

SICHERHEIT **FÜR IHRE DATEN**

mit Fellowes



***DSGVO-** und **NIS-2**-Richtlinien
verstehen – Datenschutz als
Teil Ihres Arbeitsalltags*

Fellowes

EINFÜHRUNG

Warum Datenschutz wichtiger ist als je zuvor

In einer zunehmend vernetzten Welt mit Cyber-Bedrohungen und Datenschutzrisiken ist Datenschutz nicht länger optional. Der Schutz Ihrer Unternehmensdaten ist essenziell – und die Einhaltung von Datenschutzgesetzen wichtiger denn je.

Regelungen wie die DSGVO und die aktualisierte NIS-2-Richtlinie verpflichten Unternehmen dazu, sensible und personenbezogene Daten sowohl physisch als auch digital verantwortungsvoll zu schützen. Verstöße können schwerwiegende Folgen haben – von hohen Geldbußen über Reputationsverluste bis hin zur persönlichen Haftung von Führungskräften.

Dieser Leitfaden verschafft Ihnen einen klaren Überblick über beide Regelwerke, erklärt Ihre Pflichten verständlich und unterstützt Sie dabei, gezielt und sicher Maßnahmen zur Einhaltung zu ergreifen.

***Mehr Sicherheit für Ihre Daten.
Schützen Sie Ihr Unternehmen.
Bleiben Sie rechtskonform.***



Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die sich auf eine lebende Person beziehen, die direkt oder indirekt identifiziert werden kann, z. B.:



Name



Adresse



Sozialversicherungsnummer



Videoüberwachungsmaterial

***Datenschutz bedeutet,
sowohl digitale als auch
papierbasierte Informationen
zu schützen – denn ein
Datenleck kann in beiden
Formen auftreten.***



WAS IST NIS-2?

Cybersecurity in Europa stärken

Die Richtlinie über Netz- und Informationssicherheit 2 (NIS-2) ist die neueste EU-Gesetzgebung zur Verbesserung der Cybersicherheit und Erhöhung der Resilienz in kritischen Sektoren. Sie trat 2023 in Kraft, alle EU-Mitgliedstaaten müssen sie bis Oktober 2024 umgesetzt haben.

NIS-2 erkennt an, dass moderne Volkswirtschaften zunehmend auf digitale Infrastrukturen angewiesen sind – und dass Cyberangriffe erhebliche, teils existenzbedrohende Folgen haben können. Deshalb erstreckt sich der Geltungsbereich der Richtlinie auf sowohl essenzielle als auch wichtige Einrichtungen.

Gilt NIS-2 für Ihr Unternehmen?

Wenn Ihr Unternehmen eine Schlüsselrolle in der Wirtschaft oder Gesellschaft spielt, auch indirekt, fällt es wahrscheinlich unter NIS-2. Die Richtlinie betrifft Produkte und Dienstleistungen, die als „essenziell“ oder „wichtig“ eingestuft werden.

Essenzielle Einrichtungen:



Energie



Transport



Digitale
Infrastruktur



Banken



Finanzmarktinfrastruktur



Trinkwasser



ICT-Management



Öffentliche
Verwaltung



Raumfahrt



Abwasser



Gesundheit

Wichtige Einrichtungen:



Post- &
Kurierdienste



Abfallwirtschaft



Produktion



Chemieproduktion



Forschung



Lebensmittelproduktion



Digitale Anbieter

Die zwei Grundprinzipien von NIS-2

Unternehmen, die unter NIS-2 fallen, müssen sowohl präventive Maßnahmen als auch Reaktionsmechanismen implementieren.



Sorgfaltspflicht:

Organisationen müssen angemessene technische, operative und organisatorische Maßnahmen zur Sicherung der digitalen Sicherheit und Kontinuität ergreifen.

Dazu gehören IT-Systemschutz, Schwachstellenbewertung, Lieferkettenrisiken und Verantwortlichkeit auf Managementebene.



Meldepflicht:

Organisationen müssen relevante nationale Behörden über signifikante Vorfälle informieren. Größere Störungen müssen innerhalb von 24 Stunden gemeldet werden, andere Vorfälle innerhalb von 72 Stunden. Ein abschließender detaillierter Bericht muss innerhalb eines Monats vorgelegt werden.

Strafen bei Nichteinhaltung:

Verstöße können zu schweren finanziellen und operativen Konsequenzen führen:

GELDBÜßEN
Bis zu



10 Mio. €

oder 2% des weltweiten Jahresumsatzes
für **essenzielle Einrichtungen**

GELDBÜßEN
Bis zu



7 Mio. €

oder 1,4% des weltweiten Jahresumsatzes
für **wichtige Einrichtungen**

Geschäftsführer können persönlich haftbar gemacht werden, einschließlich temporärer oder permanenter Berufsverbote in bestimmten Sektoren.

Das unterschätzte Risiko: Papierdatenlecks

NIS-2 legt den Fokus auf digitale Resilienz – doch auch physische Daten bergen erhebliche Risiken. Werden sie vernachlässigt, drohen Sicherheitslücken, die Bußgelder und Reputationsschäden nach sich ziehen können. Jeder Vorfall, bei dem personenbezogene Daten verloren gehen, entwendet oder unbefugt offengelegt werden, gilt als Datenschutzverletzung – auch bei Papierdokumenten. Dazu zählen etwa Verträge im Restmüll, offen liegende Tabellen auf Schreibtischen, unverschlossene Personalakten oder Rechnungen im Altpapier. Jede dieser Situationen kann zu erheblichen Konsequenzen führen – einschließlich Geldstrafen, rechtlicher Haftung und nachhaltiger Rufschädigung.

WAS IST DIE DSGVO?

Schutz personenbezogener Daten

Die Datenschutz-Grundverordnung (DSGVO) regelt seit 2018 den Datenschutz in der EU und im Vereinigten Königreich. Sie stellt sicher, dass personenbezogene Daten rechtmäßig, transparent und sicher verarbeitet werden.

Die 6 Grundprinzipien des Datenschutzes

Diese Prinzipien bilden das Fundament jeder Datenschutzstrategie:

- 1. Rechtmäßigkeit:** faire und transparente Verarbeitung
- 2. Zweckbindung:** Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden und nicht in einer Weise weiterverarbeitet werden, die mit diesen Zwecken unvereinbar ist.
- 3. Datenminimierung:** Die Verarbeitung muss auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt, angemessen und relevant sein.
- 4. Richtigkeit:** Personenbezogene Daten müssen sachlich richtig und – wenn nötig – auf dem neuesten Stand sein. Ungenauigkeiten sind unverzüglich zu korrigieren oder zu löschen
- 5. Speicherbegrenzung:** Daten dürfen nur so lange gespeichert werden, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist.
- 6. Integrität und Vertraulichkeit:** Eine angemessene Sicherheit der Daten muss gewährleistet sein

Wann müssen Datenverstöße gemeldet werden?

Verstöße müssen innerhalb von 72 Stunden an die Aufsichtsbehörden gemeldet werden, in bestimmten Fällen auch an betroffene Personen.



Strafen bei Nichteinhaltung:

Verstöße können hohe Geldstrafen nach sich ziehen:

GELDBÜßEN
Bis zu



20 Mio. €

oder 4% des globalen Umsatzes, je nachdem, **welcher Wert höher ist**

NIS-2 vs. DSGVO

Die Unterschiede verstehen

Zusammenfassend ein kurzer Überblick über die Unterschiede der beiden Regelwerke:

ASPEKT	NIS-2	DSGVO
Fokus	Cybersicherheit & digitale Resilienz in essenziellen und wichtigen Sektoren	Schutz personenbezogener Daten (digital & Papier) für alle Organisationen, die Daten von EU-/UK-Bürgern verarbeiten
Anwendungsbereich	Essenzielle & wichtige Einrichtungen (Energie, Transport, Banken, Gesundheit, digitale Infrastruktur etc.)	Jede Organisation, die personenbezogene Daten sammelt, speichert oder verarbeitet
Grundprinzipien	Sorgfaltspflicht & Meldepflicht	Sechs Datenschutzprinzipien (Rechtmäßigkeit, Zweckbindung, Datenminimierung, Genauigkeit, Speicherbegrenzung, Integrität & Vertraulichkeit)
Meldepflicht bei Verstößen	Behörden innerhalb von 24 Std. (Störung), 72 Std. (andere Fälle)	Aufsichtsbehörde innerhalb von 72 Std. ggf. auch betroffene Personen
Strafen	Bis zu 10 Mio. € oder 2 % (essenzielle), bis 7 Mio. € oder 1,4 % (wichtige)	Bis 20 Mio. € oder 4 % des globalen Umsatzes
Managementhaftung	Geschäftsführer können persönlich haftbar gemacht werden	Organisation wird bestraft, Verantwortlichkeit kann Datenschutzbeauftragten/Manager betreffen

Praktische Maßnahmen

Konformität stärken

Für die meisten Organisationen bedeutet die Einhaltung von NIS-2 und DSGVO eine Kombination aus klaren Richtlinien, sicherer Technologie und täglichem Bewusstsein der Mitarbeitenden.

1 Rechtliche Pflichten klären

Prüfen, ob Ihr Unternehmen als essenzielle oder wichtige Einrichtung unter NIS-2 fällt

DSGVO-Verantwortlichkeiten prüfen und verstehen, welche Daten warum verarbeitet werden

2 Sicherheitspraktiken stärken

Firewalls, Verschlüsselung und Incident-Response-Pläne implementieren und regelmäßig aktualisieren

Physische Risiken nicht übersehen – Kontrolle von Druckausgaben, Ablage und sicherer Entsorgung

3 Meldeverfahren definieren

Klare Eskalationswege für Vorfälle festlegen

Zuständigkeiten für Meldung und Dokumentation zuweisen

Team auf strenge Meldefristen (24–72 Std.) vorbereiten

4 Mitarbeitende regelmäßig schulen

Datenschutz im Alltag verankern, nicht nur in der IT-Policy.

Digitale Risiken (Phishing, Passwortpflege) und Papierhandhabung (Aufbewahrung, Vernichtung) abdecken

5 Dokumenten-Lifecycle kontrollieren

Sichere Prozesse zu zur sicheren Vernichtung nicht mehr benötigter Papierunterlagen etablieren

Sensible Dokumente bis zur Entsorgung sicher lagern

Nur notwendige Unterlagen aufbewahren – Archive regelmäßig prüfen und ablaufende Dokumente sicher vernichten

Fellowes-Lösungen

Praktische Tools zur Unterstützung der Richtlinien-Einhaltung

Von DSGVO-konformer Aktenvernichtung bis zu organisierter Archivierung und Bildschirm-Privatsphäre helfen Fellowes-Lösungen, Informationen in jeder Phase des Produkt-Life-Cycles zu schützen – und unterstützen die Einhaltung von NIS-2 und DSGVO.

Herausforderung:

Papierbasierte Datenschutzverletzungen vermeiden

Lösung:

Aktenvernichter – In die Dokumentenrichtlinie integriert, minimieren sie das Risiko von Datenschutzverstößen. Nicht mehr benötigte Unterlagen werden mit einem Partikelschnitt-Aktenvernichter sicher vernichtet, sodass sensible Daten nicht mehr gelesen und missbraucht werden können.

Aktenvernichter entdecken



Herausforderung:

Physische Dokumente sicher und systematisch aufbewahren

Lösung:

Archivierungslösungen – Mit klar gekennzeichneten, gut organisierten BANKERS BOX®-Produkten können Dokumente sicher zwischen Standorten transportiert werden, bis sie entsorgt werden.

Entdecken Sie unsere Aufbewahrungs- und Organisationslösungen



Herausforderung:

Bildschirmdaten vor neugierigen Blicken schützen

Lösung:

Blickschutzfilter – Verhindern visuelle Datendiebstähle auf Bildschirmarbeitsplätzen, ideal für hybride Arbeitsplätze und gemeinsam genutzte Büros.

PrivaScreen™ Blickschutzfilter



Herausforderung:

Geräte unterwegs oder in Gemeinschaftsbereichen sichern

Lösung:

Laptop-Schutz – Die Breyta™-Laptop-Tasche mit Schloss schützt Laptop, wichtige Dokumente und Zubehör. Sie dient zugleich als Laptop-Erhöhung für ergonomisches Arbeiten.

Einführung von Breyta™





Datenschutz ist längst keine reine IT-Aufgabe mehr. Es ist eine organisationsweite Verpflichtung. Durch die Ausrichtung an DSGVO und NIS-2 und die Integration sicherer Dokumenten- und Datenpraktiken in den Arbeitsalltag lassen sich Bußgelder vermeiden, Vertrauen stärken und die organisatorische Resilienz erhöhen.

Machen Sie Datenschutz zu einem Teil Ihres Arbeitsalltags.

Fellowes
Brands-

FAMILIENUNTERNEHMEN
SEIT 1917

www.fellowes.com