Informationssicherheitsleitlinie EuroDaT GmbH

Vertraulichkeit: EuroDaT-intern[1]

EuroDaT GmbH
Gerichtsstraße 2
65185 Wiesbaden
Germany

info@eurodat.org
www.eurodat.org

[1] Weitergabe an Kunden auf Anfrage möglich.

Dokumenteninformation	
Version:	0.1
Verantwortlich:	ISB
Freigabe:	Freigabe erfolgt am XX.XX.2024 durch den ISB
Nächste Überprüfung:	XX.XX.2025

Änderungshistorie:

Version	Datum	Bearbeiter	Änderungshinweise
0.1	31.10.2024	Lukas Klose	Erstellung initiale Draft-Version
0.2	05.11.2024	Alexander Alldridge	Korrektur gelesen
0.3	13.11.2024	Lukas Klose	Einarbeitung Korrekturen

Inhaltsverzeichnis

1. Präambel

Die vorliegende Informationssicherheitsleitlinie legt die Informationssicherheitsstrategie, also die strategische Ausrichtung der Informationssicherheit, der EuroDaT GmbH (im Folgenden auch als EuroDaT bezeichnet) fest. In der Informationssicherheitsleitlinie werden die Grundsätze und die Organisation der Informationssicherheit bei EuroDaT definiert und Vorgaben für ein formales Rahmenwerk der Informationssicherheit aufgestellt. Es werden die Grundlagen für den Aufbau eines Informationssicherheits-Management-Systems (ISMS) gegeben, dass die Prozesse und Verantwortlichkeiten für die nachhaltige Steuerung der Informationsrisiken bei EuroDaT bereitstellt. Die Informationssicherheitsrichtlinie legt darüber hinaus den Orientierungsrahmen für das Management und alle Mitarbeiter:innen zur Ausgestaltung der Informationssicherheit bei EuroDaT fest.

Die Vorgaben der Informationssicherheitsrichtlinie resultieren u.a. aus der Geschäftstätigkeit von EuroDaT, welche im Kern die Tätigkeit als transaktionsbasierter Datentreuhänder beinhaltet. Basierend darauf stellt die Firma Richtlinien, Konzepte und Arbeitsanweisungen für alle Mitarbeiter:innen zur Verfügung, die den Umgang und die Prozesse zur Einhaltung der Sicherheit von Informationsgegenständen der Firma vorgeben. Darüber hinaus greifen die Vorgaben des ISMS für die Zusammenarbeit mit Kund:innen und Geschäftspartner:innen.

2. Informationssicherheit bei EuroDaT

EuroDaT ist ein transaktionsbasierter Datentreuhänder, welcher die technologischen, prozessualen und juristischen Rahmenbedingungen für einen Datentreuhänder als einen zentralen Baustein eines europäischen Daten-Ökosystems schaffen möchte. Der Grundgedanke hinter EuroDaT ist die unabhängige und neutrale Durchführung von Datentransaktionen.

Dabei legt EuroDaT Wert auf einen fairen Umgang mit Mitarbeiter:innen, Kunden und Geschäftspartner:innen. Der Erfolg des Datentreuhänders und der auf ihm aufbauenden Anwendungsfälle liegt in der engen und vertrauensvollen Zusammenarbeit mit den Kunden und innerhalb der Firma begründet.

Um diese strategischen Ziele als Datentreuhänder erreichen zu können, ist ein vertrauensvoller Umgang mit Informationswerten sowohl innerhalb der Organisation als auch der im Rahmen von Anwendungsfällen verarbeiteten Informationen von Kunden unerlässlich. Deshalb ist die Informationssicherheit ein fester Bestandteil der Geschäftsorganisation von EuroDaT. Ziel der Steuerung von Informationsrisiken ist die Vermeidung des Eintritts von Schäden bzw. die Minimierung oder der Transfer nicht vermeidbarer Risiken.

Bei jedem Einsatz von Informationen ist dabei der Schutzbedarf der Information hinsichtlich Vertraulichkeit, Integrität, Verfügbarkeit und Authentizität zu beachten. Dafür müssen die Sicherheitsrisiken der einzelnen Informationen (z.B. personenbezogene Daten, Kundendaten, Transaktionsdaten etc.) bewertet und Maßnahmen deren Sicherung praktiziert werden, um sie vor unsachgemäßer oder unzulässiger Verwertung, Verlust oder Manipulation zu schützen.

Nur durch eine Sachgemäße Anwendung der Informationswerte kann der Schutz der Informationssicherheit gewährleistet werden, um z.B. einen Reputationsverlust der Firma bei Kunden, Geschäftspartner:innen und allgemein am Markt zu vermeiden.

2.1.Methodik

Bei dem Schutz von Informationswerten orientiert sich EuroDaT an internationalen Standards, die sich in der Praxis bewährt haben. Dazu wurden die Vorgaben des ISO 27001:2022 Standards für Informationssicherheits-Managementsysteme herangezogen.

2.2.Gültigkeit (Scope)

Die vorliegende Sicherheitsleitlinie und somit der Anwendungsbereich des ISMS gilt für die gesamte Organisation und Tätigkeitsbereich von EuroDaT, d.h. die Entwicklung, Implementierung, Wartung und Betrieb von Software, die im Kontext von Datentreuhandschaft bei Kunden verschiedener Branchen, insbesondere des Finanzsektors, der Industrie und der öffentlichen Hand eingesetzt werden.

Für den Geltungsbereich des ISMS strebt EuroDaT eine Zertifizierung nach ISO 27001:2022 an.

2.3.Gesetzliche und vertragliche Rahmenbedingungen

Die Sicherheitsleitlinie der EuroDaT GmbH berücksichtigt regulatorische und gesetzliche Vorgaben, die ebenfalls eine Auswirkung auf die Informationssicherheit haben, sowie interne Richtlinien und vertragliche Verpflichtungen, insbesondere:

- **Datenschutz Grundverordnung der Europäischen Union (DSGVO):** Der in dieser Verordnung geregelte Umgang mit personenbezogenen Daten ist Teil der Sicherheitsleitlinie der EuroDaT GmbH. Verantwortlich für die Einhaltung der DSGVO ist der Datenschutzbeauftragte von EuroDaT.
- **Geistiges Eigentum:** Als Unternehmen beauftragt EuroDaT die Entwicklung von Software und verwaltet datentreuhänderisch Informationswerte. Bei den erstellten Lösungen und Konzepten ist auch das geistige Eigentum zu beachten, das als immaterielles Gut ebenfalls als Eigentum gemäß §14 BGB zu schützen ist.
- **Vertragliche Vereinbarungen:** Im Rahmen der Dienstleistungsverträge finden i.d.R. auch die kundenseitigen vertraglich vereinbarten Vorgaben hinsichtlich Informationssicherheit, Softwareentwicklung und Nutzung der Datentreuhandschaft EuroDaTs Anwendung. Darüber hinaus schließt EuroDaT auch Verträge mit u.a. Lieferanten und Geschäftspartnern ab, bei denen ebenfalls die Vorgaben zur Informationssicherheit mit in Betracht gezogen werden, sofern dies aufgrund des Vertragsgegenstandes und des Risikogehalts erforderlich ist.
- **Digital Operational Resilience Act (DORA):** Da EuroDaT unter anderem als Dienstleister für Finanzunternehmen agiert, sind das Beachten von Anforderungen an IKT-Drittdienstleister von DORA ein wichtiger Bestandteil des ISMS von EuroDaT.

3. Grundannahmen und Schutzziele der Informations-sicherheit bei EuroDaT

Die Grundsätze für die Informationssicherheit wird von der Geschäftsführung der EuroDaT GmbH vorgegeben und spiegeln die Geschäfts- und Risikostrategie der Firma wider.

Die Grundsätze verfolgen dabei die Einhaltung für die folgenden Schutzziele der Informationswerte:

3.1. Schutzziele

Für alle Informationswerte der EuroDaT GmbH, unabhängig davon, ob diese in elektronischer Form, als Ausdruck oder als mündliche Übermittlung vorliegen, sind stets die folgenden Schutzziele zu beachten und einzuhalten:

- **Vertraulichkeit:** Informationen dürfen nur den jeweiligen autorisierten Personen zugänglich sein. Es ist zu vermeiden, dass Informationen durch Zufall, Fehler oder durch Cyberangriffe offengelegt werden.
- **Integrität:** Die Informationswerte sind auf Richtigkeit und Vollständigkeit hin zu schützen. Hierunter fallen alle denkbaren Manipulationen, wie das Einfügen oder Löschen von Zeichen, das Umordnen von Daten oder Nachrichten, sowie Duplikate und weitere Möglichkeiten der unautorisierten Manipulation von Informationswerten.
- **Verfügbarkeit:** Die Verfügbarkeit bezeichnet die Eigenschaft einer Information oder eines Wertes, für einen berechtigten Nutzer verfügbar und nutzbar zu sein, sobald der Nutzer dies verlangt, sofern nicht andere zeitliche Vereinbarungen zur Verfügungstellung getroffen wurden (z.B. Einspielen eines Backups). Die Verfügbarkeit wird z.B. durch technische Störungen, aber auch durch Elementarschäden oder Naturkatastrophen bedroht. Im Hinblick auf das Schutzziel der Vertraulichkeit müssen neben den Daten von Kunden, Mitarbeitern und Geschäftspartnern auch die zu verarbeitenden Daten der Datentreuhandschaft ein besonderes Augenmerk erfahren.
- **Authentizität:** Die Authentizität bezieht sich auf die Eigenschaft, dass die Identität einer Person, eines Systems oder einer Information sicher und eindeutig verifiziert werden kann. Dies erfordert, dass kein unberechtigte:r Dritte:r in der Lage ist, die Identität einer anderen Partei erfolgreich zu imitieren oder vorzugeben, um auf die betroffenen Daten zuzugreifen oder diese zu manipulieren. Durch Nutzung vertrauenswürdiger Verifizierungsmethoden wie Passwörtern, biometrischen Daten oder digitalen Zertifikaten wird die Authentizität sichergestellt. Die Authentizität ist wichtig, um das Risiko von Identitätsdiebstahl, betrügerischem Datenzugriff und unautorisierten Handlungen zu minimieren.

3.2. Sicherheitsziele

Folgende übergeordnete Ziele wurden in Einklang mit der Informationssicherheitsstrategie festgelegt:

- Das ISMS der EuroDaT GmbH wird von einem von der Geschäftsführung ernannten Informationssicherheitsbeauftragten (ISB) betrieben;

- Es findet ein regelmäßiger Soll-Ist-Abgleich der von der Informationssicherheit vorgegebenen Maßnahmen statt;
- es wird eine ausreichende Verfügbarkeit informationsverarbeitender Einrichtungen und der verarbeiteten Informationen zur Erfüllung der Geschäftsanforderungen garantiert;
- es liegt ein ausreichendes Maß an Vertraulichkeit der Informationen durch Schutz vor unautorisierten Zugriffen vor;
- gesetzliche Bestimmungen, sonstige rechtsverbindliche Regelungen, sowie relevante interne Vorgaben müssen eigehalten werden;
- vertrauliche Informationen sollen nur verschlüsselt übertragen werden;
- Zugriffsberechtigungen auf vertrauliche Daten und Programme richten sich nach den Anforderungen der Organisationseinheiten aus und werden auf das notwendige Maß beschränkt („Need-to-Know-Prinzip“);
- die Mitarbeiter:innen werden hinsichtlich der Einhaltung der Informationssicherheit regelmäßig sensibilisiert, darüber hinaus werden allen Mitarbeiter:innen die für ihren Arbeitsbereich relevanten Sicherheitsaspekte bekanntgegeben;
- die Risiken des Auftretens von Informationssicherheitsvorfällen werden gesteuert und in geeigneter Form minimiert;
- Maßnahmen zum Umgang mit Ereignissen und Vorfällen zur Informationssicherheit werden getroffen;
- die Arbeitsabläufe innerhalb von EuroDaT werden sichergestellt;
- IT-Produktions- und IT-Test- bzw. Entwicklungsumgebungen werden getrennt;
- passwortgeschützte Datensicherungen werden regelmäßig angefertigt und an sicheren Orten verwahrt;
- geeignete Maßnahmen zur Überwachung von Aktionen privilegierter Benutzer werden umgesetzt;
- geeignete Maßnahmen zum Schutz von Schadsoftware und Cyberangriffen werden ergriffen;
- ausreichender Gebäudeschutz und Zutrittsregelungen für Schutzbereiche werden implementiert;
- identitätsabhängige, passwortgeschützte Zugänge zu Anwendungen und Daten werden bereitgestellt.

Zur Überwachung der Sicherheitsziele werden KPIs und weitere spezifische Sicherheitsziele festgelegt, die eine Überwachung und eine kontinuierliche Verbesserung des ISMS ermöglichen.

3.3. Grundannahmen

Die Informationssicherheit der EuroDaT GmbH basiert auf folgenden Prämissen, die als Grundannahmen in die Ausgestaltung des ISMS einfließen:

- **Zentraler Bestandteil der Geschäftspolitik:** Die Informationssicherheit ist ein

zentraler Bestandteil der Geschäftspolitik und liegt somit in der direkten Verantwortung der Geschäftsführung. Ziel ist es, dass nur solche Restrisiken für die Informationssicherheit verbleiben, die als akzeptabel angesehen werden.

- **Einführung eines ISMS:** Für die Steuerung der Informationssicherheit wurde ein Informationssicherheits-Management-System (ISMS) eingeführt, das sich nach den Vorgaben von ISO27001:2022 richtet.
- **Anpassung des Sicherheitsmanagements:** Das ISMS wird im Rahmen eines kontinuierlichen Verbesserungsprozesses laufend optimiert und angepasst. Durch Audits können Schwachstellen identifiziert und beseitigt werden. Darüber hinaus wird festgestellt, ob Erweiterungen notwendig sind, z.B. aufgrund einer Anpassung der Normen. Dadurch kann die Wirksamkeit und Effizienz des ISMS kontinuierlich verbessert werden.
- **Public Corporate Governance Kodex (PCGK) des Landes Hessen:** Als 100%ige Gesellschaft des Landes Hessen verpflichtet sich EuroDaT zur Einhaltung des PCGK, welcher wesentliche Regeln und Handlungsempfehlungen für die Steuerung, Leitung und Überwachung von Unternehmen darstellt, an denen das Land Hessen beteiligt ist. Der PCGK soll eine anhaltende Verbesserung der Leitung und Überwachung von Unternehmen anstoßen und dadurch eine Erfüllung der mit der Beteiligung verfolgten Ziele sicherstellen.
- **Weitere Dokumentation des Informationssicherheitsmanagements:** Der Aufbau des ISMS geht davon aus, dass eine Datenschutzrichtlinie, ein Rechtskataster, ein Business Continuity Management (BCM), ein Qualitätsmanagement und eine Compliance-Richtlinie bei EuroDaT außerhalb des ISMS vorliegen.

Diese Grundannahmen bilden die Basis für die Steuerung der Informationssicherheit (ISMS) bei der EuroDaT GmbH.

4. Informationssicherheitsmanagementsystem (ISMS)

Zur Steuerung der Informationssicherheits-Risiken wurde in der EuroDaT GmbH ein Informationssicherheitsmanagement-System (ISMS) auf Basis der in Kapitel 3.3 definierten Grundannahmen aufgebaut.

Das ISMS wird von dem:der Informationssicherheitsbeauftragten[2] (ISB) der EuroDaT GmbH verantwortet. Diese:r berichtet regelmäßig an die Geschäftsführung, welche alle notwendigen Ressourcen für die Sicherstellung der Informationssicherheit bei EuroDaT zur Verfügung stellt und bei Bedarf auch als Eskalationsinstanz dient.

In regelmäßigen Audits werden die Maßnahmen und Umsetzungen des ISMS geprüft und angepasst. Somit wird das ISMS einer kontinuierlichen Verbesserung und Aktualisierung (z.B. aufgrund neuer Bedrohungen) unterzogen. Verantwortlich für die Durchführung der Audits ist der:die ISB.

Das ISMS basiert auf den Vorgaben der ISO27001:2022-Norm, wobei der PDCA-Zyklus (Plan-Do-Check-Act) bei EuroDaT aus folgenden Phasen besteht:

4.1.Informationssicherheitsorganisation

Die Informationssicherheits-Organisation (IS-Organisation) gibt den Rahmen der Organisationssicherheit für EuroDaT vor und wird vom:von der ISB verantwortet.

Die IS-Organisation verfolgt dabei folgende Teilaspekte:

- Definition von Vorgaben und Prozessen
- Festlegung der Risikoakzeptanz der Geschäftsführung hinsichtlich Informationsrisiken

[2] In der Praxis wird der:die ISB auch mit dem englischen Begriff des Chief Information Security Officers (CISO) bezeichnet.

- Identifikation von Risiken, die eine Bedrohung für die Informationssicherheit darstellen
- Rollendefinition im Rahmen des ISMS
- Kapazitätsplanung der Ressourcen
- Schulungen der Mitarbeiter:innen
- Aufsetzen eines kontinuierlichen Verbesserungsprozesses

Im Rahmen des Verbesserungsprozesses sind periodisch die bei Einführung des ISMS festgelegten Ausarbeitungen dieser Teilaspekte hinsichtlich neuer Anforderungen und Änderungen anzupassen. Die Organisation des Verbesserungsprozesses obliegt dabei dem:der ISB.

4.2.Analyse der Informationswerte

Dieser Themenblock umfasst die Prozesse zur Identifikation und Analyse aller Informationswerte von EuroDaT. Enthalten in der Analyse ist auch der Ablageort bzw. Standort des Informationswertes. Dabei können Informationswerte auch in Klassen zusammengefasst werden, falls dies sinnvoll ist. Die Informationswerte werden in einer zentralen Information-Asset-Liste geführt.

4.3.Definition des Schutzniveaus

Dies umfasst Prozesse zur Festlegung des Schutzniveaus der einzelnen Informationswerte oder Informationsklassen anhand der möglichen Auswirkungen und der Bedrohungen. Die Einordnung richtet sich nach geschäftlichen bzw. betrieblichen Anforderungen oder nach Anforderungen Dritter. Dabei muss der Schutzbedarf hinsichtlich der Vertraulichkeit, Integrität und Verfügbarkeit der Informationswerte ermittelt werden.

4.4.Zuordnung von Maßnahmen

Für jeden Informationswert oder jede Klasse von Informationswerten werden Maßnahmen hin- sichtlich des ermittelten Schutzniveaus definiert. Hierzu wird auch der:die Owner des Informationswertes hinzugezogen. Die Umsetzung der Maßnahmen erfolgt dabei durch den:die Owner des Informationswertes. Der ISB überprüft regelmäßig, ob die Umsetzung mit den identifizierten Maßnahmen übereinstimmt.

4.5.Risikoanalyse

Über die Risikoanalyse werden die identifizierten Risiken analysiert und hinsichtlich ihrer Eintrittswahrscheinlichkeit und dem potenziellen Schaden bewertet. Dabei sind die eingeführten Maßnahmen hinsichtlich des verbleibenden Risikos mit einzubeziehen.

4.6.Risikomaßnahmen, Kontrollen und Monitoring

Die ermittelten Risiken werden mit Maßnahmen belegt, die zu einer Risikoreduzierung führen oder im Falle eines akzeptierten Restrisikos anzuwenden sind. Zudem findet eine Nachverfolgung dieser Maßnahmen durch den:die ISB statt.

Darüber hinaus wird auch ein Berichtswesen für die Informationssicherheit sowie ein kontinuierlicher Verbesserungsprozess etabliert. Verantwortlich dafür ist der:die ISB.

4.7. Meldung und Behandlung von Sicherheitsvorfällen

Es werden Prozesse zum Melden und Nachverfolgen von Sicherheitsvorfällen implementiert. Zusätzlich werden hinsichtlich gemeldeter Sicherheitsfälle KPIs definiert. Der ISB verfasst einen regelmäßigen Bericht der gemeldeten Schadensfälle für die Geschäftsführung.

5. Weitergehende Regelungen

5.1. Wahrung der Informationssicherheit bei Verträgen mit Dritten

Bei Verträgen mit Dritten ist die Wahrung der Informationssicherheit mit zu berücksichtigen und, sofern möglich, deren Einhaltung stichprobenhaft zu überprüfen. Insbesondere wird bei Verträgen mit Lieferanten die Einhaltung der Informationssicherheit, wie im Rahmen der vertraglichen Erfüllung sinnvoll, im Vertrag oder durch spezielle Service-Level-Vereinbarungen (SLAs) festgehalten. Bei externen Firmen, mit denen ein Vertragsverhältnis besteht, sind bei groben Verstößen Eskalationen bis hin zu Vertragsstrafen oder Vertragsbeendigung zu erwägen.

5.2. Durchsetzung

Das ISMS umfasst umfangreiche Kontrollen, so dass Verstöße identifiziert, korrigiert und ggf. auch geahndet werden können. Im Extremfall kann dies bei wiederholten bzw. dauerhaften Verstößen für Mitarbeiter:innen in arbeitsrechtliche Konsequenzen und für Geschäftspartner:Innen in die Auflösung der Geschäftsbeziehung münden.