ISMS – Informationssicherheitsmanagement

Richtlinie zum BCM

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:	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	06.11.2024	Koray Önder	Erstellung initiale Draft-Version
1.0	10.12.2024	Alexander Alldridge	Kleinere Korrekturen; Freigabe erteilt

Inhaltsverzeichnis

1 Einleitung

Die Geschäftskontinuität ist für den Erfolg und die Reputation von EuroDaT von zentraler Bedeutung. Als cloudbasierter Datentreuhänder, der ausschließlich auf digitale Infrastrukturen und Anwendungen angewiesen ist, sieht sich EuroDaT einzigartigen Herausforderungen und Risiken gegenüber. Ziel dieser Business Continuity Management (BCM) Richtlinie ist es, die fortlaufende Verfügbarkeit der Dienstleistungen sicherzustellen, selbst im Falle unerwarteter Störungen oder Notfälle.

Die Richtlinie verfolgt einen klaren, präventiven und reaktiven Ansatz:

- Es wird angestrebt, kritische Prozesse und Systeme durch zuverlässige Cloud-Technologien abzusichern.
- Datenverluste und Betriebsunterbrechungen sollen durch robuste Backup- und Wiederherstellungsmechanismen minimiert werden.
- Durch detaillierte Notfallprozeduren wird nach Eintreten eines Schadensfalles ein schnelles und geordnetes Hochfahren aller relevanten Systeme garantiert.

Diese Richtlinie berücksichtigt die spezifischen Anforderungen und Risiken einer cloudbasierten Arbeitsweise und richtet den Fokus auf digitale Resilienz. Sie ist bindend für alle internen Mitarbeiterinnen und externen Dienstleisterinnen, die an EuroDaTs Geschäftsprozessen beteiligt sind.

Die Implementierung, regelmäßige Überprüfung und Weiterentwicklung dieser Richtlinie soll sicherstellen, dass EuroDaT auch in herausfordernden Situationen handlungsfähig bleibt und unseren Kunden sowie Partnern ein Höchstmaß an Verlässlichkeit bietet.

2 Business Continuity Management bei EuroDaT

EuroDaT besitzt ein Reaktiv-BCMS gemäß BSI-Standard 200-4.

Als reaktives BCM beschränkt sich die Notfallplanung nur auf ausgewählte, als sehr zeitkritisch eingeschätzte Geschäftsprozesse. Anders als im Standard-BCMS werden nicht alle Geschäftsprozesse analysiert. Stattdessen wird in einer Voranalyse der Prozessumfang eingeschränkt. Die Methoden im Reaktiv-BCMS sind auf das Maß reduziert, das erforderlich ist, um nur die zeitkritischsten Geschäftsprozesse mit vorhandenen Mitteln der Institution abzusichern. Das BCMS kann zukünftig weiter zu einem Standard-BCMS ausgeweitet werden.

Als ausgewählte Szenarien mit Auswirkungen auf besonders zeitkritische Prozesse wurden identifiziert:

- Datensicherung und Wiederherstellung
- Notfallkonzept und Wiederanlauf (Notbetrieb)

Aspekte, die physische Räumlichkeiten wie Büros, Rechenzentren oder andere bauliche Einrichtungen betreffen, sind für EuroDaT aufgrund der strukturellen Ausrichtung nicht von Relevanz und finden daher in dieser Richtlinie (zunächst) keine Berücksichtigung.

Gleiches gilt für Fragestellungen im Zusammenhang mit Personalausfällen oder der Überbrückung von Ausfällen einzelner Mitarbeiter. Da das operative Modell von EuroDaT stark auf die Nutzung cloudbasierter Systeme sowie die Zusammenarbeit mit externen Dienstleistern ausgerichtet ist, ist die Thematik nur insofern relevant, als das von den externen Dienstleistern eine hauseigene BCM-Richtlinie (ISO 22301) gefordert wird. Es wird jedoch erwogen, diesen Aspekt zukünftig in die Richtlinie zu integrieren, um auch in diesem Bereich auf mögliche Risiken vorbereitet zu sein.

2.1 Informationssicherheit im Rahmen des BCM

Die Vorgaben und Prozesse sollen sicherstellen, dass auch in Notfällen die Informationssicherheit gewährleistet ist.

Der derzeitige Umfang der Notfall-Szenarien im Rahmen des Reaktiv-BCMS umfasst dabei jedoch noch nicht alle Notfälle, die im Rahmen des ISMS betrachtet werden sollen.

Aus diesem Grund ist die Notfall-Behandlung des ISMS derzeit noch losgelöst vom eigentlichen BCMS der Firma EuroDaT. Bei Einführung eines Standard-BCMS wird das Dokument entsprechend auf die dort getroffenen Vorgaben angepasst.

Die Aufrechterhaltung der Informationssicherheit in Notfällen wird somit als eigenständiger Prozess angesehen, der noch von der ISB kontrolliert wird.

3 Informationssicherheit und BCM

Auch bei Notfällen, also dem Eintreten widriger Umstände, ist die Informationssicherheit auf- recht zu erhalten. Dazu hat EuroDaT mehrere Vorkehrungen getroffen, die die Aufrechterhaltung informationssicherheitsrelevanter Prozesse bestmöglich sicherstellen.

Im Folgenden werden die einzelnen Aspekte des Continuity-Managements der Informations- sicherheit dargestellt.

3.1 Datensicherung und Wiederherstellung

Diese Richtlinie definiert den Ansatz zur Sicherstellung der kontinuierlichen Verfügbarkeit geschäftskritischer Daten und Anwendungen. Sie beschreibt die Prinzipien, Prozesse und Verantwortlichkeiten im Bereich Datensicherung und Wiederherstellung, insbesondere in einer cloudbasierten Umgebung. Ziel ist es, den Geschäftsbetrieb auch im Falle von Systemausfällen, Cyberangriffen oder anderen Vorfällen schnell und effektiv wieder aufnehmen zu können.

Diese Richtlinie gilt für alle cloudbasierten Anwendungen, Datenspeicher und IT-Systeme, die geschäftsrelevante Daten verarbeiten, speichern oder sichern. Physische Speichermedien und lokale Server fallen nicht unter den Anwendungsbereich dieser Richtlinie.

3.1.1 Grundsätze der Datensicherung und Wiederherstellung

Die effektive Sicherung und Wiederherstellung geschäftskritischer Daten bildet die Grundlage für die Aufrechterhaltung der Geschäftsprozesse in jeder Situation. Dabei geht es nicht nur um die regelmäßige Erstellung von Backups, sondern auch um deren Schutz, Integrität und Wiederverwendbarkeit im Ernstfall. Insbesondere in einer cloudbasierten Umgebung ist es entscheidend, klar definierte Standards und Abläufe zu etablieren, die den besonderen Anforderungen an Sicherheit, Verfügbarkeit und Compliance gerecht werden.

Im Folgenden sind die wesentlichen Grundsätze aufgeführt, die den Umgang mit Datensicherung und Wiederherstellung strukturieren:

- Regelmäßige Backups

Alle geschäftsrelevanten Daten werden regelmäßig gesichert.

Die Häufigkeit der Sicherungen richtet sich nach der Kritikalität der Daten und den vereinbarten Wiederherstellungszielen. Backups erfolgen automatisiert und werden in einer sicheren, geografisch redundanten Cloud-Umgebung gespeichert. Hierzu zählen auch jegliche Backups auf der Applikationsebene.

- Verschlüsselung und Schutz der Backups

Alle gesicherten Daten werden mit kryptografischen Verfahren verschlüsselt.

Zugriff auf Backup-Daten ist streng kontrolliert und nur autorisierten Personen oder

Systemen möglich.

- Prüfung und Validierung der Backups

Backups werden regelmäßig auf Integrität und Vollständigkeit überprüft.

Testwiederherstellungen werden in regelmäßigen Zeitabständen durchgeführt, um die Funktionsfähigkeit der Backup- und Recovery-Prozesse zu gewährleisten.

- Zugriffskontrolle und Rollenmanagement

Der Zugang zu Backup-Systemen ist auf dedizierte Rollen beschränkt.

Änderungen an den Backup-Richtlinien und -Einstellungen dürfen nur von autorisierten Administratoren durchgeführt werden.

3.1.2 Prozesse zur Wiederherstellung

Die Wiederherstellung geschäftskritischer Daten und Systeme erfolgt auf Basis definierter Prozesse, die für Notfälle und geplante Wiederherstellungen geeignet sind. Im Falle eines Vorfalls wird ein definierter Notfall-Wiederherstellungsprozess (Disaster Recovery) eingeleitet, der sicherstellt, dass die betroffenen Daten und Systeme priorisiert und so schnell wie möglich wiederhergestellt werden. Die Reihenfolge der Wiederherstellung orientiert sich dabei an der Kritikalität der betroffenen Daten und den im Notfallplan festgelegten Prioritäten.

Für geplante Wiederherstellungen, wie sie nach Systemupdates oder Migrationen erforderlich sein können, gelten kontrollierte Abläufe. Diese stellen sicher, dass alle relevanten Daten vollständig und konsistent verfügbar sind, ohne die Integrität oder den Betrieb der Systeme zu gefährden. Die Backup- und Wiederherstellungsmaßnahmen werden dabei stets in Übereinstimmung mit den in dieser Richtlinie definierten Vorgaben durchgeführt.

Die Zusammenarbeit mit externen Dienstleistern spielt eine zentrale Rolle bei der Umsetzung der Wiederherstellungsprozesse. Diese Dienstleister sind verpflichtet, die in Service-Level-Agreements (SLAs) festgelegten Standards einzuhalten. Regelmäßige Audits und Überprüfungen dienen dazu, die Einhaltung der vereinbarten Maßnahmen sicherzustellen und die Effektivität der Wiederherstellungsprozesse kontinuierlich zu verbessern.

3.1.3 Verantwortlichkeiten

Die Implementierung und Überwachung der Datensicherungs- und Wiederherstellungsprozesse liegt in der Verantwortung **der IT-Abteilung**. Diese ist zuständig für die Einhaltung der definierten Standards, die regelmäßige Durchführung von Backups sowie deren Validierung und Sicherstellung der Wiederherstellungsfähigkeit. **Die Geschäftsführung trägt die Verantwortung für die Überwachung und Genehmigung der Backup-Strategien sowie die Festlegung der Wiederherstellungsziele.**

Externe Dienstleister, die für die Bereitstellung und den Betrieb der Backup- und

Wiederherstellungsinfrastruktur zuständig sind, haben die Einhaltung aller vertraglich vereinbarten Standards und Sicherheitsmaßnahmen zu gewährleisten. Dabei werden ihre Leistungen regelmäßig überprüft, um die Einhaltung der Richtlinie sicherzustellen und mögliche Schwachstellen frühzeitig zu erkennen und zu beheben.

3.1.4 Überprüfung und Aktualisierung der BCM-Richtlinie

Die BCM-Richtlinie zur Datensicherung und Wiederherstellung wird regelmäßig überprüft, um sicherzustellen, dass sie den aktuellen technologischen Entwicklungen und geschäftlichen Anforderungen entspricht. Mindestens einmal jährlich erfolgt eine umfassende Revision der Richtlinie, bei der auch Erkenntnisse aus Vorfällen oder Prüfungen berücksichtigt werden.

Darüber hinaus kann die Richtlinie bei Bedarf jederzeit aktualisiert werden, etwa bei Einführung neuer Technologien, geänderten regulatorischen Anforderungen oder Erweiterungen der Geschäftsprozesse. Diese dynamische Anpassung gewährleistet, dass die Datensicherungs- und Wiederherstellungsmaßnahmen stets den höchsten Standards entsprechen und den langfristigen Geschäftserfolg unterstützen.

3.2 Notfallkonzept und Wiederanlauf (Notbetrieb)

Diese Richtlinie definiert die Vorgaben und Prozesse für das Notfallkonzept und den Wiederanlauf (Notbetrieb) EuroDaTs. Sie gewährleistet, dass im Falle eines schwerwiegenden Vorfalls der Geschäftsbetrieb schnellstmöglich auf einem minimalen, aber funktionsfähigen Niveau fortgeführt werden kann. Ziel ist es, die Verfügbarkeit geschäftskritischer Dienste sicherzustellen und die Auswirkungen auf Kunden, Partner und andere Interessensgruppen zu minimieren. Auch die Informationssicherheit bleibt während einer Störung ein zentrales Element des Notfallkonzepts und des Wiederanlaufs. Ziel hier ist es, Risiken für die Verfügbarkeit, Integrität und Vertraulichkeit sensibler Informationen selbst in Krisensituationen zu minimieren.

Diese Richtlinie gilt für die folgenden geschäftskritischen Prozesse:

- Entwicklung der EuroDaT-Plattform
- Updaten von Dependencies
- Deployment
- Ausführen von Datentransaktionen auf dem Datentreuhänder

Physische Systeme oder lokale IT-Infrastrukturen fallen nicht in den Anwendungsbereich.

3.2.1 Grundsätze des Notfallkonzepts und Wiederauflaufs

Das Notfallkonzept legt dar, wie der Geschäftsbetrieb bei einem unerwarteten Ereignis aufrechterhalten oder in einem minimalen Umfang wiederhergestellt werden kann. Der Wiederanlauf beschreibt die Maßnahmen zur Rückkehr in den Normalbetrieb nach der Überwindung des Notbetriebs. Folgende Prinzipien gelten:

- Priorisierung geschäftskritischer Systeme und Anwendungen: Es werden klare

Kriterien festgelegt, welche Dienste und Daten im Notbetrieb höchste Priorität haben.
- Sicherstellung minimaler Funktionsfähigkeit: Im Notbetrieb wird ein definierter Leistungsumfang bereitgestellt, der die grundlegenden Bedürfnisse der Kunden abdeckt.
- Geografisch redundante Infrastruktur: Die Nutzung cloudbasierter Dienste ermöglicht die Implementierung einer hochverfügbaren Infrastruktur mit geografischer Redundanz.

3.2.2 Prozesse im Notfallkonzept

Im Notfall wird ein definierter Ablaufplan initiiert, der folgende Schritte umfasst:

- Erkennung und Bewertung des Vorfalls: **Ein Incident-Response-Team** bewertet die Art und den Umfang des Vorfalls und entscheidet über die Aktivierung des Notbetriebs.
- Aktivierung des Notbetriebs: Die geschäftskritischen Systeme und Anwendungen werden auf die für den Notbetrieb vorgesehenen Cloud-Infrastrukturen umgeleitet oder wiederhergestellt.
- Kommunikation: Interne und externe Stakeholder werden unverzüglich über den Vorfall und den Notbetrieb informiert. Dies umfasst auch Transparenz gegenüber Kunden und Regulierungsbehörden.
- Überwachung und Anpassung: Während des Notbetriebs werden Systeme und Dienste kontinuierlich überwacht, um die Stabilität und Funktionsfähigkeit zu gewährleisten.

3.2.3 Übergang zum Normalbetrieb

Nach Stabilisierung der Situation erfolgt die Rückkehr zum Normalbetrieb. Der Wiederanlauf umfasst:

- Datenmigration: Vollständige Wiederherstellung aller Daten in die regulären Umgebungen.
- Validierung: Überprüfung der Integrität der Daten und Systeme nach dem Wechsel.
- Lessons Learned: Analyse des Vorfalls und Anpassung der BCM-Richtlinie, um zukünftige Vorfälle effektiver zu bewältigen.

3.2.4 Verantwortlichkeit und Überprüfung

Die Verantwortung für die Umsetzung und Überwachung des Notbetriebs ist klar verteilt. Die **IT-Abteilung** trägt die Hauptverantwortung für die technische Implementierung des Notbetriebs sowie die Wiederherstellung der Systeme. Die Geschäftsführung übernimmt die übergeordnete Überwachung der Prozesse und sorgt für eine effektive Kommunikation mit internen und externen Stakeholdern. Externe Dienstleister sind verpflichtet, die vereinbarten Maßnahmen und Standards für den Notbetrieb einzuhalten, um die Kontinuität der geschäftskritischen Prozesse sicherzustellen.

Das Notfallkonzept sowie die zugehörigen Wiederanlaufprozesse werden mindestens einmal jährlich überprüft. Diese regelmäßige Aktualisierung berücksichtigt neue technologische

Entwicklungen sowie Erkenntnisse aus Vorfällen oder Tests, um die Effektivität des Konzepts kontinuierlich zu verbessern.