ISMS – Informationssicherheitsmanagement

Richtlinie Dokumentenlenkung

Vertraulichkeit: EuroDaT-intern

EuroDaT GmbH
Gerichtsstraße 2
65185 Wiesbaden
Germany

info@eurodat.org
www.eurodat.org

Dokumenteninformation	
Version:	1.0
Verantwortlich:	Alexander Alldridge
Freigabe:	Freigabe erfolgt am 10.12.2024 durch Alexander Alldridge
Nächste Überprüfung:	10.12.2025

Änderungshistorie:

Version	Datum	Bearbeiter	Änderungshinweise
0.1	29.10.2024	Lukas Klose	Erstellung initiale Draft-Version
0.2	05.11.2024	Alexander Alldridge	Korrektur gelesen
0.3	13.11.2024	Lukas Klose	-Einarbeitung Korrekturen -Ergänzung 2.3 – Schutzbedarfsklassen -generisches Femininum
1.0	10.12.2024	Alexander Alldridge	Freigabe erteilt

Inhaltsverzeichnis

1 Einleitung

Die Dokumentenlenkung spielt eine wichtige Rolle im Rahmen des Qualitätsmanagements der Firma. Für alle dokumentierten Informationen von EuroDaT, mit Richtung weisendem oder grundlegendem Charakter für die Organisation der Firma und die Mitarbeiterinnen, ist es von zentraler Bedeutung, dass die Leserin bzw. Empfängerin der Dokumentation die Aktualität des Dokuments nachvollziehen kann.

1.1 Anwendungskreis

Die in diesem Dokument gemachten Vorgaben gelten für die dokumentierten Informationen von EuroDaT, die Bestandteil der schriftlich fixierten Ordnung (SFO) sind. Dies sind insbesondere dokumentierte Informationen im Rahmen von Management-Systemen, internen Richtlinien oder weiteren geltenden Vorschriften. Dies gilt insbesondere für die Dokumentation nach ISO 27001:2022.

Für sonstige Dokumente dienen die Vorgaben in dieser Richtlinie als Empfehlung.

2 Umsetzung der Dokumentenlenkung

Die Dokumentenlenkung bei EuroDaT geschieht in Anlehnung an ISO27001:2022 Normkapitel 7.5. Für die Erstellung und die Aktualisierung von dokumentierten Informationen sind bei EuroDaT folgende Vorgaben zu beachten[1]:

- angemessene Kennzeichnung,
- angemessenes Format,
- angemessenes Medium, sowie
- angemessene Überprüfung und Genehmigung.

Für das ISMS soll die Lenkung zusätzlich Eignung, Verfügbarkeit und einen angemessenen Schutz der Informationen sicherstellen. Dazu werden folgende Aspekte berücksichtigt:

- Verteilung, Zugriff, Auffindung und Verwendung,
- Ablage und Sicherung,
- Überwachung von Änderungen,
- Aufbewahrung und weiterer Verbleib.

2.1 Schritte bei der Erstellung oder Aktualisierung von Dokumenten

Bei der Erstellung einer dokumentierten Information wird in der Regel ein Zyklus von 6 Schritten durchlaufen:

Abbildung 1: Regelzyklus der Erstellung einer dokumentierten Information

Im Folgenden werden die einzelnen Schritte vorgestellt.

- **Bearbeitung:** Die Erstellung oder Aktualisierung eines Dokuments wird durch eine mit der Materie vertraute Autorin durchgeführt. Die Autorin ist gleichzeitig Ansprechpartnerin für Rückfragen in den nachfolgenden Prozessschritten.

[1] Vgl. ISO27001:2022 Normkapitel 7.5.2

- **Prüfung:** Das von der Autorin erstellte Dokument oder die durchgeführten Ergänzungen werden von einer Prüferin einem Lektorat unterzogen. Dabei sind nur Änderungen zu prüfen, die eine fachliche bzw. inhaltliche Auswirkung haben. Ausschließlich redaktionelle Änderungen, die keine oder nur unwesentliche Änderungen der im Dokument getroffenen Regelungen nach sich ziehen, müssen keiner Prüfung und Freigabe unterzogen werden[2]. Die Prüfung kann nicht von der Autorin selbst, sondern nur von einer weiteren fachlich betrauten Mitarbeiterin durchgeführt werden. Dabei werden formale Aspekte und Inhalt des geschriebenen Textes überprüft. Anmerkungen und Änderungswünsche werden an die Autorin zur Korrektur übergeben. Bei signifikanten inhaltlichen Nachbesserungen ist im Anschluss eine erneute Prüfung notwendig.
- **Freigabe:** Bevor eine neue Version eines Dokuments Gültigkeit erlangt, ist grundsätzlich eine Freigabe oder Abnahme des Dokuments durch eine fachlich verantwortliche Mitarbeiterin erforderlich. Dies ist in der Regel die Eigentümerin des Dokuments, die Abnahme kann jedoch delegiert werden. Die Freigabe darf nicht durch die Autorin erfolgen, Prüferin und Abnehmerin können jedoch identisch sein. Dabei ist zu beachten, dass die freigebende Mitarbeiterin auch die Legitimation und das fachliche Wissen zur Durchführung der Abnahme besitzt[3]. Wie in Punkt „Prüfung“ angesprochen, bedürfen rein redaktionelle oder unwesentliche Änderungen keiner Freigabe.
- **Verteilung:** Nach der Abnahme müssen die Dokumente an den Verteilerkreis übergeben werden. Für interne Richtlinien und Dokumente der Management-Systeme kann ein dafür vorgesehener Ablageort genutzt werden.
- **Schulung:** Sofern notwendig, werden Schulungen durchgeführt oder gemäß den Änderungen angepasst. Dies ist insbesondere der Fall, wenn es sich um Dokumente im Rahmen des Management-Systems oder um Compliance-Richtlinien handelt.
- **Verwendung**: Nach Abnahme und Verteilung eines Dokuments sind die darin beschriebenen Vorschriften und Maßnahmen gültig und von den betreffenden Mitarbeiterinnen anzuwenden.

2.2 Anforderungen an Dokumente

Zur Sicherstellung der Qualität und Richtigkeit dokumentierter Informationen bei EuroDaT werden die folgenden Anforderungen an die Dokumente gestellt.

2.2.1 Angemessene Kennzeichnung

Für jede Mitarbeiterin, die die dokumentierte Information liest, muss erkenntlich sein, dass der Inhalt geprüft und gültig ist. Dazu sind mindestens folgende Informationen in den Dokumenten zu hinterlegen:

---

[2] Dieses Vorgehen soll die Möglichkeit von geringfügigen Anpassungen, z.B. Grammatikfehler, geänderte Organisationsnamen etc., ohne Freigabeprozess unterstützen. Die Beurteilung, ob Änderungen als redaktionell oder unwesentlich einzustufen sind, liegt hier (zunächst) im Ermessen des:der Autors:in.

[3] Wenn der:die fachliche Eigentümer:in eines Dokuments aus mehreren Personen besteht, z.B. aus einem Board, so ist die Freigabe in der Regel auch durch diesen Personenkreis notwendig.

- **Name der Organisation:** Das Firmenlogo bzw. der Firmenname sollte auf dem Dokument angegeben sein, damit ersichtlich ist, dass es sich bei diesem um ein firmeninternes Dokument handelt.
- **Titel:** Der Titel des Dokuments muss angegeben werden. Bei Office-Produkten ist der Titel auch in der Dokumenten-Information der Datei zu berücksichtigen.
- **Autorin:** Es muss ersichtlich sein, wer das Dokument geschrieben oder die Änderungen durchgeführt hat. Die Autorin ist auch erste Ansprechpartnerin für Rückfragen zu der Dokument-Version.
- **Verantwortlich:** Die Angabe der Dokument-Verantwortlichen (oder Owner) ist notwendig, um Fragen bezüglich des Inhalts und der Gültigkeit klären zu können.
- **Abnahme:** Es muss ersichtlich sein, wann und von wem das Dokument abgenommen wurde.
- **Revisionsstand/Version:** Der aktuelle Stand des Dokuments muss ersichtlich sein. Die Information sollte im Fall von Text-Dokumenten im Dokument sichtbar sein. Das reviewte Dokument mit dem höchsten Revisionsstand ist immer das aktuell gültige Dokument.
- **Schutzbedarfsklasse:** Der Schutzbedarf des Dokuments wird anhand der in Kapitel 2.3.1 definierten Schutzbedarfsklassen festgelegt und im Dokument festgehalten.
- **Änderungshistorie:** Es muss eine Änderungshistorie dargestellt sein, aus der die durchgeführten Änderungen und Freigaben entnehmbar sind. Es muss auch ersichtlich sein, wann die Änderung durchgeführt wurde. Dadurch wird gewährleistet, dass die Leserin sich auf die geänderten Inhalte konzentrieren kann.
- **Gültigkeit:** (falls sinnvoll): Der nächste geplante Reviewtermin ist im Dokument zu vermerken (sofern notwendig). Bei Dokumenten des ISMS bzw. QMS beträgt das Review- Intervall i.d.R. 12 Monate. Dokumente können aber auch „bis auf Weiteres“ (d.h. unbefristet) gültig sein.

Die tatsächliche Ausgestaltung der Dokumenteninformation ist jeder Autorin freigestellt; ein Beispiel für Word findet sich im Anhang. Dokumente einer Dokumentenfamilie (z.B. Dokumente des ISMS) sollten Dokumenteninformationen im identischen Format besitzen.

Es ist auch darauf zu achten, für in Microsoft Office geschriebene Dokumente die Dokumenteninformationen der Datei aktuell zu halten (Titel, Autorin, etc.).

2.2.2 Angemessenes Format

Für den jeweiligen Zweck des Dokuments muss ein angemessenes Format gewählt werden. Dabei sind folgende Punkte zu berücksichtigen:

- **Sprache:** Dokumente sind in einer dem jeweiligen Adressatenkreis angemessenen Sprache zu verfassen. Falls notwendig sind dabei Anforderungen externer Leserinnen zu berücksichtigen.
- **Grafiken:** Bei der Einbindung von Bildern und Grafiken ist auf eine angemessene Nummerierung zu achten. Etwaige Eigentumsrechte sind zu berücksichtigen und die Herkunft zu kennzeichnen.

2.2.3 Angemessenes Medium

Bei den unter die Dokumentenlenkung fallenden Dokumenten handelt es sich um

Textdokumente. Mithin liegen sie als Google Workspace-Dokumente und teils als PowerPoint oder Excel vor. Google Workspace-Dokumente sollten in der Regel als PDF-Versionen veröffentlicht werden.

2.2.4 Angemessene Überprüfung und Genehmigung

Auf den Prüfungs- und Freigabeprozess sowie die regelmäßige Überprüfung wird in Abschnitt 2.1 eingegangen. Für Dokumente des ISMS und des QMS initiiert der ISB die anstehenden Überprüfungen.

2.3 Klassifizierung von Dokumenten

Jedes Dokument bei EuroDaT muss hinsichtlich der Vertraulichkeit und des Risikos, das für EuroDaT aufgrund einer unautorisierten Kenntnisnahme oder Manipulation der Information entsteht, eingeschätzt werden. Dafür werden bei EuroDaT sogenannte Schutzbedarfsklassen definiert.

Anhand der Vorgaben für die Schutzbedarfsklassen kann eine entsprechende Einordnung des Schutzbedarfs von Informationen vorgenommen werden, um Informationswerte entsprechend vor unautorisiertem Zugriff zu schützen.

2.3.1 Die Schutzbedarfsklassen bei EuroDaT

Folgende Schutzbedarfsklassen zur Klassifizierung von Dokumenten finden bei EuroDaT Anwendung:

- **Öffentlich:** Dokumente der Schutzbedarfsklasse „öffentlich“ unterliegen keinem eigentlichen Schutzbedarf und können von allen Personen außerhalb der Firma gelesen werden. Informationen dieser Schutzbedarfsklasse müssen nicht gesondert gekennzeichnet werden.
- **EuroDaT-intern:** Informationen dieser Schutzklasse dürfen unabhängig von ihrer Speicher- (elektronische Form oder Papierform) oder Kommunikationsform (schriftlich, mündlich) von jeder Mitarbeiterin von EuroDaT eingesehen werden. Prinzipiell sind diese Informationen jedoch nicht für Außenstehende bestimmt, so dass eine Weitergabe dieser Informationen an Außenstehende nur nach Erlaubnis durch die Geschäftsführung erfolgen darf. Falls notwendig, können EuroDaT-interne Dokumente mit dem Hinweis versehen werden, dass diese Dokumente für einen bestimmten Personenkreis außerhalb EuroDaTs freigegeben werden können. Jede Mitarbeiterin hat darauf zu achten, dass keine unbefugten Personen Zugriff auf diese Dokumente oder Informationen haben.
- **Vertraulich:** Informationen dieser Schutzklasse dürfen nur einem eingeschränkten Kreis von Mitarbeiterinnen zugänglich sein und müssen somit vor dem Zugriff durch nicht autorisierte EuroDaT-Mitarbeiterinnen geschützt werden. Der Kreis der leseberechtigten Personen wird von der Erstellerin der Information definiert und kann im Zweifel bei ihr erfragt werden. Prinzipiell sind alle personenbezogenen Daten immer als vertraulich zu markieren. Speichermedien, die solche Dokumente beinhalten, müssen verschlüsselt werden und anderen Mitarbeiterinnen unzugänglich sein. Eine Versendung per Mail muss immer verschlüsselt erfolgen. Bei der Ablage auf Netzlaufwerken ist auf die Berechtigung der Personen zu achten, die diese

Information lesen und bearbeiten dürfen.

Sind in einem Dokument Informationen unterschiedlicher Schutzbedarfsklassen enthalten, so ist zur Klassifikation das Maximalprinzip anzuwenden. Dies ist auch bei Änderungen an dem Dokument zu beachten, das heißt, dass das Dokument so abgespeichert werden muss (z.B. auf Laufwerken mit beschränktem Zugriff), dass der maximale Schutzbedarf eingehalten wird.

2.4 Änderungsmanagement

Bei einem geplanten Review soll neben bestehendem Aktualisierungsbedarf auch auf mögliches Verbesserungspotenzial geachtet werden.

2.4.1 Überwachung von Änderungen

Die Dokumente enthalten Informationen über den Revisionsstand sowie eine Liste der jeweiligen Änderungen gegenüber der Vorgängerversion (siehe Abschnitt 2.2.1).

2.4.2 Abhängigkeiten zwischen Dokumenten

Bei grundlegenden Änderungen an einer dokumentierten Information sollten die Owner von auf dieser Dokumentation aufbauenden Dokumenten informiert werden, damit eine zeitnahe Überprüfung eines möglichen Anpassungsbedarfs durchgeführt werden kann.

Im Rahmen des regelmäßigen Reviews müssen sich zwischenzeitlich veränderte Vorgaben in anderen Dokumenten, auf die sich das vorliegende Dokument bezieht, entsprechend berücksichtigt werden.

2.4.3 Aufbewahrung und weiterer Verbleib

Nicht mehr gültige und abgelöste Dokumente werden klar als solche gekennzeichnet, und so archiviert, dass sie nicht versehentlich genutzt werden. Dazu wird eine neue Version des Dokuments erstellt, welche einen deutlich sichtbaren Vermerk enthält.

Wird ein Dokument durch ein komplett neues Dokument ersetzt, ist es hilfreich, einen Verweis auf das neue Dokument mit anzugeben.

2.5 Vor Einführung der Dokumentenlenkung gültige Dokumente

Dokumente der schriftlich fixierten Ordnung, die vor der Einführung der Dokumentenlenkung erstellt wurden, erfüllen i.d.R. noch nicht die Vorgaben dieser Richtlinie. Diese Dokumente behalten unverändert ihre Gültigkeit. Sie sollten bei anstehenden Überarbeitungen schrittweise auf die hier beschriebenen Vorgaben angepasst werden.

3 Annex A Beispiel für Word

Dokumenteninformation	
Version:	1.0
Verantwortlich:	ISB
Freigabe	Erteilt am xxx durch YYY / nicht erforderlich
Nächste Überprüfung	19.04.2023 / nicht erforderlich

Änderungshistorie:

Version	Datum	Bearbeiter	Änderungshinweise
0.5	28.03.2022	Hans Mustermann	Erstellung initiale Draft-Version
1.0	19.04.2022	Hans Mustermann	Anpassung Feedback von Gerda Musterfrau, anschließende Freigabe und Versionsnummer auf 1.0 gesetzt.

4 Annex B Beispieltext für aufgehobene Dokumente

Richtlinie über …

--- Dieses Dokument wurde mit Wirkung vom 19.04.2023 aufgehoben und durch die Richtlinie über … ersetzt ---

Dokumenteninformation	
Version:	1.1 (aufgehoben)
Verantwortlich:	ISB
Freigabe	Erteilt am xxx durch YYY / nicht erforderlich
Nächste Überprüfung	nicht erforderlich

Änderungshistorie:

Version	Datum	Bearbeiter	Änderungshinweise
0.5	28.03.2022	Hans Mustermann	Erstellung initiale Draft-Version
1.0	19.04.2022	Hans Mustermann	Anpassung Feedback von Gerda Musterfrau, anschließende Freigabe und Versionsnummer auf 1.0 gesetzt.
1.1	19.04.2023	Hans Mustermann	Außerkrafttreten eingepflegt, anschließende Freigabe und Versionsnummer auf 1.1 gesetzt