GDPC GbR | Ludwig-Erhard-Straße 12 | 34131 Kassel

Informationsbrief – Mandanteninformation gemäß Art. 39 Abs. 1 lit. a DSGVO

GLOBAL DATA PROTECTION CONSULTING
Securing Business for the Future

Datum: 05.11.2024

NIS 2-Richtlinie – Was bedeutet das für Unternehmen?

Sehr geehrte Mandanten der GDPC,

wir möchten Sie heute über die Entwicklungen im Rahmen der NIS-2-Richtlinie informieren. NIS 2 bringt viele offene Fragen und Herausforderung mit sich; wir als GDPC planen, Sie Anfang nächsten Jahres im Bereich NIS 2 und Informationssicherheit konzeptionell mit einem neuen Portfolio-Baustein konkret unterstützen zu können. Ob Sie grundsätzlich in den Anwendungsbereich der NIS 2 Richtlinie fallen und welche Anforderungen sich daraus ergeben, haben wir Ihnen nachfolgend summarisch zusammengefasst.

1 Was ist die NIS 2 Richtlinie?

Die NIS 2 Richtlinie ist eine Überarbeitung der bisherigen EU-Richtlinie zur Netz- und Informationssicherheit (NIS-1). Deutschland und die anderen EU-Mitgliedstaaten mussten aber die neue NIS 2 Richtlinie bis 17. Oktober 2024 in nationales Recht überführen. In Deutschland existieren bisher jedoch nur Referentenentwürfe und ein Diskussionspapier für das „NIS 2 Umsetzungs- und Cybersicherheitsstärkungsgesetz“, https://www.bundestag.de/presse/hib/kurzmeldungen-1022586. Deutschland hat die Umsetzungsfrist folglich verpasst. Das BMI rechnet derzeit mit einer Verabschiedung / Inkrafttreten des Gesetzes Q1 2025 (https://nis2-navigator.de/aktueller-stand-nis2/).

2 Falle ich unter den Anwendungsbereich der NIS 2 Richtlinie?

Eine der zentralen Fragen ist, ob bzw. welche Unternehmen unter den Anwendungsbereich der Richtlinie bzw. des nationalen Umsetzungsgesetzes fallen. NIS 2 betrifft nicht mehr nur sogenannte „Betreiber kritischer Infrastrukturen“, sondern auch eine Vielzahl weiterer Sektoren und Unternehmen. Dazu gehören beispielsweise:

- **Digitale Dienstleister**: Anbieter von Cloud-Diensten, Rechenzentren, Content Delivery Networks (CDNs), Domain-Registrierungsdienste und Plattformen für E-Commerce.
- **IT-Dienstleister und Softwarehersteller**: Unternehmen, die essenzielle IT-Dienstleistungen oder Softwareprodukte herstellen / anbieten.
- **Energieunternehmen**: Hierzu zählen bspw. Betreiber von Stromnetzen, Öl- und Gasunternehmen, sowie Unternehmen im Bereich erneuerbare Energien.
- **Transportwesen**: Luftverkehrsunternehmen, Reedereien, Eisenbahnunternehmen und Betreiber öffentlicher Verkehrsmittel sind Teil des erweiterten Anwendungsbereichs.
- **Gesundheitswesen**: Krankenhäuser, pharmazeutische Unternehmen, Labore und Forschungseinrichtungen im Bereich Medizin.

- **Finanzwesen u. Versicherungssektor**: Banken, Finanzdienstleister und Versicherungen.
- **Wasserwirtschaft**: Unternehmen, die für die Bereitstellung und Verteilung von Trinkwasser und die Abwasserbehandlung verantwortlich sind.
- **Lebensmittelproduktion und -versorgung**: Unternehmen, die eine wesentliche Rolle bei der Herstellung und Lieferung von Lebensmitteln spielen, wie Agrarbetriebe und Lebensmittelgroßhändler.
- **Abfall- und Entsorgungsunternehmen**: Betriebe, die für die Abfallentsorgung und das Recycling zuständig sind, werden ebenfalls als kritische Dienste eingestuft.
- **Öffentliche Verwaltung und Regierungsstellen**: Staatliche Einrichtungen, die für wichtige Verwaltungsdienste zuständig sind.

Ob Ihr Unternehmen konkret in den Anwendungsbereich der NIS 2 fällt, hängt von mehreren Faktoren ab, darunter Ihre Branche, die Größe Ihres Unternehmens und dessen Relevanz für die allgemeine Wirtschaft oder Gesellschaft. Ein wesentlicher Punkt ist dabei auch die Einstufung nach Schwellenwerten, wie der Anzahl der Beschäftigten und dem jährlichen Umsatz. Kleinere Unternehmen und Organisationen (unter 50 Mitarbeiter / Jahresumsatz weniger als 10 Millionen € pro Jahr) könnten zwar ausgenommen sein, unterliegen jedoch der NIS 2, wenn sie von wesentlicher Bedeutung für die Versorgungssicherheit oder Wirtschaft (bspw. kritische Infrakturanbieter) sind. Für sog. "große Unternehmen", die mehr als 249 Mitarbeiter beschäftigen oder einen Jahresumsatz von 50 Millionen € erzielen, gelten erhöhte Anforderungen.

Konzernunternehmen / Unternehmensverbund**:** Für Konzerngesellschaften bedeutet das, dass jedes Unternehmen im Verbund unabhängig für die Erfüllung dieser Sicherheitsanforderungen verantwortlich ist, sofern die entsprechenden Voraussetzungen (Schwellwerte, Branchen-/Sektor Tätigkeit) vorliegen. Inwiefern die Daten (Umsatz, MA-Anzahl) der verbundenen Unternehmen hinzuzurechnen sind, ist kompliziert und muss separat geprüft werden (siehe hierzu S. 156 des Referentenentwurfs).

Wichtig: Während die EU-Richtlinie einen Mindeststandard für alle Mitgliedstaaten festlegt, bietet sie Spielraum für den deutschen Gesetzgeber, bestimmte Definitionen zu präzisieren oder sektorspezifische Ausnahmen zu bestimmen. Deutschland könnte beispielsweise Schwellenwerte, wie die Anzahl der Beschäftigten oder den Jahresumsatz, genauer definieren und anpassen, um den Anwendungsbereich auf Unternehmen zu beschränken, die als besonders wichtig für die Versorgungssicherheit gelten. Zudem ist es denkbar, dass das nationale Gesetz bestimmte Branchen differenziert behandelt oder zusätzliche Sektoren, die von lokaler Bedeutung sind, einbezieht. Auch könnten Klarstellungen zur Abgrenzung zwischen großen Unternehmen und KMU vorgenommen werden. Da das nationale Gesetz noch nicht verabschiedet wurde, lässt sich noch nicht in allen Fällen mit 100%-Sicherheit der Anwendungsbereich bestimmen.

Um allerdings eine erste Einschätzung zu erhalten, ob Ihr Unternehmen voraussichtlich unter den Anwendungsbereich der NIS 2 fallen könnte, können Sie einen Self-Check auf der Webseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) durchführen, abrufbar unter: BSI - NIS-2-Betroffenheitsprüfung oder alternativ unter: https://nis2-navigator.de/nis2-betroffenheitsanalyse. Dieser Test hilft Ihnen, die Relevanz der Richtlinie für Ihr Unternehmen zu prüfen und gegebenenfalls die notwendigen Schritte einzuleiten.

3 Was beinhaltet die NIS 2 Richtlinie konkret?

Die Umsetzung der NIS 2 Richtlinie und des geplanten deutschen NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetzes wird Unternehmen verpflichten, umfassende Maßnahmen zur Cyber-/Datensicherheit einzuführen. Nachfolgend finden Sie eine Liste von exemplarischen/beispielhaften Umsetzungsmaßnahmen:

1. Einführung eines umfassenden Cybersicherheits-Risikomanagements

- **Maßnahmen**: Regelmäßige Risikoanalysen durchführen, um potenzielle Schwachstellen zu identifizieren und zu bewerten.
- **Beispiel**: Ein Energieversorger erstellt halbjährlich einen Risikobericht und passt seine Schutzmaßnahmen auf Grundlage der neuesten Bedrohungslage an.

2. Technische Schutzmaßnahmen

- **Maßnahmen**: Implementierung von Firewalls, Intrusion-Detection-Systemen (IDS) und Verschlüsselungstechniken, inkl. Implementierung von Ende-zu-Ende-Verschlüsselungen, je nach Art der Daten.
- **Beispiel**: Ein Gesundheitsdienstleister verwendet Datenverschlüsselung, um den Schutz sensibler Patientendaten zu gewährleisten und installiert ein IDS zur Erkennung unbefugter Zugriffsversuche.

3. Vorfallmanagement und Meldepflichten

- **Maßnahmen**: Einführung eines Prozesses zur Erkennung, Reaktion und Meldung von Sicherheitsvorfällen innerhalb der Fristen (in der Regel 24 bis 72 Stunden).
- **Beispiel**: Ein Cloud-Dienstleister richtet ein 24/7-Überwachungssystem ein und schult ein Incident-Response-Team, das bei einem Vorfall sofort Maßnahmen einleitet und den Vorfall an die zuständige Behörde meldet.

4. Sensibilisierung und Schulung der Mitarbeiter

- **Maßnahmen**: Regelm. Schulungen zur Cyber-/Informationssicherheit für Mitarbeiter.
- **Beispiel**: Ein Transportunternehmen führt regelmäßige Schulungen für Fahrer und Disponenten durch, um sie über Phishing-E-Mails und andere potenzielle Cyberbedrohungen zu informieren.

5. Sicherheitsmaßnahmen für die Lieferkette

- **Maßnahmen**: Sicherstellung, dass auch Lieferanten und Partnerunternehmen Cybersicherheitsanforderungen erfüllen.
- **Beispiel**: Ein Pharmaunternehmen überprüft Verträge mit Zulieferern und fordert von diesen die Einhaltung bestimmter IT-Sicherheitsstandards.

6. Sicherheitsrichtlinien und Dokumentation

- **Maßnahmen**: Erstellung und regelmäßige Aktualisierung von internen Sicherheitsrichtlinien sowie Dokumentation von Maßnahmen und Prozessen.

- **Beispiel**: Ein IT-Dienstleister entwickelt ein Handbuch mit genauen Anweisungen zu Sicherheitsprozessen und aktualisiert es monatlich anhand neuer regulatorischer Vorgaben.

7. Durchführung regelmäßiger Penetrationstests

- **Maßnahmen**: Simulierte Cyberangriffe, um die Widerstandsfähigkeit der Netzwerke und Systeme zu prüfen.
- **Beispiel**: Ein Unternehmen beauftragt externe Sicherheitsfirmen, um seine Online-Plattform (E-Commerce) durch Penetrationstests auf Schwachstellen zu überprüfen.

8. Notfallpläne und Resilienzmaßnahmen

- **Maßnahmen**: Erarbeitung von Notfallplänen zur Sicherstellung der Geschäftskontinuität im Fall eines Angriffs / Vorfalls.
- **Beispiel**: Ein Wasserwirtschaftsunternehmen entwickelt einen Plan, der die Aufrechterhaltung der Wasserversorgung bei einem IT-Ausfall sicherstellt.

9. Regelmäßige Überprüfungen und Audits

- **Maßnahmen**: Interne und externe Audits zur Bewertung der Informationssicherheitsmaßnahmen durchführen.
- **Beispiel**: Ein Unternehmen beauftragt jährlich eine unabhängige Prüfung der Sicherheitsmaßnahmen, um Schwachstellen zu identifizieren.

10. Stärkung der Zugriffsrechte und -kontrollen

- **Maßnahmen**: Implementierung von Multi-Faktor-Authentifizierung (MFA) und strengen Zugriffsrechten für kritische Systeme, einschließlich Implementierung einer technischen Passwortrichtlinie (PWL).
- **Beispiel**: Ein Finanzdienstleister richtet MFA für alle internen Systeme ein, um den Zugriff durch unautorisierte Personen zu verhindern und implementiert eine PWL, die als Mindeststandard ein Passwort mit 14 Zeichen, inkl. Komplexität vorschreibt.

11. Datensicherung und Backups

- **Maßnahmen**: Regelmäßige Datensicherungen und Testwiederherstellungen zur Sicherstellung der Datenintegrität.
- **Beispiel**: Ein mittelständisches Produktionsunternehmen erstellt wöchentliche Backups aller kritischen Daten und testet vierteljährlich die Wiederherstellung, um die Funktionsfähigkeit sicherzustellen.

Für Unternehmen, die schon länger auch datenschutzrechtliche Maßnahmen umsetzen, ist der Aufwand reduziert. Einige Maßnahmen wurden schon aus Gründen des Datenschutzes umgesetzt und müssen nun – zumindest teilweise – vor dem Hintergrund der NIS-2-Vorgaben angepasst werden (z.B. Erweiterung bestehender Richtlinien/Prozesse, inkl. Maßnahmen).

4 Was bedeutet das für mein Unternehmen – wie gehe ich am besten vor?

Unternehmen, die den neuen Anforderungen unterliegen, müssen ihre bestehenden Informationssicherheitsmaßnahmen überdenken und gegebenenfalls verbessern. Dabei ist exemplarisch wie folgt vorzugehen:

1. Betroffenheit / Anwendungsbereich klären bzw. prüfen (siehe Link oben)

2. Ressourcen einplanen: Planen Sie Budget und personelle Ressourcen für die Umsetzung ein.

3. Verantwortlichkeit klären:

   - Bestimmen Sie eine Person im Unternehmen, die für die Umsetzung der Regelungen operativ (haupt-)verantwortlich ist.
   - Suchen Sie sich rechtzeitig kompetente Partner, die Sie bei der Umsetzung unterstützen.

4. Risikoanalyse und Lücken in Bezug auf NIS2 (Bestandsaufnahme der derzeitigen Sicherheitsmaßnahmen und Prozesse)

5. Maßnahmen ermitteln und umsetzen (Sicherstellung Geschäftskontinuität)

8. Kontinuierliche Überprüfung (Audits, Monitoring etc.)

Sollten Sie Fragen haben oder Unterstützung bei der Umsetzung in Teilbereichen zum Datenschutz benötigen, stehen wir Ihnen gerne zur Seite.

Ihre Datenschutzbeauftragten von der GDPC

Dr. Kevin Marschall und Stephan Blazy

GDPC GbR
Gesellschafter:
Dr. Kevin Marschall und Stephan Blazy
Ludwig-Erhard-Straße 12
34131 Kassel

Tel. 1: +49 (0)1575 200 80 35
Tel. 2: +49 (0)179 932 70 55
Mail: info@GDPC.de