



ATLANTIC Hotel Kiel

08.09.2025

Mit Sicherheit ein Datenschutzverstoß?

**Dr. h.c. Marit Hansen
Landesbeauftragte für Datenschutz
Schleswig-Holstein**



Unabhängiges Landeszentrum für
Datenschutz Schleswig-Holstein

Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA
4. Cybersicherheit UND Grundrechtsschutz
5. Wenn schon, denn schon

Mit Sicherheit ein Datenschutzverstoß?



Überblick

1. Sicherheit ... ist doch gut für Datenschutz

2. Ja, aber ...

3. Hilfe via NIS-2-RL und CRA

4. Cybersicherheit und Grundrechtsschutz

5. Wenn schon, denn schon

Hansen/Probst: Souveräne Sicherheit, Zero Trust und das Datenschutzrecht, DuD 10/2023, 623–628

1. Sicherheit ... ist doch gut für Datenschutz

Art. 5 DSGVO

- (1) (f) ... [Grundsatz „Integrität und Vertraulichkeit“] ...
- (2) Der Verantwortliche ist für die **Einhaltung** des Absatzes 1 verantwortlich und muss dessen Einhaltung **nachweisen können** („Rechenschaftspflicht“).

Art. 28 DSGVO

- (3) [...] Dieser Vertrag bzw. dieses andere Rechtsinstrument sieht insbesondere vor, dass der Auftragsverarbeiter [...]
 - h) dem Verantwortlichen alle erforderlichen Informationen **zum Nachweis** der **Einhaltung** der in diesem Artikel niedergelegten Pflichten zur Verfügung stellt und **Überprüfungen** — einschließlich Inspektionen —, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden, **ermöglicht und dazu beiträgt**.

Art. 24 DSGVO

- (1) Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um **sicherzustellen** und **den Nachweis dafür erbringen zu können**, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden **erforderlichenfalls überprüft und aktualisiert**.

Art. 32 DSGVO

- (1) [...] treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes **Schutzniveau zu gewährleisten**; diese Maßnahmen schließen gegebenenfalls unter anderem Folgendes ein:
 - [...]
 - b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und **Belastbarkeit** der Systeme und Dienste im Zusammenhang mit der Verarbeitung **auf Dauer sicherzustellen**; [...]
 - d) ein Verfahren zur **regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit** der technischen und organisatorischen Maßnahmen zur **Gewährleistung** der Sicherheit der Verarbeitung.

Art. 25 DSGVO

- (1) [...] trifft der Verantwortliche **sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete** technische und organisatorische Maßnahmen — wie z.B. Pseudonymisierung —, die **dafür ausgelegt** sind, die Datenschutzgrundsätze wie etwa Datenminimierung **wirksam umzusetzen** und die notwendigen **Garantien** in die Verarbeitung aufzunehmen, um den Anforderungen dieser Verordnung zu genügen und die Rechte der betroffenen Personen zu schützen.

Art. 35 DSGVO

- (7) Die Folgenabschätzung enthält zumindest Folgendes:
 - [...]
 - d) die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich **Garantien**, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten **sichergestellt** und der **Nachweis dafür erbracht** wird, dass diese Verordnung **eingehalten** wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Effektiv: wirksam bezüglich beabsichtigter Wirkung; etwaige Nebenwirkungen im Blick

Nachprüfbar: Möglichkeit aussagekräftiger Prüfungen der zugesicherten Eigenschaften und Wirkungen

Dauerhaft: jederzeit; auch zukünftig; resilient

Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA
4. Cybersicherheit UND Grundrechtsschutz
5. Wenn schon, denn schon

2. Ja, aber ...

Exkurs: Is the cure worse than the disease?

- Was, wenn **eine Sicherheitsmaßnahme selbst ein (Datenschutz-)Risiko** darstellt?
- Bei Verarbeitung personenbezogener Daten: DSGVO (+BDSG/LDSG usw.)
- Z.B. Protokollierung, Beschäftigtenüberwachung, Einsatz von Biometrie, Virensan



Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA
4. Cybersicherheit UND Grundrechtsschutz
5. Wenn schon, denn schon

3. Hilfe via NIS-2-RL und CRA

NIS-2-Richtlinie (demnächst in BSI-G)

Verpflichtet: Betreiber oder Anbieter von **kritischen Infrastrukturen**

Sicherheitspflichten:

- Registrierungspflicht (Meldestelle von BSI und BBK)
- Risikomanagement
- Meldepflicht

<https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32022L2555>

Cyber Resilience Act (Cyberresilienz-Verordnung)

Verpflichtet: Hersteller von Anbieter von **Produkten mit digitalen Elementen**

Sicherheitspflichten:

- Cybersicherheit by Design
- Pflicht zum nachhaltigen Schwachstellenmanagement inkl. Updates

https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L_202402847

Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA
4. Cybersicherheit UND Grundrechtsschutz
5. Wenn schon, denn schon

3. Hilfe via NIS-2-RL und CRA

Anhang I des CRA (Grundlegende Cybersicherheitsanforderungen), Teil 1

(1) Produkte mit digitalen Elementen werden so **konzipiert, entwickelt und hergestellt**, dass sie angesichts der Risiken ein angemessenes Cybersicherheitsniveau gewährleisten.

Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA
4. Cybersicherheit UND Grundrechtsschutz
5. Wenn schon, denn schon



CE-Kennzeichen

3. Hilfe via NIS-2-RL und CRA

Anhang I, Teil I Abs. 2 Buchst. e-h CRA

- (2) Auf der Grundlage der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend,
- [...]
- e) ... Vertraulichkeit ...
 - f) ... Integrität ...
 - g) ...
 - h) ... Verfügbarkeit ...
- [...]

Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA



CE-Kennzeichen

Art. 5 Abs. 1 Buchst. c DSGVO

- (1) Personenbezogene Daten müssen [...]
 - c) dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („Datenminimierung“)

3. Hilfe via NIS-2-RL und CRA

Anhang I, Teil I Abs. 2 **Buchst. g** CRA

- (2) Auf der Grundlage der Bewertung der Cybersicherheitsrisiken gemäß Artikel 13 Absatz 2 müssen Produkte mit digitalen Elementen, soweit zutreffend, [...]
 - g) die Verarbeitung personenbezogener oder sonstiger Daten auf solche, die angemessen und von Bedeutung sind, und auf das für die Zweckbestimmung des Produkts mit digitalen Elementen erforderliche Maß beschränken („Datenminimierung“)

Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA
4. Cybersicherheit UND Grundrechtsschutz
5. Wenn schon, denn schon

Icons: Manual Icons by srip sowie Ce Seal Icons, Document Icons, Product Icons und Source Code Icons by Freepik - Flaticon

3. Hilfe via NIS-2-RL und CRA



CE-Kennzeichen



Info für Nutzende



Technische Dokumentation



SBOM (Software Bill of Materials)

CRA:

- Basis: **Technische Dokumentation** des Herstellers
- ... über die ganze Lieferkette
- Für Rechenschaftspflicht des Verantwortlichen wertvoll

Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA
4. Cybersicherheit UND Grundrechtsschutz
5. Wenn schon, denn schon

4. Cybersicherheit UND Grundrechtsschutz

- **Sicherheit als Rechtspflicht** in der DSGVO
- Personenbezug: **keine Verarbeitung ohne Rechtsgrundlage!**
- Das gilt auch für TOMs, die personenbezogene Daten verarbeiten
- Rechtsgrundlagen (vgl. EG 121 NIS-2-RL):
 - Interessenabwägung: Art. 6 (1) **f** DSGVO
 - Erfüllung einer gesetzlichen Pflicht: Art. 6 (1) **c** DSGVO (i.V.m. ... z.B. Art. 32 DSGVO, Regelungen des BSIG-neu)
 - Wahrnehmung einer Aufgabe im öffentlichen Interesse: Art. 6 (1) **e** DSGVO
- Stets: **Erforderlichkeit, Verhältnismäßigkeit, ...**
TOM-TOMs (TOMs für die Cybersicherheits-TOMs):
 Weitergabebeschränkung, Verschlüsselung, Pseudonymisierung, Anonymisierung, ...
 (vgl. EG 121 NIS-2-RL)

Perspektive!

Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA
4. Cybersicherheit UND Grundrechtsschutz
5. Wenn schon, denn schon

https://www.datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf

4. Cybersicherheit UND Grundrechtsschutz

- Risiko im Datenschutz verschieden von Cybersicherheit
Perspektive: alle Grundrechte
- DS-Risikobewertung nichts Neues
- Cybersicherheits-TOMs können DSFA-Pflicht auslösen (vgl. „Muss-Liste“)

Perspektive!

Liste der Verarbeitungstätigkeiten, für die eine DSFA durchzuführen ist			
Nr.	Maßgebliche Beschreibung der Verarbeitungstätigkeit	Typische Einsatzfelder	Beispiele
1	Verarbeitung von biometrischen Daten zur eindeutigen Identifizierung natürlicher Personen, wenn mindestens ein weiteres folgendes Kriterium aus WP 248 Rev. 01 zutrifft: • Daten zu schutzbedürftigen Betroffenen • Systematische Überwachung • Innovative Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen	Verwendung von biometrischen Systemen zur Zutrittskontrolle oder für Abrechnungszwecke.	Ein Unternehmen setzt flächendeckend Fingerabdrucksensoren zur Zutrittskontrolle für bestimmte Bereiche ein. Eine Schulkantine bietet den Schülern das „Bezahlen per Fingerabdruck“ an.

8	Umfangreiche Verarbeitung von personenbezogenen Daten über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese Betroffenen in anderer Weise erheblich beeinträchtigt werden	Einsatz von Data-Loss-Prevention Systemen, die systematische Profile der Mitarbeiter erzeugen
---	--	---

Überblick

1. Sicherheit ... ist doch gut für Datenschutz
2. Ja, aber ...
3. Hilfe via NIS-2-RL und CRA
4. Cybersicherheit UND Grundrechtsschutz
5. Wenn schon, denn schon

5. Wenn schon, denn schon

- Wenn schon „Cybersicherheit by Design“ ...
- ... dann erst recht Art. 25 DSGVO – „Datenschutz by Design“

