

Das ECM-System windream im Kontext der EU- Datenschutzgrundverordnung

windream GmbH – Whitepaper



Copyright © 2021

by
windream GmbH
Wasserstr.219
44799 Bochum

Stand: 10/2021 - 1.0.0.1

Alle Rechte vorbehalten. Kein Teil dieser Beschreibung darf in irgendeiner Form (Druck, Fotokopie oder einem anderen Verfahren) ohne Genehmigung der windream GmbH reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

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 Patentrechtsschutz unterliegen.

Irrtümer und kurzfristige Änderungen vorbehalten.

Inhalt

Das ECM-System windream im Kontext der EU-Datenschutzgrundverordnung

Das ECM-System windream im Kontext der EU-Datenschutzgrundverordnung (EU-DSGVO) 1

Management Summary 1

Einführung 1

Das Bundesdatenschutzgesetz „neu“ 2

Auswirkungen auf die geltende Rechtsprechung 2

Auswirkungen auf Unternehmen 2

ECM-Systeme bieten Hilfestellung 3

Dokumentationspflichten im Fokus 3

Vollständige Übersicht über Verarbeitungstätigkeiten 3

Datenkategorien, Dokument-Historien und Änderungsnachweise
4

Effizientes Vertragsmanagement im Sinne der

Auftragsdatenverarbeitung (ADV) 4

ADV-Verträge sind Pflicht 4

Beide Vertragsparteien in der Haftung 5

Der Aspekt der Sicherheit in der Datenverarbeitung 5

Die Dokumentation technisch-organisatorischer Maßnahmen 5

Verwaltung von Einwilligungserklärungen 6

Administrationsaufwand reduzieren 6

Das Recht auf Löschung und „Vergessenwerden“ 6

Löschvorgänge protokollieren 7

Hintergrund: Grundsätzliches zum Thema Löschen und
Revisionsicherheit 7

Der Begriff des Löschens 8

Ablauf eines Löschvorgangs 10

Widerspruchsrecht, Folgenabschätzung und Transparenz 10

Widerspruchsrecht 11

Datenschutz-Folgenabschätzungen 11

Transparenzpflicht 11

Weitere rechtliche Hinweise 11

Fazit: Effiziente Umsetzung der EU-DSGVO mit windream 12

windream als „Best-Practice“-Lösung 13

Anhang: windream-Funktionen zur Umsetzung der EU-DSGVO 14

Generell verwendbare windream-Features 14

Vollständige Übersicht über Verarbeitungstätigkeiten in windream 14

Vertragsmanagement in der Auftragsdatenverarbeitung 15

Beschreibung Ihrer technisch-organisatorischen Maßnahmen 16

Verwalten Sie Einwilligungserklärungen mit windream 17

Steuern Sie Löschprozesse 17

Rechte der Betroffenen 18

Unterstützung durch die windream GmbH 18

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 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 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 wurden. Die Verordnung trat am 25. Mai 2018 in Kraft und löste das bis zu diesem Zeitpunkt geltende Bundesdatenschutzgesetz (BDSG) ab. Die EU-DSGVO ist für alle Mitgliedsstaaten der Europäischen Union verbindlich. Zweck der Verordnung ist es, 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 EU-DSGVO wurde das früher 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

Die Rechtsprechung muss seit Inkrafttreten immer auf der Basis der EU-DSGVO erfolgen.

Es gilt somit festzuhalten, dass die Rechtsprechung früher 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.

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

Wie schon das BDSG, so gelten die Bestimmungen der 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

Nach den Ergebnissen der Umfragen verschiedenster Analysten ist davon auszugehen, dass sich bisher noch längst nicht alle Unternehmen adäquat auf die 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, wie windream die Anwender 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 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 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 forderte 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 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 grundsätzlich 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 Datenschutzers 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 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 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 früheren Rechtsprechung auf der Basis des BDSG ebenso gesehen. Der Prozess des „Löschen“ ist also durchaus als pragmatisch zu interpretieren, und es ist zu erwarten, dass sich dies auch mit der Rechtsprechung nach der EU-DSGVO nicht wesentlich ändern wird.

Der Konflikt zwischen Löschung und Backup

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). 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). In diesem Absatz (der eigentlich nur für öffentliche Stellen Gültigkeit hat) 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.

Ablauf eines Löschvorgangs

Auf Basis der vorstehenden Argumentation und Diskussion sollte der Prozess des Löschsens 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 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 entgegengesetzten Gesetzgebung nicht möglich ist.
6. Der 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-Datenschutzgrundverordnung. 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).

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 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.

Hinweis: Im nachfolgenden Teil dieses Dokuments werden konkrete windream-Funktionen vorgestellt, mit denen sich die Anforderungen der EU-DSGVO umsetzen lassen.

Anhang: windream-Funktionen zur Umsetzung der EU-DSGVO

Im weiteren Verlauf dieses Dokuments wollen wir aufzeigen, wie Anwender konkrete windream-Funktionen nutzen, um die Anforderungen der EU-DSGVO umzusetzen.

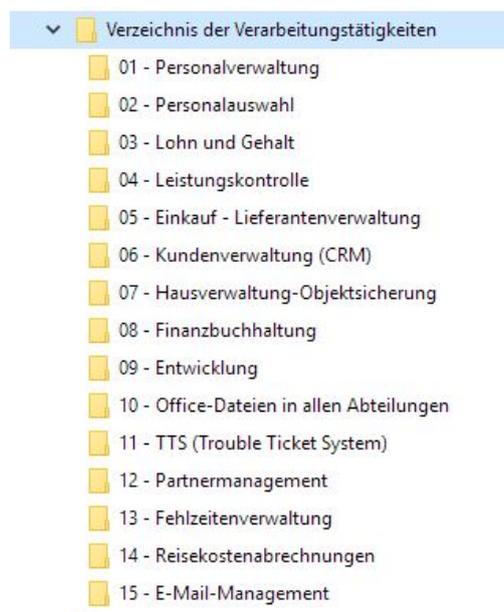
Generell verwendbare windream-Features

- Nutzen Sie das windream-Rechtekonzept zur Einschränkung der Rechte auf Dokumente durch ein ausgeklügeltes Konzept für den Datenschutz.
- Nutzen Sie die Dokument-Versionierung, um datenschutzrelevante Dokumente in verschiedenen Versionen vorzuhalten, zum Beispiel bei Änderungen oder Erweiterungen Ihrer technisch-organisatorischen Datenschutzmaßnahmen.
- Verwenden Sie die Dokument-Historie, um die „Entstehungsgeschichte“ datenschutzrelevanter Dokumente zur Erfüllung der Nachweispflichten zu verifizieren. Mit der Historie weisen Sie nach, welche Änderungen – auch der Metadaten – ein Dokument durchlaufen hat.
- Führen Sie einen Index ein, der Dokumente mit personenbezogenen Inhalten eindeutig kennzeichnet (z.B.: Indexierung mit einem möglichen Index "Personenbezogen" oder „Datenschutzrelevant“).
- Protokollieren Sie alle datenschutzrelevanten Vorgänge, und legen Sie z.B. einen Dokumenttyp „Protokoll“ mit den erforderlichen Indexwerten an.

Vollständige Übersicht über Verarbeitungstätigkeiten in windream

- Legen Sie in windream einen zentralen Ordner „Datenschutz“ an.
- Ordnen Sie die Dokumente Ihres Verfahrensverzeichnis und legen Sie für jedes beschriebene Verfahren einen separaten Ordner unterhalb des Ordners „Datenschutz“ an. Die Ordnernamen sollten mit der Nummer des jeweiligen Verfahrens beginnen, ebenso der Dateiname des jeweiligen Verfahrens, das in dem betreffenden Ordner gespeichert ist, z.B. Ordnername **01 – Personalverwaltung** und Dateiname **Verfahren 01 – Personalverwaltung**.

- Legen Sie einen Dokumenttyp für die Prozessdokumentation fest, und definieren Sie die für Sie erforderlichen Indexmerkmale für den Datenschutz. Der Dokumenttyp könnte z.B. Indexfelder wie „Verfahrensnummer“, „Thema des Verfahrens“ (z.B. „Urlaubsverwaltung“) und weitere Felder enthalten.
- Nutzen Sie die Dokument-Versionierung, um eine neue Version eines bestehenden Dokuments zur Verfahrensbeschreibung zu erstellen, bevor Sie Änderungen an einer Prozessbeschreibung vornehmen.



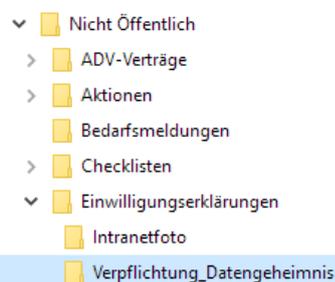
Beispiel eines Verfahrenszeichnisses in windream

Vertragsmanagement in der Auftragsdatenverarbeitung

- Nutzen Sie die Lösung der windream Vertragsverwaltung (windream Contract Management) zum Management Ihrer ADV-Verträge mit Kunden und Partnern.
- Oder erstellen Sie selber einen passenden Dokumenttyp für die Verträge mit den entsprechenden Metadaten.
- Als Indexfelder kämen z.B. „Name des Auftraggebers“, „Name des Auftragnehmers“, „ADV-Vertrag unterschrieben (ja/nein)“ oder „Datum“ sowie „Vertragsnummer“ in Frage.

Verwalten Sie Einwilligungserklärungen mit windream

- Verwalten Sie Einwilligungserklärungen als elektronische Akten in windream unter Berücksichtigung eingeschränkter Zugriffsrechte.
- Einwilligungserklärungen sollten nur vom Datenschutzbeauftragten verwaltet werden.
- Erstellen Sie einen passenden Dokumenttyp (z.B. den Dokumenttyp „Einwilligungserklärung“) für die Einwilligungserklärungen mit den entsprechenden Indexen zur schnellen Identifizierung von gespeicherten Erklärungen. Als Index könnten etwa Felder wie „Name des Betroffenen“, „Zweck der Datenspeicherung“ (z.B. Bild des Betroffenen im Intranet des Unternehmens etc.), „Funktion / Abteilung“ (im Unternehmen) und weitere Indexe stehen.
- Da Einwilligungserklärungen immer eine handschriftliche Unterzeichnung des Betroffenen erfordern, bietet es sich an, die Erklärungen mit der jeweiligen Unterschrift zu scannen und die Dokumente in einem separaten windream-Ordner abzulegen. Achten Sie auch hier auf eingeschränkte Zugriffsrechte.
- Nutzen Sie die Software-Lösungen windream Imaging oder windream connect, um den Prozess zwischen dem Einscannen der Erklärungen (mit Unterschrift des Betroffenen) und der Ablage als PDF-Datei automatisiert zu steuern.



Verwaltung von Einwilligungserklärungen in einem nicht öffentlichen Datenschutzordner des ECM-Systems windream

Steuern Sie Löschprozesse

- Definieren Sie einen Workflow-Prozess zur automatisierten Löschung von Dokumenten, z.B. im Falle des Widerspruchs eines Betroffenen (wie unter „[Ablauf eines Löschvorgangs](#)“ beschrieben).

- Erstellen Sie Löschrufen für das automatisierte Löschen von Dokumenten gemäß den Angaben in Ihrem Verfahrensverzeichnis. Dort müssen Sie Angaben zu den Löschrufen eintragen, um zu definieren, wie lange ein Dokument gespeichert werden darf oder muss.
- Stellen Sie sicher, dass Ihr DSB eine Prüfung der Löschrufen durchführen kann (z.B. als Schritt innerhalb des Workflows) und dass die Löschung protokolliert wird.
- Stellen Sie weiterhin sicher, dass die Löschrufen nur durch den DSB geführt werden und auch nur er die Protokolle lesen kann (Rechtekonzept!).
- Falls die Löschung einen "unverhältnismäßig hohen Aufwand" erfordern würde (z.B. bei Backups): Sorgen Sie für eine Sperrung der Daten durch die Einschränkung der Rechte bis auf einen einzelnen Benutzer (z.B. "nur DSB").

Rechte der Betroffenen

Stellen Sie sicher, dass der Datenschutzbeauftragte Protokollierungen in windream-Ordnern mit EXTREM geschützten Zugriffsrechten vornehmen kann. Dies kann bedeuten, dass nur der DSB auf die Dokumente in diesen Ordnern zugreifen kann und dort auch alle Rechte hat, die er zur Verwaltung der Dokumente benötigt. Als Dokumente wären beispielsweise zu nennen:

- Bekanntmachungen zu Datenschutzverletzungen
- Aussagen von Betroffenen
- Einlegen eines Widerspruchs
- Löschrufen
- (Sonstiges)

Unterstützung durch die windream GmbH

Jedes Unternehmen ist anders und arbeitet anders. Insofern werden auch die im Rahmen der EU-DSGVO getroffenen Maßnahmen nicht für alle Unternehmen gleich sein. windream ist in der Lage, diese verschiedenen Varianten problemlos abzubilden. Viele unserer Kunden implementieren ihre speziellen Anforderungen selber oder lassen sich kompetent beraten.

Die windream GmbH ist gerne dazu bereit, Sie bei der Umsetzung der EU-DSGVO mit windream zu unterstützen. Dies betrifft insbesondere auch die Implementierung der Dokumententypen, der Indizes und sonstiger Vorlagen, die für eine datenschutzkonforme Dokumentierung Ihrer Prozesse relevant sind. Bitte sprechen Sie uns an!