

Digital Omnibus

Erfolgreiche Verschlankung oder weitere Aufblähung der Europäischen Gesetzgebung?

Charlotte Berg LL.M. (Columbia University)

Lisa Grochala

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Herbstakademie 2026

Agenda

- ▶ EU Gesetzgebung im Digitalbereich (Better-Regulation Agenda & Omnibus-Technik)
- ▶ Digital Omnibus: Änderungen im Daten- und Cybersicherheitsrecht
 - ▶ Inhalt
 - ▶ Stand der Verhandlungen, Zeitplan
 - ▶ Einführung einer EU-weiten zentralen Anlaufstelle (Single-Entry-Point)
- ▶ Der Single Entry Point im „Praxistest“: Berichtspflichten nach Art. 23 NIS-2 RL vs. Art. 14 Abs. 3 CRA
- ▶ Bewertung: Verschlinkung vs. weitere Aufblähung

Better Regulation Agenda & Omnibus-Technik

EU-GESETZGEBUNG IM DIGITALBEREICH

Better Regulation Agenda

- ▶ LP 2024 – 2029
 - ▶ Ziel: „simpler, lighter, faster“ regulation
- ▶ Einfacheres, wirksameres, effizienteres und kohärenteres Regelungsumfeld
- ▶ Effektiver Rechtsverkehr in der EU
- ▶ Mehr Rechtssicherheit
- ▶ Senkung bürokratischer Hürden
- ▶ Anreize für Investitionen & stärkere Wettbewerbsfähigkeit
- ▶ Förderung der EU-Grundwerte weltweit

Omnibus-Rechtsakte

- ▶ Neues Instrument auf EU-Ebene
 - ▶ Vergleichbar mit dem deutschen Artikelgesetz
- ▶ Bündelung punktueller Änderungen verschiedener Rechtsakte in einem einzigen Legislativvorschlag
- ▶ Fokus: Entbürokratisierung und Stärkung der Wettbewerbsfähigkeit der EU
- ▶ Im Digitalbereich: „Digital Omnibus“ und „Digital Omnibus on AI“

Änderungen im Daten- und Cybersicherheitsrecht

DIGITAL OMNIBUS

Zeitplan & Kurzübersicht

- ▶ Veröffentlichung des EU-Kommissionsvorschlags am 19.11.2025; Verhandlungen im Rat und im EP dauern an
- ▶ Inkrafttreten ist noch nicht abschätzbar
- ▶ Änderungen bei einer Vielzahl von Digitalrechtsakten
 - ▶ NIS-2 RL, DSG-VO, CER-RL, DORA, eIDAS-VO, Data Act, ePrivacy RL, Single Gateway Verordnung

Inhalt

- ▶ Data Act
 - ▶ Anpassung der Regelungen zum Schutz von Geschäftsgeheimnissen
 - ▶ Anpassung der Vorgaben zur Herausgabe von Daten an öffentliche Stellen (B2G)
 - ▶ Anpassung der Regelungen im Bereich des Cloud Switching
- ▶ DSGVO
 - ▶ Anpassung des Begriffs personenbezogene Daten
 - ▶ Vorgaben für die Entwicklung und das Training von KI
 - ▶ Anpassung der Informationspflichten
- ▶ Schaffung eines Single Entry Points zur Vorfallsmeldung

Berichtspflichten nach Art. 23 NIS-2 RL vs. Art. 14 Abs. 3 CRA

DER SINGLE-ENTRY POINT IM „PRAXISTEST“

Idee: Report Once, Share Many

- ▶ „One-Stop-Shop“
 - ▶ Aktuell zersplitterte Meldeverpflichtungen
 - ▶ Betroffene sollen meldepflichtige Vorfälle schnell und unkompliziert an die zuständige Aufsichtsbehörde melden können.
- ▶ Entlastung der Betroffenen, besonders KMU
- ▶ Potentiell Erhöhung des Meldeaufkommens
- ▶ Schnellere Eingriffsmöglichkeiten der Aufsichtsbehörden
- ▶ Bessere Zusammenarbeit bei grenzüberschreitenden Vorfällen

Umsetzung

- ▶ Einrichtung bei der ENISA vorgesehen
- ▶ ENISA als reine Eingangsstelle der Meldungen
 - ▶ Keine eigenen Aufsichtspflichten
 - ▶ Kein Zugriff auf Meldungen/Daten
 - ▶ Aufbau auf der einheitlichen Meldeplattform nach Art. 14 CRA
- ▶ Bündelung der Meldepflichten nach dem CRA, NIS-2-RL, DSG-VO, DORA, eIDAS-VO und CER-RL
- ▶ Verpflichtung zur Nutzung der zentralen Anlaufstelle

Praxistauglichkeit

- ▶ Zusammenfassung der einzelnen Meldepflichten ist **nicht** vorgesehen.
 - ▶ Inhaltliche Anforderungen der einzelnen Meldepflichten müssen weiterhin erfüllt werden
- ▶ Ausnahme: Art. 23 Abs. 12 NIS-2 RL-E
 - ▶ Meldungen nach Art. 14 Abs. 3 CRA und Art. 23 Abs. 1 NIS-2 RL sollen in Zukunft gebündelt möglich sein.

Norm

Art. 23 Abs. 12 NIS-2 RL (Vorschlag nach Art. 6 Nr. 2 lit b) Digital Omnibus)

Meldet ein Hersteller einen **schwerwiegenden Sicherheitsvorfall** gemäß Artikel 14 Absatz 3 CRA und enthält die Meldung des Sicherheitsvorfalls nach dem genannten Artikel **einschlägige Informationen** gemäß Absatz 4 des vorliegenden Artikels [*erg. Meldepflicht von erheblichen Sicherheitsvorfällen nach NIS-2 RL*], so gilt die Meldung des Herstellers nach Art. 14 Abs. 3 CRA auch als Meldung nach Artikel 23 Abs. 4 NIS-2 RL. [*redaktionelle Anpassungen vorgenommen*]

- Anknüpfungspunkt: Übermittlung einschlägiger Vorschriften
- Keine Widersprüche
- Keine Schutzlücken
- Praxistauglichkeit

Praxistauglichkeit?

	Art. 14 CRA	Art. 23 NIS-2 RL
Adressaten	Hersteller von Produkten mit digitalen Elementen	Wesentliche und wichtige Einrichtungen
Auslöser	„schwerwiegender“ Sicherheitsvorfall	„erheblicher“ Sicherheitsvorfall
Fristen	• Frühwarnung: 24 • Erste Bewertung: 72	• Frühwarnung: 24 • Erste Bewertung: 72
Inhalte	• Verursachung des Vorfalls durch rechtswidrige oder böswillige Handlungen (24 Stunden) • Grenzüberschreitende Auswirkungen (24 Stunden) • Allgemeine Informationen über die Art des Vorfalls, erste Bewertung und ergriffene Abhilfemaßnahmen, ggf. Sensibilität der Informationen (72 Stunden)	• Verursachung des Vorfalls durch rechtswidrige oder böswillige Handlungen (24 Stunden) • Grenzüberschreitende Auswirkungen (24 Stunden) • Aktualisierung der Frühmeldung (72 Stunden) • Erste Bewertung, einschließlich Schweregrad und Auswirkungen, ggf. Kompromittierungsindikatoren (72 Stunden)

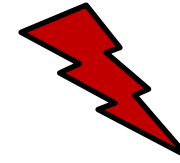
Nicht ohne Weiteres!



Hersteller einer industriellen
Steuerungsplattform



Einsatz



Wesentliche
Einrichtungen

Verschlankung vs. weitere Aufblähung

BEWERTUNG

Bewertung

- ▶ Begrüßenswerte Idee
- ▶ Prüfungsaufwand wird in der Praxis kaum verringert
- ▶ Bündelung der Meldepflicht nach Art. 14 Abs. 3 CRA und Art. 23 Abs. 1 NIS-2 RL dürfte kaum eine praktische Anwendbarkeit haben
- ▶ Gefahr eines Single Point of Failure
 - ▶ Gefahr des Zugriffs auf große Menge sensibler Daten durch feindliche Angreifer
 - ▶ Mitgliedstaaten müssen als Back-Up eigene Meldestrukturen weiterhin vorhalten

Charlotte Berg, LL.M (Columbia University)

Lisa Grochala

Exzellenzzentrum IT-Sicherheitsrecht: cybersicherheitsrecht@bsi.bund.de

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT