FAQ
EU DSGVO d.velop

Die Inhalte wurden mit großer Sorgfalt recherchiert. Dennoch kann d.velop keine Haftung für die Richtigkeit, Vollständigkeit und Aktualität der bereitgestellten Informationen übernehmen. Die Informationen sind insbesondere auch allgemeiner Art und stellen keine Rechtsberatung im Einzelfall dar. Zur Lösung von konkreten Rechtsfällen, insbesondere im Rahmen der DSGVO, konsultieren Sie bitte unbedingt einen Rechtsanwalt.

Stand: April 2018

Inhaltsverzeichnis

1.0 Allgemein

1.1 Welche Dokumente erwartet eine Aufsichtsbehörde?

Die Aufgabe der Aufsichtsbehörden im Datenschutz ist es, die Beachtung der Datenschutzgesetze durch Unternehmen und Behörden (öffentliche und nicht-öffentliche Stellen) zu überwachen.

Einen verbindlichen Katalog der Dokumente, die von der Aufsichtsbehörde verlangt werden können, gibt es nicht. Das Gesetz formuliert jedoch eine Verpflichtung aller datenverarbeitenden Stellen (sog. Verantwortliche im Datenschutz), Rechenschaft über die Beachtung der Gesetze zum Datenschutz ablegen zu können (Art. 5 Abs. 2 DSGVO). Dazu gehört eine Dokumentation über die Organisation des Datenschutzes im Unternehmen.

Üblicherweise besteht diese Dokumentation aus einer Datenschutz-Leitlinie (verabschiedet von der Unternehmensleitung), einem Datenschutzmanagementkonzept (mit der Beschreibung der Abläufe und Zuständigkeiten im Datenschutz, einschließlich Organigramm) und den sich aus dem Managementkonzept ergebenden konkreten Arbeitsabläufen (Prozessen) im Datenschutz. Ergänzt werden diese Dokumente dann durch ein Verzeichnis der Verarbeitungstätigkeiten (Art. 30 DSGVO), eine Dokumentation der technischen und organisatorischen Schutzmaßnahmen (Art. 32 DSGVO), einer Dokumentation über durchgeführte Datenschutz-Folgeabschätzungen (Art. 35 DSGVO) und eine Dokumentation der Anfragen von Betroffenen (z.B. Auskunft) sowie ein Löschkonzept. Im Einzelfall können weitere Dokumente dazu kommen.

Beispiele lassen sich aus den Praxishilfen zur DSGVO der GDD entnehmen (https://www.gdd.de/gdd-arbeitshilfen/praxishilfen-ds-gvo/praxishilfen-ds-gvo)

1.1.1 Was muss den betroffenen Personen mitgeteilt/ausgegeben werden: die Datensätze oder auch alle betreffenden Dokumente?

Das hängt von den Daten ab. Sofern die Daten Informationen von weiteren Personen oder Firmengeheimnisse enthalten, reicht ggf. der Hinweis auf deren Existenz. Ansonsten alle Informationen die gespeichert sind. Es ist allerdings nicht erforderlich reine Datenbankinhalte in Dokumente (z.B. PDF) umzuwandeln. Es reicht aus, wenn diese maschinenlesbar ausgeliefert werden z.B. JSON oder XML.

2.0 DSGVO und d.velop Software

2.1 Wie geht die d.velop AG intern mit der DSGVO um (Aufbewahrung im d.3ecm System auch DSGVO-konform)?

Die Beachtung des Datenschutzes und der Informationssicherheit hat in der gesamten d.velop AG übergeordnete Bedeutung. Selbstverständlich hat die d.velop AG daher entsprechende Maßnahmen im Rahmen Ihres internen DSGVO-Umsetzungsprojektes eingeleitet, um den Anforderungen der DSGVO am 25.05.2018 in angemessener Art und Weise zu genügen. Neben der internen Umsetzung der DSGVO erarbeitet die d.velop AG für Ihre Kunden Handreichungen und Konzepte, um aufzuzeigen, dass auch ab dem 25.05.2018 eine DSGVO-konforme Nutzung der d.velop-Software möglich ist. Die d.velop-Software ist je nach individueller Konfiguration grundsätzlich auch jetzt schon in der Lage, den Anforderungen des Datenschutzes durch Technikgestaltung zu genügen (Abbildung von Rollen- und Berechtigungskonzepten, Kennzeichnung von personenbezogenen Daten, Aufbewahrungen und Löschen - Umsetzung von Löschkonzepten)

Wie geht die d.velop AG intern mit der DSGVO um (Aufbewahrung im d.3ecm System auch DSGVO-konform)

2.2 Haben Sie ein Zertifikat, ein Rechtsgutachten oder eine eigene Präsentation zur DSGVO-Compliance der Software?

Hinsichtlich der Zertifizierungen der d.velop-Software zum Dokumentenmanagement ("DMS" oder "ECM") ist anzuführen, dass die Software selbst zunächst die revisionssichere Ablage von Dokumenten, E-Mails und anderen Inhalten ermöglicht, um den steuerrechtlichen sowie handelsrechtlichen Vorgaben zu genügen. Die d.velop Software ist diesbezüglich entsprechend nach den Standards PS880 und ISAE3000 zertifiziert. Auf Basis dieser handels- bzw. steuerrechtlich relevanten Zertifizierungen ist entsprechend der individuellen Konfiguration der d.velop-Lösung vom Kunden bzw. mit Unterstützung der d.velop eine Verfahrensdokumentation zu erstellen, die sodann von einem Wirtschaftsprüfer zu bestätigen ist. Auf dieser Grundlage erkennen die Finanzämter die Revisionssicherheit gemäß der Vorgaben der GOBD an (Grundsätze zur ordnungsmäßigen Führung und Aufbewahrung von Büchern, Aufzeichnungen und Unterlagen in elektronischer Form sowie zum Datenzugriff.)

Als Hilfsmittel zum Nachweis der DSGVO-Konformität sieht die DSGVO u.a. in Art. 42 DSGVO für Verantwortliche (=Kunde einer d.velop Software) sowie Auftrags Verarbeiter (= ggf. d.velop sofern eine Auftragsverarbeitung gem. Art. 28 DSGVO etwa im Rahmen der Nutzung der d.velop cloud vorliegen sollte), die Möglichkeit zur DSGVO-Zertifizierung oder die Erlangung eines Datenschutzsiegels vor. Zum jetzigen Zeitpunkt sind solche Zertifizierungen von den zuständigen Akkreditierungsstellen jedoch noch nicht aufgesetzt worden. Die d.velop AG wird die Möglichkeit zur Zertifizierung ihrer Softwareprodukte prüfen, sobald entsprechende Zertifizierungen erlangt werden können.

Gleiches gilt für den Anschluss an sog. "Verhaltensregeln" oder "Code of Conducts" nach Art. 40 DSGVO. Zurzeit ist vor dem Hintergrund der Einschränkungen in Art. 42 DSGVO auf den Verantwortlichen bzw. auf die Reichweite der Auftragsverarbeitung aufgrund fehlender aufsichtsbehördlicher Positionierungen noch nicht erkennbar, in wie weit sich reine softwarebezogene Zertifizierungen nach DSGVO etablieren werden bzw. ob die Aufsichtsbehörden bspw. als Nachweis der Konformität zu Datenschutz durch Technikgestaltung solche Zertifizierungen ermöglichen werden.

2.3 Muss die d.velop AG (als Hersteller) eine Datenschutz-Folgeabschätzung (DSFA) für Ihre Programme bereitstellen und die dann bei den Endkunden hausspezifisch anpassen?

Zuerst einmal eine kurze Erläuterung, was eine Datenschutz-Folgeabschätzung (DSFA) ist. Eine Datenschutz-Folgenabschätzung (DSFA) ist gemäß Art. 35 DS-GVO ein Verfahren,

- *anhand dessen die Verarbeitung beschrieben wird,*
- *welches die Notwendigkeit und Verhältnismäßigkeit der Verarbeitung bewertet*
- *welches die Risiken für die Rechte und Freiheiten der betroffenen Personen kontrolliert, durch*
- *Risikoabschätzung und*
- *Ermittlung von Gegenmaßnahmen*

Abschätzung der Folgen der Verarbeitungsvorgänge für den Schutz personenbezogener Daten, besteht (mindestens) aus:

- *Systematische Beschreibung der Verarbeitung und der Zwecke*
- *Bewertung von Notwendigkeit und Verhältnismäßigkeit in Bezug auf den Zweck*
- *Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen*
- *Zur Bewältigung der Risiken geplante Abhilfemaßnahmen, durch die der Datenschutz sichergestellt und der Nachweis zur Einhaltung der GVO (auch des Art. 32) erbracht wird*

Pflicht zur Durchführung bei hohen Risiken für Rechte und Freiheiten natürlicher Personen:

- *auf Grund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung*
- *Insbesondere bei der Verwendung neuer Technologien*
- *Standpunkte der Betroffenen oder deren Vertreter ggf. einzuholen*

- *Erforderlichenfalls Überprüfung der Verarbeitung, ob sie gemäß der Folgenabschätzung durchgeführt wird*

Die Durchführung der DSFA obliegt grundsätzlich dem Verantwortlichen. Adressat der Pflicht zur Durchführung einer DSFA ist der Verantwortliche; dies folgt schon aus dem Wortlaut von Art. 35 Abs. 1 S. 1 DSGVO: „Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge, so führt der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch." Für den Auftragsverarbeiter besteht hinsichtlich der von ihm tatsächlich durchgeführten Verarbeitungen (Support & Pflege) im Rahmen seiner Tätigkeit als Auftragsverarbeiter keine Pflicht zur Durchführung der DSFA.

Um aber eine den Vorgaben von Art. 35 DSGVO entsprechende DSFA bezogen auf bestimmte Softwareprodukte durchführen zu können, wird der Verantwortliche aber regelmäßig auf Informationen vom Auftragsverarbeiter auch hinsichtlich seines Softwareproduktes welches er geliefert hat, angewiesen sein. Ausgehend von den Erwägungsgründen 83 und 95 zur DSGVO ist der Auftragsverarbeiter deshalb angehalten, erforderlichenfalls den Verantwortlichen auf Anfrage bei der Durchführung der DSFA zu unterstützen. Dieser Unterstützungsleistung kommt die d.velop AG, nach entsprechender Beauftragung, gerne durch Beratungsleistung nach. Hinsichtlich des reinen Softwareproduktes handelt es sich um eine freiwillige Dienstleistung.

Die d.velop AG wird in Kürze abstrakte Informationen bereitstellen, wie und auf welcher Grundlage bezogen auf d.3ecm eine DSFA durchgeführt werden kann und welche grundsätzlichen Möglichkeiten bestehen, Maßnahmen mit d.3ecm zu ergreifen um eine Risikominimierung zu erlangen.

Ob eine DSFA für eine bestimmte d.3-Konfigutation als Teil eines Verfahrens in einem Verarbeitungsprozess durchzuführen ist, muss der Verantwortliche für sich selbst entscheiden. Hierbei kann die d.velop AG allenfalls hinsichtlich von Konfigurationsmaßnahmen unterstützen.

2.4 Auf welche Weise werden die Anforderungen der DSGVO in d.3ecm erfüllt?

d.3ecm stellt eine Vielzahl von Möglichkeiten bereit, das System durch den Anwender datenschutzkonform zu konfigurieren. Das betrifft z.B. das Rollen- und Berechtigungskonzept, das Löschen von Dokumenten und Metadaten nach einer vom Kunden festgelegten Aufbewahrungszeit und die Möglichkeit zur Verschlüsselung der Kommunikation zwischen verschiedenen d.3ecm Komponenten, beim Zugriff auf d.3ecm oder bei der Ablage von Dokumenten in d.3ecm.
Ob und wie die Anforderungen der DSGVO in d.3ecm abgebildet werden, hängt dabei aber maßgeblich von den mit d.3ecm durchgeführten Verarbeitungen sowie der Konfiguration von d.3ecm durch den Anwender ab. Die DSGVO adressiert nicht den Software-Hersteller (also die d.velop), sondern denjenigen, der mit einer Software personenbezogene Daten verarbeitet (den Anwender, in der Sprache des

Datenschutzes den Verantwortlichen). Die d.velop kann den Anwender bei datenschutzkonformen Konfiguration von d.3ecm unterstützen. Die Anforderungen müssen aber jeweils vom Anwender selbst erfüllt werden.

2.5 Gibt die d.velop AG Empfehlungen hinsichtlich der Auswahl des Storage Systems?

Wir geben keine Empfehlung zur Auswahl des Storage Systems. Die Notwendigkeit Dokumente eines Betroffenen innerhalb von 4 Wochen löschen zu können besteht nur, wenn der Kunde für die Speicherung der Daten keine Rechtsgrundlage hat. D.h. sofern der Kunde nur Dokumente verwaltet und auf Sekundärspeicher ablegt, zu deren Aufbewahrung verpflichtet ist, muss er diese nicht vor Ablauf der gesetzlichen Aufbewahrungsfristen löschen. Legt der Kunde hingegen Dokument ab zu deren Aufbewahrung er nicht verpflichtet ist, muss er dieses Löschen können. In diesem Fall müsste er sich entweder für ein System entscheiden mit dem dies möglich ist oder er speichert diese Dokumente nur im d.3ecm Dokumentenbaum und nicht auf dem Sekundärspeicher.

3.0 Umsetzung der DSGVO in d.velop-Software

3.1 Wie erfolgt die Ablage personenbezogener Daten in d.3ecm? Müssen gewisse Daten in Indexfelder eingetragen werden?

Die Ablage erfolgt weiterhin so, wie der Kunde es für seine Prozesse benötigt. Es gibt keine Daten die verpflichtend in Indexfelder gespeichert werden müssen. Im Gegenteil kann es sinnvoll sein, schützenswerte Daten weder in Indexfeldern noch im Volltext zu speichern und diese nur im verschlüsselten Dokument aufzubewahren. Dies ist allerdings die Entscheidung des Kunden, die er nach Ermittlung des Schutzbedürfnisses der Daten treffen muss.

3.2 Erfolgt die Suche nach personenbezogen Daten über Indexfelder, über Volltext oder wird es ggf. andere intelligente Möglichkeiten geben

Die Suche erfolgt wie bisher auch entweder über Indexfelder oder über den Volltext. Dies ist davon abhängig, wie der Kunde die Daten ablegen möchte. Um dem Kunden die Suche in unterschiedlichen Dokumentarten zu erleichtern arbeiten wir an einem Konzept komplexere Suchtemplates erzeugen zu können, die gleichzeitig in unterschiedlichen Dokumentarten auf unterschiedliche Weise suchen.

3.3 Beim Ablegen von Dokumenten im d.3ecm wird der Bearbeiter als nachträglich nicht mehr änderbare Standard-Eigenschaft im d.3ecm hinterlegt. Ist dieser Datenwert im Rahmen der DSGVO bei der Beauskunftung oder Löschung zu berücksichtigen?

Zu beauskunften sind grundsätzlich alle personenbezogenen Daten, also auch die Angabe als Bearbeiter in d.3ecm und andere Metadaten mit Personenbezug. Eine Ausnahme besteht nur dann, wenn die Daten gespeichert werden entweder (a) für die Erfüllung gesetzlicher, vertraglicher oder satzungsgemäßer Aufbewahrungspflichten, oder (b) für Zwecke der Datensicherheit und der Datenschutzkontrolle. Wenn eine der beiden Ausnahmen vorliegt muss nur die Auskunft erteilt werden, dass weitere Daten gespeichert werden, diese aber aus dem vorgenannten Grund nicht in der Auskunft enthalten sind. Ob eine der Ausnahmen vorliegt ist eine Einzelfallbetrachtung; meist wird das aber der Fall sein.

Anders ist dies beim Löschen: Besteht kein Zweck mehr für die weitere Speicherung von personenbezogenen Daten (das gilt auch für Metadaten wie hier den Eintrag des Bearbeiters als Standard-Eigenschaft im d.3ecm), sind nach Ablauf aller Aufbewahrungsfristen auch sämtliche Meta-Daten zu löschen. Eine Ausnahme wie früher, dass die Löschung dann nicht erforderlich ist, wenn aus technischen Gründen die Löschung unmöglich oder nur mit unverhältnismäßigem Aufwand möglich ist, kennt die

DSGVO nicht mehr. Damit sind die Löschkonzepte so zu erstellen, dass auch die Metadaten erfasst werden.

3.4 Welche Anforderungen beim Speichern von Daten / E-Mails sind im Zusammenhang mit dem Beschäftigtendatenschutz zu berücksichtigen

Soweit die Nutzung der d.velop Software im Zusammenhang mit der Verarbeitung von personenbezogenen Daten ("pbD") von Ihren Beschäftigen oder Kunden steht, so sollte diese Verarbeitung stets in der d.velop Software erfasst werden; die entsprechenden Möglichkeiten stehen zur Verfügung. Nur die strukturierte Speicherung von pbD ermöglicht die ordnungsgemäße Erfüllung der sog. Betroffenenrechte gem. Art. 12f. DSGVO. Nur so sind Sie in der Lage, die Anfragen der Betroffenen (Beschäftigte, Kunde, Verbraucher etc.) mit Blick auf Auskunft, Löschung, Widerspruch zur Verarbeitung ihrer pbD effektiv zu gewährleisten. Dies setzen Sie bei der Einführung ihrer d.velop Software als Verarbeitungstätigkeit am besten dadurch um, dass die d.velop Software und ihre konkrete Implementierung vollständig hinsichtlich der Anforderungen aus Art. 30 DSGVO (Verzeichnis der Verarbeitungstätigkeiten und Berücksichtigung der Anforderungen zur Sicherheit der Verarbeitung gem. Art. 32 DSGVO) beschrieben wird. Die d.velop AG wird in Kürze das Produkt "d.velop GDPR compliance center" veröffentlichen, mit dessen Hilfe Sie das Verzeichnis der Verarbeitungstätigkeiten für alle ihre Verarbeitungen auch außerhalb von d.velop Software erstellen können.

Auf Grundlage des Verzeichnisses der Verarbeitungstätigkeit ist sodann ein Aufbewahrungs- und Löschkonzept zu entwickeln. In diesem Konzept ist nach den verschiedenen Datensätzen zu strukturieren und festzulegen, welchen konkreten Aufbewahrungsfristen ein Dokument oder eine E-Mail unterfällt. So gilt bspw. für bestimmte Handelsbriefe gem. § 147 Abs. 1, 3 AO eine Aufbewahrungsfrist von 6 Jahren (Handels- oder Geschäftsbriefe) für andere Unterlagen eine 10-jährige Aufbewahrungsfrist (Bücher und Aufzeichnungen, Inventare, Jahresabschlüsse, Lageberichte, die Eröffnungsbilanz sowie die zu ihrem Verständnis erforderlichen Arbeitsanweisungen und sonstigen Organisationsunterlagen). Bei der Erstellung des Löschkonzeptes kann man sich bspw. an der DIN 66398 oder anderen marktüblichen Standards orientieren.

Zur Erreichung der handels- und steuerrechtlich relevanten Revisionssicherheit werden Dokumente, E-Mails und sonstige Inhalte auf Grundlage der entsprechend dem auch bei der d.velop AG zertifizierten Standard PS880 bzw. ISAE3000 revisionssicher in den Storage Systemen gespeichert. Im Übrigen haben Sie auch diesbezüglich vermutlich schon eine sog. "Verfahrensdokumentation" erstellen lassen, denn nur mit dieser - von einem Wirtschaftsprüfer zu bestätigenden - Dokumentation, werden die Finanzbehörden die Revisionssicherheit anerkennen. Auch diese Dokumentation wird Ihnen bei der Erstellung des Löschkonzeptes behilflich sein.

Macht nun ein Betroffener bspw. von seinem Recht auf Löschen aus Art. 17 DSGVO u.a. dann Gebrauch, wenn er aus Ihrem Unternehmen ausgeschieden ist, haben Sie zu prüfen, ob Sie zum Löschen tatsächlich verpflichtet sind. Das ist insbesondere immer dann der Fall, wenn Sie zur Aufbewahrung eines Dokumentes, E-Mail oder sonstigen Inhaltes

aufgrund dessen nicht mehr berechtigt sind, dass eine Aufbewahrungsfrist abgelaufen ist. Dann war die Aufbewahrung - ggf. auch ohne Anfrage eines Betroffenen - wohl schon ab Ablauf der Aufbewahrungsfrist datenschutzrechtlich betrachtet, rechtswidrig. Wenn keine Aufbewahrungsfrist mehr besteht und sie auch nicht aufgrund satzungsgemäßer oder vertraglicher Pflichten heraus gem. § 35 Abs. 3 BDSG (Neu) (Anmerkung: Das BDSG (Neu) konkretisiert unter anderem die Betroffenenrechte der DSGVO), haben Sie auch revisionssicher gespeicherte Inhalte zu löschen. Soweit die Aufbewahrungsfrist jedoch nicht abgelaufen ist, sind Sie zur weiteren Speicherung bis zum Ablauf der Frist berechtigt; dies ist dem Betroffenen sodann auch mitzuteilen. Zur Vermeidung des Eintritts eines rechtswidrigen Zustandes im Zusammenhang mit der Nichterfüllung von Betroffenenrechten sollten Sie unabhängig von dem Anlass ("Betroffener verlangt Löschung") bereits ereignisbezogen ("Aufbewahrungsfrist ist abgelaufen") ein automatisiertes Löschen vorsehen. Die d.velop Software ermöglichst die Umsetzung von Löschkonzepten.

3.5 Wie sieht das Verfahren im d.3ecm bezüglich Löschung von Daten aus (Art. 17), insbesondere im Hinblick auf die unterschiedlichen Storage Systeme im d.3ecm?

Um die Möglichkeit Informationen oder personenbezogene Daten im Sinne der DSGVO im d.3 Server zu löschen, müssen folgende Funktionen im d.3ecm aktiviert werden:

ALLOW_DELETE_FROM_RELEASE muss aktiviert sein, damit ein berechtigter Anwender alle Dokumente löschen kann.

DELETE_DOCS_ELAPSED_SEC_STORAGE muss aktiv sein, damit das Löschen zum Storagemanager übertragen wird.

RECYCLE_STORAGE_PERIOD muss auf einen kleineren Wert gesetzt werden, wenn die logische Löschung frühzeitig physikalisch erfolgt. Im Standard wird erst nach 365 Tagen physikalisch gelöscht

Für das Löschen im Hinblick auf die Storage Systeme ist nicht die d.velop AG verantwortlich, sondern der jeweilige Anwender von d.3. Hier muss im Einzelfall geprüft werden, ob und wie ein Löschen in den Storage Systemen möglich ist. Ggf. sind Anpassungen der Backup-/Archivierungsstrategien vorzunehmen, wenn diese unterschiedliche Löschfristen und das Löschen von Einzeldaten nicht erlauben ist.

3.6 Wie kann die Verarbeitung gem. Art. 18 im d.3ecm eingeschränkt werden?

Eine Einschränkung der Verarbeitung ist in den in Art. 18 Abs. 1 DSGVO bezeichneten Fällen vorzunehmen. Die Einschränkung der Verarbeitung bewirkt gemäß Art. 18 Abs. 2 DSGVO, dass die von der Einschränkung betroffenen "personenbezogenen Daten – von ihrer Speicherung abgesehen – nur mit Einwilligung der betroffenen Person oder zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses der Union oder eines Mitgliedstaats verarbeitet werden" dürfen.

Für eine Einschränkung ist deshalb erforderlich, dass die davon betroffenen Daten so markiert sind, dass für den Bearbeiter erkennbar wird, dass es sich um eingeschränkte Daten handelt (z.B. durch eine farbige Kennzeichnung) oder die Daten technisch "gesperrt" sind, sodass eine weitere Verarbeitung bis zur Aufhebung der Einschränkung nicht oder nur mit Sonderrechten möglich ist.

Im d.3ecm gibt es dazu das gesperrt Flag, was durch ein Verbotsschild sichtbar gemacht wird. Ferner kann der Zugriff darauf für die Anwender komplett oder teilweise eingeschränkt werden. Beispielweise könnte es so konfiguriert werden, dass der Anwender zwar einen Treffer erhält, dass Dokument aber nicht anzeigen kann.

Im ecspand / SharePoint Umfeld würde man diese Daten in eine SiteCollection verschieben, in der keine Verarbeitung stattfindet und die mit einem entsprechenden Berechtigungskonzept (Policies) einschränkend abgesichert ist.

3.7 Wie können wir die gem. Art. 19 geltenden Verpflichtungen über die offengelegten personenbezogenen Daten im d.3ecm realisieren?

Art. 19 DSGVO zwingt den Verantwortlichen, bei der Löschung, Berichtigung oder Einschränkung der Verarbeitung etwaige Empfänger der Daten darüber zu informieren, dass diese beim Verantwortlichen gelöscht, berichtigt oder eingeschränkt verarbeitet wurden/werden. Damit das d.3ecm hierbei unterstützen kann, müsste überhaupt in d.3ecm protokolliert werden, wem gegenüber als Empfänger (Art. 4 Nr. 9 DSGVO) die Daten offengelegt wurden.

Eine Möglichkeit wäre ein eigenes d.3ecm System so zu konfigurieren (inkl. Workflows) um Betroffenenanfragen zu verarbeiten. D.h. sämtliche Anfragen bezüglich Löschung, Berichtigung oder Einschränkung würden über dieses System gesteuert und dokumentiert. Auch die Aktivitäten die nicht in einem d.3ecm System durchgeführt wurden. Ferner würde dieses d.3ecm System so konfiguriert, dass die Dokumente automatisch nach 12 Monaten gelöscht würden bzw. zu 31.12 des Folgejahres.