

Der Risikobegriff der Datenschutz- Grundverordnung

Cybersicherheitstag Niedersachsen 2018

22.10.2018

Rasmus Robrahn

rasmus.robrahn@lfd.niedersachsen.de



Agenda

- Datenschutz-Grundverordnung kurz vorgestellt
- Risiko als zentraler Begriff
- Angemessene technisch-organisatorische Maßnahmen
- Informationssicherheit und Datenschutz

Datenschutz-Grundverordnung kurz vorgestellt

■ Anwendbar seit dem 25. Mai 2018

■ Ziele:

- Vereinheitlichung des Datenschutzrechts in Europa
- Modernisierung des Datenschutzrechts
- Effektive Bußgelder
- „Diese Verordnung schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten“

Risiko als zentraler Begriff

- Verantwortung des für die Verarbeitung Verantwortlichen
- Datenschutz durch Technikgestaltung
- Sicherheit der Verarbeitung
- Umgang mit Meldungen von Datenschutzverletzungen
- Datenschutz-Folgenabschätzung und vorherige Konsultation

Risiko als zentraler Begriff

- „Risiken für Rechte und Freiheiten natürlicher Personen“
 - Es geht nicht um Reputationsrisiken oder Bußgeldrisiken für den Verantwortlichen
 - Was bedeutet ein Schaden für die betroffene Person?
 - Beispiele für Schäden (EG 75):
 - Diskriminierung
 - Identitätsdiebstahl
 - Finanzieller Verlust
 - Rufschädigung
 - Gesellschaftliche Nachteil
 - Kontrollverlust über personenbezogene Daten
 - Unbefugte Aufhebung einer Pseudonymisierung

Angemessene technisch-organisatorische Maßnahmen

■ Art. 24, 25 und 32 DSGVO

■ Ziel der Normen: angemessene technisch-organisatorische Maßnahmen zum Schutz der betroffenen Personen

■ Abwägung

- Schwere und Eintrittswahrscheinlichkeiten von Risiken
- Kosten der Implementierung
- Stand der Technik

Angemessene technische und organisatorische Maßnahmen

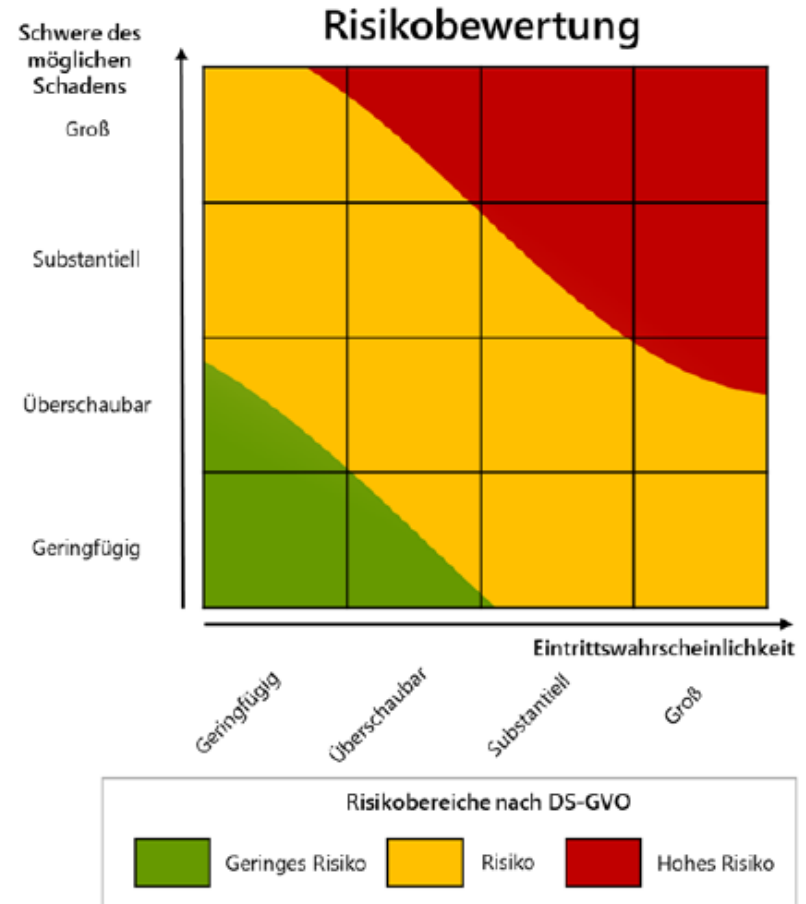
Risikoidentifikation

- Welche Schäden?
- Wodurch?

Bestimmung von Eintrittswahrscheinlichkeit und Schwere

- Bildung von Stufen und entsprechende Einstufung

Zuordnung zu Risikoabstufungen



■ Art. 32 DSGVO: Sicherheit der Verarbeitung

- Vertraulichkeit, Integrität und Verfügbarkeit
- Aber Angemessenheit der Maßnahmen ist in Hinblick auf den Schutz von betroffenen Personen zu gewährleisten

■ Datenschutzspezifische Gewährleistungsziele

- Datensparsamkeit, Nichtverkettung, Transparenz, Intervenierbarkeit

- Kurzpapier Nr. 18 – Risiko für die Rechte und Freiheiten natürlicher Personen
- WP 248 – Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 „wahrscheinlich ein hohes Risiko mit sich bringt“