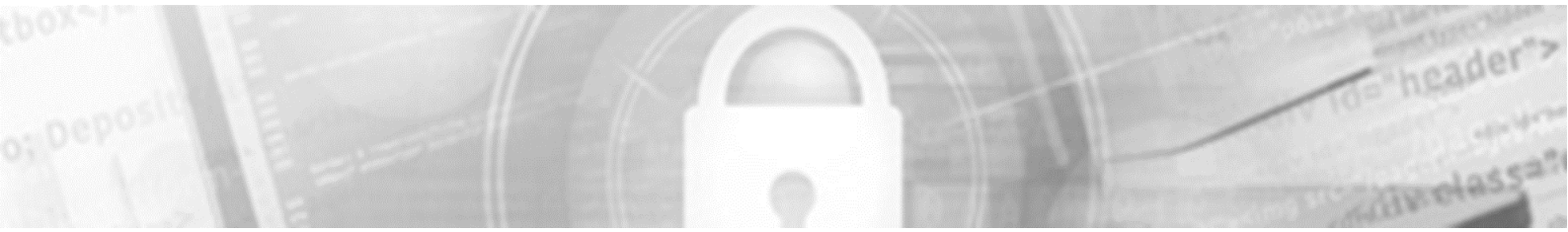


AdOrga Solutions

Datenschutz - Informationssicherheit

Synergien zwischen DS-GVO und DORA: Ein umfassender Ansatz zur Datensicherheit.

Autorin:
Regina Mühlich

Stand:
Mai 2024

Inhaltsverzeichnis

* Hinweis: Der Übersichtlichkeit wegen wurden nur männliche Formen verwendet.

Wie der Digital Operation Resilience Act (DORA) und die Datenschutz-Grundverordnung (DS-GVO) zusammenwirken, um Finanzunternehmen vor digitalen Bedrohungen zu schützen und die Sicherheit personenbezogener Daten zu gewährleisten. DORA, die NIS-2 für Finanzdienstleistungsunternehmen.

1 Einleitung

Mit der Verordnung (EU) 2022/2554 des europäischen Parlaments und des Rates vom 14.12.2022 über die **digitale operationale Resilienz im Finanzsektor** und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014, (EU) Nr. 909/2014 und (EU) 2016/1011 verpflichtet die Europäische Union Finanzunternehmen zur Stärkung ihrer digitalen operationalen Resilienz.[1]

> **Der Digital Operational Resilience Act (DORA) ist eine finanzsektorübergreifende europäische Verordnung und bündelt und harmonisiert Regelungen bestehender sektoraler europäischer Verordnungen und Richtlinien.**

Was sind Finanzsektoren?
Neben dem Kreditgewerbe gehören zum Finanzsektor Kapitalanlagegesellschaften, Leasinggesellschaften, Private-Equity-Unternehmen, Vermögensverwaltungen, Versicherungsunternehmen sowie die Zentralbanken. Unter „finanzsektorübergreifend" wird dabei eine stärkere Vernetzung der unterschiedlichen Sektoren verstanden.

Eines der **Hauptziele des DORA** ist es, dass Finanzunternehmen die volle Kontrolle über die Risiken behalten, die mit dem Einsatz von Informations- und Kommunikationstechnologien (IKT) verbunden sind. Dazu müssen die Unternehmen ein umfassendes IKT-Risikomanagement einführen. Das IKT-Risikomanagement schreibt vor, dass Finanzunternehmen bestimmte Anforderungen erfüllen müssen. Wie das IKT-Risikomanagement auszusehen hat, wird nicht vorgeschrieben. Der Digital Operational Resilience Act zielt also darauf ab, die **digitale Widerstandsfähigkeit** von Finanzunternehmen zu stärken.

2 Wesentliche Anforderungen des DORA

Die wesentlichen Anforderungen des DORA sind:

1. IKT-Risikomanagement

Unternehmen müssen robuste Strategien und Verfahren für das Management von Informations- und Kommunikationstechnologierisiken (IKT-Risiken) entwickeln und implementieren.

[1] https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022R2554 (abgerufen am 09.05.2024)

2. IKT-Sicherheitsanforderungen

Einführung und Aufrechterhaltung von Sicherheitsmaßnahmen, die auf dem neuesten Stand der Technik basieren, um IT-Systeme und Daten zu schützen.

3. Berichtspflichten bei IKT-Vorfällen

Verpflichtung zur Meldung signifikanter IKT-Vorfälle an die zuständigen Behörden innerhalb definierter Fristen.

4. Überwachung von Drittdienstleistern

Strenge Vorschriften zur Überwachung und Kontrolle von Drittanbietern, die kritische IT-Dienstleistungen erbringen.

5. Resilienz-Tests

Regelmäßige Durchführung von Tests zur Überprüfung der Widerstandsfähigkeit gegenüber ICT-Bedrohungen, einschließlich Penetrationstests und anderen Simulationen.

Obwohl die grundlegenden Ziele und Prinzipien der IT-Sicherheit und des Risikomanagements in den verschiedenen Sektoren ähnlich sind, gibt es spezifische Anpassungen und Anforderungen, die auf die besonderen Bedürfnisse und Risiken des jeweiligen Sektors zugeschnitten sind. VAIT, KAIT und ZAIT haben viele gemeinsame Ziele, unterscheiden sich jedoch in der Art und Weise, wie diese Ziele umgesetzt werden, um den branchenspezifischen Herausforderungen gerecht zu werden.

3 Regulatorische Leitlinien für IT in der Finanzbranche

BaFin-Rundschreiben zu IT-Management und Informationssicherheit

Der Einsatz von Informationstechnik (IT) in den Unternehmen, auch unter Einbeziehung von IT-Services, die durch IT-Dienstleister bereitgestellt werden, hat eine zentrale Bedeutung. Die von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)[2] veröffentlichten Rundschreiben enthalten Hinweise zur Auslegung der Vorschriften über die Geschäftsorganisationen, soweit sie sich auf die technisch-organisatorische Ausstattung der Unternehmen beziehen. Die Rundschreiben geben einen flexiblen und praxisnahen Rahmen vor, insbesondere für das Management der IT-Ressourcen, für das Informationsrisikomanagement und das Informationssicherheitsgesetz.
Die BaFin hat für die einzelnen Sektoren nachstehende Rundschreiben mit IT-Anforderungen veröffentlicht:

- **BAIT** – Bankaufsichtliche Anforderungen an die IT
  https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1710_ba_BAIT.pdf?__blob=publicationFile&v=2
- **VAIT** – Versicherungsaufsichtliche Anforderungen an die IT
  https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1810_vait_va_Aktualisierung_2022.pdf?__blob=publicationFile&v=2

- **KAIT** – Kapitalverwaltungsaufsichtliche Anforderungen an die IT https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1911_kait_wa.pdf?__blob=publicationFile&v=2
- **ZAIT** – Zahlungsdiensteaufsichtliche Anforderungen an die IT https://www.bafin.de/SharedDocs/Downloads/DE/Rundschreiben/dl_rs_1121_BA_ZAIT.pdf?__blob=publicationFile&v=2

4 Gemeinsame Ziele und Prinzipien der Sektoren

Die Grundprinzipien und Ziele der IT-Sicherheit und des Risikomanagements sind in den verschiedenen Finanzsektoren ähnlich.

Die Gemeinsamkeiten sind:

- **IT-Sicherheit**
  - Schutz der IT-Systeme und Datenintegrität
  - Prävention und Abwehr von Cyberangriffen
- **Risikomanagement**
  - Systematische Identifizierung, Bewertung und Steuerung von IT-Risiken
  - Integration von IT-Risiken in das Gesamt-Risikomanagement
- **Compliance**
  - Einhaltung gesetzlicher und regulatorischer Anforderungen
  - Regelmäßige Überwachung und Berichterstattung

Die Ziele und Prinzipien ähneln sich für die einzelnen Sektoren. So wie es in den Branchen unterschiedliche Prozesse gibt, so sind auch unterschiedliche und branchenspezifische Anforderungen und Schwerpunkte zu berücksichtigen. So sind im KAIT z.B. Liquidationsrisiken und Sicherheit von Banksystemen relevant, im VAIT sind dies z.B. das Schadenmanagement und die Integrität der IT-Systeme. Beim ZAIT dagegen steht u.a. die Transaktionssicherheit im Vordergrund.

5 Schnittstellen zwischen DORA und DS-GVO

Es gibt wichtige Schnittstellen zwischen DORA und dem Datenschutzrecht, der Datenschutz-Grundverordnung (DS-GVO). Beide Regelungen verfolgen das Ziel, Datensicherheit und Datenschutz zu gewährleisten, wenn auch aus unterschiedlichen Perspektiven.

Im Folgenden werden die wichtigsten Schnittstellen und ihre Auswirkungen dargestellt:

5.1 Schutz personenbezogener Daten

	DORA	DS-GVO
Fokus:	Sicherstellung der operativen Resilienz von Finanzunternehmen gegen digitale Bedrohungen, was indirekt auch den Schutz personenbezogener Daten umfasst.	Schutz der Privatsphäre und personenbezogener Daten von natürlichen Personen.
Anforderungen:	Einführung robuster Sicherheitsmaßnahmen, die auch den Schutz von Datenintegrität und Vertraulichkeit umfassen.	Vorschriften über die Verarbeitung, Speicherung und den Schutz personenbezogener Daten.
Schnittstelle:	Beide Regelungen erfordern die Implementierung von Sicherheitsmaßnahmen, die sicherstellen, dass (personenbezogene) Daten vor unbefugtem Zugriff, Verlust oder Missbrauch geschützt sind.	

5.2 Meldung von Sicherheitsvorfällen

	DORA	DS-GVO
Anforderungen:	Verpflichtet Finanzunternehmen, erhebliche IKT-Sicherheitsvorfälle innerhalb kurzer Zeit an die zuständigen Aufsichtsbehörden zu melden.	Verpflichtet Unternehmen, Datenschutzverletzungen, die zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führen, innerhalb von 72 Stunden an die Datenschutzbehörden zu melden.
Ziel:	Minimierung der Auswirkungen von Sicherheitsvorfällen auf die operative Resilienz und den Finanzmarkt.	Schutz der Privatsphäre und der Rechte betroffener Personen.
Schnittstelle:	Beide Regelungen legen Wert auf eine schnelle Meldung von Vorfällen, um die Auswirkungen auf betroffene Personen und Unternehmen zu minimieren. Unternehmen müssen Mechanismen einführen, um sicherzustellen, dass sowohl Datenschutzverletzungen als auch ICT-Sicherheitsvorfälle effizient gemeldet werden.	

5.3 Risikomanagement

	DORA	DS-GVO
Anforderungen:	Entwicklung und Implementierung eines umfassenden IKT-Risikomanagements zur Identifizierung, Bewertung und Steuerung von Risiken, einschließlich derer, die personenbezogene Daten betreffen könnten.	Erfordert die Durchführung von Datenschutz-Folgenabschätzungen (DSFA) für Verarbeitungsvorgänge, die voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen darstellen.
Schnittstelle:	Beide Regelungen erfordern ein systematisches Risikomanagement, das die Identifizierung und Bewertung von Risiken umfasst, einschließlich derer, die sich auf personenbezogene Daten auswirken.	

5.4 Technische und organisatorische Maßnahmen (Sicherheit der Verarbeitung)

	DORA	DS-GVO
Anforderungen:	Finanzunternehmen müssen geeignete technische und organisatorische Maßnahmen implementieren, um die Widerstandsfähigkeit ihrer IT-Systeme sicherzustellen.	Unternehmen müssen technische und organisatorische Maßnahmen treffen, um ein dem Risiko angemessenes Mindestschutzniveau für personenbezogene Daten zu gewährleisten.
Schnittstelle:	Beide Regelungen verlangen die Implementierung geeigneter Maßnahmen, um die Sicherheit und den Schutz von IT-Systemen und Daten zu gewährleisten.	

5.5 Kontrollen und Audits

	DORA	DS-GVO
Anforderungen:	Regelmäßige Überprüfung und Auditierung der IKT-Risikomanagement- und Sicherheitsprozesse.	Verpflichtet Unternehmen zur regelmäßigen Überprüfung der Einhaltung der Datenschutzbestimmungen und zur Durchführung von Datenschutz-Audits.

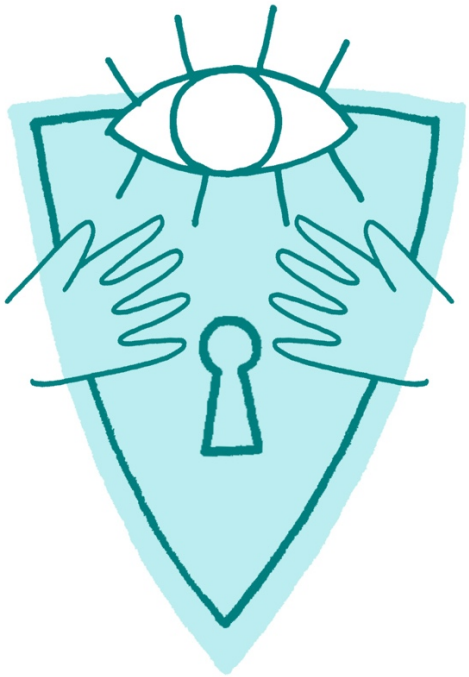
Schnittstelle:	Beide Regelungen fordern eine regelmäßige Überprüfung und Auditierung, um die Wirksamkeit der implementierten Maßnahmen sicherzustellen.

6 Zusammenfassung

Die Schnittstellen zwischen DORA und DSGVO zeigen, dass beide Regelungen auf die Sicherstellung der Datenintegrität, Vertraulichkeit und Verfügbarkeit abzielen, wenn auch mit unterschiedlichem Schwerpunkt. Während DORA primär auf die operative Resilienz und IT-Sicherheit im Finanzsektor fokussiert ist, legt die DSGVO den Schwerpunkt auf den Schutz personenbezogener Daten. Die Implementierung von Maßnahmen zur Einhaltung beider Regelungen erfordert einen integrierten Ansatz, der sowohl IT-Sicherheits- als auch Datenschutzaspekte berücksichtigt.

7 Autorin

Regina Mühlich ist Wirtschaftsjuristin und Geschäftsführerin der AdOrga Solutions GmbH und seit über 20 Jahren im Datenschutz tätig. Sie ist zert. Datenschutzbeauftragte, CIPM (IAPP), anerkannte und geprüfte Sachverständige für Systeme und Anwendungen der Informationsverarbeitung im kaufmännisch-administrativen Bereichen (IT) und für Datenschutz, Informationssicherheitsbeauftragte (TÜV), IT Security Fundamentals in ISO 27001, Penetration Testing & Forensic Investigation (ICO Certificate, ID 003E1KQR), Auditoren für Datenschutz und Qualitätsmanagement, Scrum Master (PMI), zert. Compliance Manager sowie zert. CSR-/ Nachhaltigkeits-Beauftragte. Als Datenschutzexpertin und Compliance Manager berät und unterstützt sie mit ihrem Team nationale und internationale Unternehmen aus unterschiedlichsten Branchen. Sie ist Vorständin des Berufsverbands der Datenschutzbeauftragten Deutschlands (BvD) e. V.



(Bildquelle: © AdOrga Solutions GmbH)