungen durch eine lückenlose Dokument-Historie nachweisen. Ein gutes ECM-System wie windream ist jederzeit in der Lage, einen vollständigen Nachweis über Änderungen bzw. Erweiterungen quasi „auf Knopfdruck“ zu liefern.

Effizientes Vertragsmanagement im Sinne der Auftragsdatenverarbeitung (ADV)

Das ECM-System windream ist in der Lage, auch ganz spezielle elektronische Akten oder Dokument-Kategorien elegant zu managen und zu systematisieren, zum Beispiel Verträge. „Vertragsverwaltung“ lautet hier das zentrale Stichwort. Konkret geht es darum, elektronische Vertragsakten so anzulegen und zu verwalten, dass die mit ihnen assoziierten Dokumente und deren Inhalte ohne zeitliche Verzögerung verfügbar gemacht werden können. Dies gilt insbesondere für den Nachweis gegenüber den Datenschutz-Aufsichtsbehörden und für die Erfüllung des Artikels 28 der EU-DSGVO.

ADV-Verträge sind Pflicht

Für den Fall, dass Unternehmen – sei es als Auftraggeber, Auftragnehmer oder als Subunternehmer – personenbezogene Daten

im Auftrag verarbeiten, fordert die EU-DSGVO in Artikel 28 ein umfassendes Vertragswerk für jede Art der Auftragsdatenverarbeitung (ADV). Stellt eine Aufsichtsbehörde fest, dass zu einer ADV kein Vertrag geschlossen wurde oder dass ein Vertrag nicht auffindbar ist, so kann dies – je nach Einzelfall - mit hohem Bußgeld sanktioniert werden.

Durch den Einsatz des windream ECM-Systems mit integrierter Vertragsverwaltung lässt sich dieses Risiko deutlich minimieren, indem die ADV-Verträge sicher in windream archiviert werden.

Beide Vertragsparteien in der Haftung

Dazu noch ein weiterer wichtiger Hinweis: Das frühere (bis Ende Mai 2018) geltende Bundesdatenschutzgesetz sah bisher vornehmlich den Auftraggeber in der Pflicht zur Kontrolle und Einhaltung des Datenschutzes durch den Auftragnehmer. Die EU-DSGVO hingegen verpflichtet beide Vertragsparteien gleichermaßen. Es gibt also keinen „Haftungsunterschied“ mehr zwischen Auftraggeber und Auftragnehmer; ein weiteres Kriterium, das – zumindest indirekt – für den Einsatz eines ECM-Systems zur Vertragsverwaltung auf beiden Seiten spricht.

Der Aspekt der Sicherheit in der Datenverarbeitung

„Safety first“ – das fordert auch die Grundverordnung, und zwar in Artikel 32. Dort geht es um die vollständige Beschreibung aller technisch-organisatorischen Maßnahmen, die ein Unternehmen treffen muss, um den angemessenen Schutz personenbezogener Daten sicherzustellen. Auch diese Anforderung ist aus dem Bundesdatenschutzgesetz schon bekannt, erfordert aber nichtsdestotrotz auch zukünftig eine vollständige Dokumentation.

Die Dokumentation technisch-organisatorischer Maßnahmen

Technisch-organisatorische Maßnahmen (kurz TOMs) unterliegen normalerweise einem stetigen Wandel. Denn sie müssen ständig angepasst, erweitert und verändert werden; sei es etwa aufgrund neuer Einbruch-Sicherungsmaßnahmen im Unternehmen, durch eine Erweiterung der Geschäftsräume in Verbindung mit baulichen Maßnahmen, aufgrund eines kompletten Firmenumzugs oder auch durch Modifikationen der IT-Infrastruktur.

windream bietet eine ideale Funktion, um genau diese Veränderungen dokumentarisch zu erfassen: die Versionierung von Dokumenten. Sie ermöglicht es, bestehende Beschreibungen zu erhalten und eine neue Version des jeweiligen bestehenden Dokuments zu erstellen, bevor das Dokument verändert bzw. um die Beschreibung neuer technischer Maßnahmen ergänzt wird. Zusammen mit der windream

Standardfunktion der Dokument-Historie ergibt sich ein vollständiger Nachweis darüber, wann, von wem und in welchem Ausmaß die Beschreibung der technisch-organisatorischen Maßnahmen geändert wurde.

Verwaltung von Einwilligungserklärungen

Gemäß Artikel 6 („Rechtmäßigkeit der Verarbeitung“) und Artikel 7 („Bedingungen für die Einwilligung“, dort unter (1)) kann die Verarbeitung personenbezogener Daten auch durch die Einwilligungserklärung des Betroffenen autorisiert sein. Artikel 7 (1) schreibt in diesem Kontext vor, dass der Verantwortliche das Einverständnis des Betroffenen explizit nachweisen muss. Das Problem dabei: Die EU-DSGVO schreibt prinzipiell nicht vor, dass eine Einwilligung schriftlich zu erfolgen hat. Wie aber soll man im Zweifelsfall eine Einwilligung nachweisen, die nicht in Schriftform vorliegt? Deshalb gilt: Ohne schriftliche Einwilligungserklärung ist kein Nachweis möglich!

Administrationsaufwand reduzieren

Erfahrungsgemäß – das zeigt sich im Alltag eines Datenschützers immer wieder – erfordert die Verwaltung der Einwilligungserklärungen einen beträchtlichen Administrationsaufwand. Er liegt auch darin begründet, dass Einwilligungen immer zweckgebunden sein müssen, also auf einen bestimmten Aspekt der Datenverarbeitung beschränkt sind (z.B. Einwilligungen zur Veröffentlichung von Mitarbeiterfotos im Intranet, Zustimmung zur Veröffentlichung personenbezogener Daten in einem Newsletter und vieles mehr). Jede Änderung eines Zwecks und somit auch jeder „neue Zweck“ erfordert die Einholung einer erneuten Einwilligungserklärung – von allen betroffenen Personen.

Auch ein ECM-System kann einem Datenschutzbeauftragten diese Arbeit nicht abnehmen, aber es hilft ungemein dabei, die „eingeholten“ Erklärungen zu verwalten; zum Beispiel durch eine systematische Ablage in einem Personenregister oder durch eine elektronische Akte (siehe oben) in windream, auf die nur der Datenschutzbeauftragte zugreifen kann. Das dazu erforderliche Recht lässt sich anhand eines Rechtekonzepts innerhalb des ECM-Systems bequem regeln. Die Mechanismen des windream ECM-Systems greifen also auch in diesem Fall.

Das Recht auf Löschung und „Vergessenwerden“

Grundsätzlich haben Betroffene nach Artikel 17 EU-DSGVO das Recht, eine Löschung ihrer personenbezogenen Daten zu verlangen, sofern einer der in diesem Artikel genannten Gründe zutrifft.

Hinweis: Wie schon eingangs erwähnt, ist eine Löschung personenbezogener Daten nur erlaubt, wenn keine anderen Gesetze oder Vorschriften dem entgegenstehen (zum Beispiel finanz- und steuerrechtliche Bestimmungen wie die GoBD in Deutschland).

Während sich das Recht auf Vergessenwerden „nur" auf „öffentlich gemachte" Daten bezieht, zum Beispiel in sozialen Netzwerken, kann die Datenlöschung aus einem ECM-System wesentlich einfacher und – je nach Anforderung – auch automatisiert erfolgen. Abgesehen von einem Entzug aller Rechte, die eine Einsichtnahme in die Daten für alle Anwender wirksam unterbindet, ist eine Löschung auch auf anderen technischen Wegen innerhalb des ECM-Systems windream möglich, beispielsweise durch ein automatisiertes Konzept auf der Basis von Lebenszyklus-Einstellungen für Dokumente. Diese Einstellungen ermöglichen es, Daten automatisch nach einer definierten Frist zu löschen, etwa nach Entfall des Zwecks, für den die Datenspeicherung vorgesehen war.

Löschvorgänge protokollieren

Generell gilt aber: Auch der Prozess einer Datenlöschung muss dokumentiert werden. Diese Anforderung ergibt sich aus § 76 des BDSG-neu, also aus der angepassten Version des BDSG, das die EU-DSGVO über eine Öffnungsklausel (wie bereits eingangs beschrieben) ergänzt und konkretisiert. § 76 präzisiert die Protokollierung eines Löschvorgangs insofern, als er vorschreibt, dass in einem Unternehmen nur der Datenschutzbeauftragte die Protokolle der Löschprozesse verwalten darf.

Die Rolle des Administrators

Im Umkehrschluss ergibt sich daraus, dass die Verwaltung der Löschprotokolle nicht in der Hand zum Beispiel eines Administrators liegt. Zwar befindet sich der Systemadministrator in Bezug auf die IT-Infrastruktur eines Unternehmens in einer durchaus herausragenden Rolle, da er zum Beispiel für Datenhaltung, Datensicherheit, Datenverfügbarkeit, Systemwartung und damit auch für die Löschvorgänge „per se" verantwortlich ist. Diese Rolle ist aber streng von der Verantwortlichkeit eines betrieblichen Datenschutzbeauftragten abzugrenzen.

Hintergrund: Grundsätzliches zum Thema Löschen und Revisionssicherheit

Grundsätzlich widerspricht der Gedanke der Löschung dem Zweck einer revisionssicheren Archivierung, bei dem gerade verhindert werden soll, dass Dokumente in irgendeiner Form geändert, manipuliert oder gelöscht werden können. Stichworte sind hierbei „Vollständigkeit", „Unveränderbarkeit" oder auch „zeitnahes Auffinden". Dazu verwendet windream eine Menge unterschiedlicher Mechanismen, um diese Aspekte sicherzustellen und ein unberechtigtes

Löschen zu verhindern. Dies gilt insbesondere für z.B. steuerrelevante Unterlagen, Kreditakten und für die Einhaltung der GoBD-Vorschriften, für die eine revisionssichere Ablage unerlässlich ist.

Erschwerend kommt hinzu, dass es z.B. im Steuerrecht keine klare Definition gibt, welche Unterlagen als steuerrelevant einzustufen sind. Dies hat den Sinn, dass die Finanzbehörde zu jeder Zeit die Möglichkeit hat, eine Unterlage als steuerrelevant zu deklarieren.

Aus diesem Grund muss **vor** einem Löschvorgang unbedingt geprüft werden, ob der geplanten Löschung personenbezogener Daten nach der EU-DSGVO eine andere Gesetzgebung entgegensteht, die eine Löschung für unzulässig erklärt.

Widersprechende Gesetzgebungen

Wie gerade dargestellt, widerspricht z.B. die Aufbewahrungspflicht von steuerrelevanten Unterlagen dem „Recht auf Vergessen / Löschen“ der EU-DSGVO. Und dies ist nur ein offensichtlicher Konflikt mit anderen Gesetzgebungen.

Wichtiger Hinweis: An dieser Stelle ist die EU-DSGVO aber eindeutig und sagt, dass im Falle eines solchen Widerspruchs zu einer anderen Gesetzgebung kein Anspruch auf Löschung der Daten besteht.

Der Begriff des Löschens

Löscht man ein Dokument aus einem normalen Dateisystem, so wird das Dokument (unter Windows) zunächst in den Papierkorb verschoben und kann von dort aus noch wiederhergestellt werden. Wird das Dokument jedoch auch aus dem Papierkorb gelöscht, so wird auch der Verweis auf das Dokument aus dem Verzeichnis auf der Festplatte entfernt. Das Dokument wird dadurch nicht mehr im System gelistet und ist somit auf normalem Wege nicht mehr zugreifbar. Das heißt: Nach dem Löschvorgang sind die Daten physisch zwar weiterhin noch vorhanden, gelten aber als „gelöscht“.

Dies wurde in der bisherigen Rechtsprechung auf der Basis des BDSG ebenso gesehen. Der Prozess des „Löschens“ ist also durchaus als pragmatisch zu interpretieren, und es ist zu erwarten, dass sich dies auch mit der Rechtsprechung nach der neuen EU-DSGVO nicht wesentlich ändern wird.

Der Konflikt zwischen Löschung und Backup

In Bezug auf hochsensible Systeme gibt es eine spezielle Definition für Löschvorgange. Siehe hierzu https://www.haufe.de/unternehmensfuehrung/profirma-professional/dateien-und-datentraeger-sicher-loeschen-3-standards-und-verfahren-zum-sicheren-loeschen_idesk_PI11444_HI2288085.html.

In dem unter diesem Link erreichbaren Beitrag werden auch verschiedenste Standardmethoden beschrieben, die ein sicheres Löschen ermöglichen, zum Beispiel gemäß den Richtlinien des BSI.

Ein weiterer Aspekt bei restriktiver Interpretation des Löschbegriffs sind Backups. Aus diesen müssten dann auch die zu löschenden Informationen entfernt werden, was aber einerseits technisch nahezu unmöglich sowie andererseits vom Aufwand her offensichtlich nicht leistbar ist.

Ein „österreichischer" Ansatz zur Konfliktlösung

Erleichternd und – bis zu einem gewissen Grad problemlösend – könnte ein Interpretationsansatz sein, der von österreichischer Seite kommt (siehe https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-datenschutz-anpassungsgesetz-2018.html). Dabei handelt es sich um das österreichische Anpassungsgesetz 2018 zur EU-DSGVO, also um das österreichische Pendant zum deutschen „BDSG-neu". In der österreichischen Anpassung an die EU-DSGVO wird argumentiert, dass der Zugriff auf personenbezogene Daten auch eingeschränkt werden könnte, sofern eine Löschung nicht unverzüglich erfolgen kann, weil sie aus wirtschaftlichen oder technischen Gründen nur zu bestimmten Zeiten möglich ist.

Ein österreichischer Rechtsexperte interpretierte diese Überlegungen so, dass personenbezogene Daten in Backups ja mit der Zeit und abhängig vom jeweiligen Backup-Konzept aus den Backups „herauswachsen", sie also z.B. nach mehrmaligem Überschreiben der Backup-Medien bzw. nach Ablauf einer bestimmten zeitlichen „Backup"-Frist „automatisch" nicht mehr vorhanden sind.

Betonung der Verhältnismäßigkeit im BDSG-neu

Ein ähnlich pragmatischer Ansatz findet sich allerdings auch in den Ausführungen des deutschen BDSG-neu, und zwar in § 58 (*Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung*, Absatz 1). Dort heißt es, dass an die Stelle einer Löschung auch eine „eingeschränkte" Verarbeitung treten kann, wenn eine Löschung nicht oder nur mit „unverhältnismäßigem Aufwand" möglich ist - ein ganz klarer Hinweis darauf, dass sich der Begriff des Löschens als durchaus „dehnbar" interpretieren lässt.

Somit kann man im Sinne der EU-DSGVO von einem „normalen" Löschen personenbezogener Daten ausgehen, wenn die Daten nicht mehr für Anwender sichtbar, recherchierbar und von daher auch nicht zugreifbar sind. Die bisherige Rechtsprechung auf der Basis des „alten" BDSG hat übrigens diese Sichtweise bisher ebenfalls untermauert.

Keine Präzisierung in der EU-DSGVO

Tatsache ist, dass die EU-Datenschutzgrundverordnung auf derartige Verfahren und Konflikte überhaupt keinen Bezug nimmt, also den Begriff des „Löschens" nicht präzisiert und deshalb viel Raum für

Spekulationen und Interpretationen lässt. Erst die zukünftige Rechtsprechung wird (hoffentlich) zeigen, wie dieser Konflikt konkret zu interpretieren ist.

Ablauf eines Löschvorgangs

Auf Basis der vorstehenden Argumentation und Diskussion sollte der Prozess des Löschens personenbezogener Daten etwa folgendermaßen ablaufen:

1. Ausgangssituation: Ein Betroffener verlangt die Löschung seiner personenbezogenen Daten.
2. Die Forderung wird durch den Datenschutzbeauftragten registriert, dokumentiert und an die verantwortlichen Personen weitergeleitet.
3. Die verantwortlichen Personen im Unternehmen prüfen, ob die Forderung rechtmäßig ist oder ob andere geltende Gesetze einer möglichen Löschung widersprechen.
4. Nach der Prüfung mit dem Ergebnis, dass die angeforderte Löschung rechtmäßig ist, wird die Löschung durchgeführt und protokolliert. Deutet das Ergebnis der Prüfung auf eine unrechtmäßige Löschung hin, so wird keine Löschung veranlasst.
5. Der Betroffene wird durch den betrieblichen Datenschutzbeauftragten oder durch die verantwortliche Stelle über die erfolgte Löschung informiert. Ist eine Löschung aufgrund einer anderweitigen Gesetzgebung als unzulässig einzustufen, so wird der Betroffene darüber informiert, dass eine Löschung aufgrund einer entgegenstehenden Gesetzgebung nicht möglich ist.
6. Der betriebliche Datenschutzbeauftragte archiviert das Löschprotokoll an einem nur für ihn zugreifbaren Speicherort, um den Löschvorgang aufgrund der Dokumentationspflichten auch zu einem späteren Zeitpunkt noch nachweisen zu können.

Widerspruchsrecht, Folgenabschätzung und Transparenz

Generell lassen sich natürlich alle Dokumente in windream erstellen und verwalten, die im Kontext der EU-Verordnung relevant sind – und das mit allen Vorteilen, die ein ECM-System bietet: vom Rechtekonzept über die Dokument-Historie, Versionierung und die Indexierung zum schnellen Wiederauffinden von Informationen bis hin zu den Lebenszyklus-Einstellungen für automatisierte oder auch manuelle Datenlöschungen.

Drei weitere Aspekte sind vor diesem Hintergrund auf jeden Fall aber noch diskussionswürdig.

Widerspruchsrecht

Nach Artikel 21 haben Betroffene das Recht, einer Speicherung ihrer Daten zu widersprechen, insbesondere nach Absatz (2), der sich auf Maßnahmen der Direktwerbung bezieht. Widersprüche von Betroffenen sollten protokolliert und zum Beispiel in einem durch entsprechende Zugriffsrechte geschützten Ordner eines ECM-Systems abgelegt werden. Gleiches gilt für festgestellte Datenschutzverletzungen, die möglicherweise gegenüber den Aufsichtsbehörden meldepflichtig sind, und für Aussagen von Betroffenen.

Datenschutz-Folgenabschätzungen

Auch Datenschutz-Folgenabschätzungen gemäß Artikel 35 müssen schriftlich dokumentiert werden. Folgenabschätzungen sind immer im Vorfeld der Einführung neuer Technologien notwendig, zum Beispiel vor der Einführung einer geplanten Videoüberwachung zur Objektsicherung oder vor der Einführung neuer Software, mit der personenbezogene Daten verarbeitet werden; klassischer Fall: die Einführung eines neuen CRM- oder ERP-Systems.

Transparenzpflicht

Und, last not least, muss immer auch die Transparenzpflicht nach Artikel 12 (1) befolgt werden. Demnach sind Auskünfte über gespeicherte Daten den Betroffenen „in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln“ – so der Originalton der EU-Datenschutzverordnung. Auch daran sollte man bei der Dokumentation datenschutzrelevanter Aspekte denken.

Weitere rechtliche Hinweise

Keine Rechtsberatung durch die windream GmbH

Die windream GmbH ist als Software-Hersteller nicht berechtigt, eine Rechtsberatung durchzuführen. Somit haben die in diesem Dokument enthaltenen Informationen keinen rechtsberatenden Charakter. Die Begriffsdeutungen und die Interpretation der einzelnen Artikel der EU-DSGVO sind keine rechtsverbindlichen Auskünfte, sondern reflektieren lediglich die Meinung und Auslegung der Verordnung aus Sicht der windream GmbH.

Anpassung an nationales Recht

Die EU-DSGVO sieht mit ihren Öffnungsklauseln ausdrücklich vor, dass die Bestimmungen von den Regierungen der EU-Mitgliedsstaaten an nationales Recht angepasst werden können (in Deutschland das *Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU* vom 30. Juni 2017).

Spezielle Regelungen für die Verarbeitung besonderer personenbezogener Datenkategorien

Spezielle gesetzliche Regelungen gelten für alle Branchen, in denen besondere Kategorien personenbezogener Daten verarbeitet werden (z.B. Banken, Krankenhäuser usw.). Gerade in Bezug auf das Löschen von Informationen von Datenträgern gibt es in diesen Branchen Anforderungen, die weit über die Anforderungen der EU-DSGVO hinausgehen können (z.B. mehrfaches Überschreiben mit Zufallsdaten).

Weiterführende Links

- Der Originaltext der EU-DSGVO ist unter dem folgenden Link abrufbar: http://eur-lex.europa.eu/legal-content/DE/TXT/?qid=1462345886854&uri=OJ:JOL_2016_119_R_0001
- Der Text des an die EU-DSGVO angepassten BDSG (*BDSG-neu* bzw. *Datenschutz-Anpassungs- und -Umsetzungsgesetz EU – DSAnpUG-EU* vom 30. Juni 2017) kann als PDF-Datei unter folgendem Link heruntergeladen werden: https://www.ldi.nrw.de/mainmenu_Aktuelles/Inhalt/Neues-Bundesdatenschutzgesetz/BDSG-neu.pdf
- Für Interessenten in Österreich bietet die österreichische Wirtschaftskammer weitere detaillierte Informationen zur EU-DSGVO unter dem folgenden Link an: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-datenschutz-grundverordnung.html.

Fazit: Effiziente Umsetzung der EU-DSGVO mit windream

Die vorgenannten Aspekte der EU-DSGVO zeigen in aller Deutlichkeit, dass eine systematische, konsequente, nachhaltige, rechtskonforme und auch benutzerfreundliche Umsetzung der EU-Datenschutzgrundverordnung nur mit einem Software-Tool erfolgen kann, das all diesen Anforderungen gerecht wird. Im Kontext aller auf dem Markt erhältlichen Systeme sind diejenigen besonders hervorzuheben, die sich kompromisslos auf das Management von Informationen spezialisiert haben – und das sind Enterprise-Content-Managementsysteme wie windream.

Unternehmen, die sich bisher schon um den Datenschutz wie vom Gesetz gefordert gekümmert haben, sollten auch in Zukunft trotz der im Vergleich zum BDSG höheren Sanktionen nichts zu befürchten haben. Dennoch ist es unumgänglich, seine Datenschutzpraxis zu überprüfen und das Datenschutzmanagement bis zum 25. Mai 2018 nach den Vorgaben der EU-DSGVO anzupassen und weiterzuentwickeln. Dabei gibt es keine Musterlösung, da jedes Unternehmen durch sein individuelles Geschäftsmodell auch unterschiedliche Datenverarbeitungsvorgänge durchführt.

windream als „Best-Practice“-Lösung

Die konkrete Umsetzung der Datenschutz-Maßnahmen, die ein Unternehmen im Sinne der EU-DSGVO zu realisieren und vor allem in Hinblick auf die damit verbundenen Dokumentationspflichten zu erfüllen hat, ist höchst individuell. Die Tatsache, dass windream universell einsetzbar, nicht auf bestimmte Einsatzbereiche beschränkt und individuell an die spezifischen Organisationsstrukturen eines Unternehmens anpassbar ist, macht das ECM-System zu einer Best-Practice-Lösung bei der Umsetzung der DSGVO-Anforderungen.

In diesem Kontext steht einmal mehr die vollständige Integration aller ECM-Funktionen in das Windows-Betriebssystem auf der Basis einer patentierten Software-Technologie im Vordergrund. Effizienter kann man die gesetzlichen Bestimmungen der neuen EU-Datenschutzgrundverordnung nicht umsetzen.