cyberlegal

Auswirkungen der EU-DSGVO auf die IT in Unternehmen

RA Robert Niedermeier
CIPP/E CIPT CIPM FIP

cyberlegal

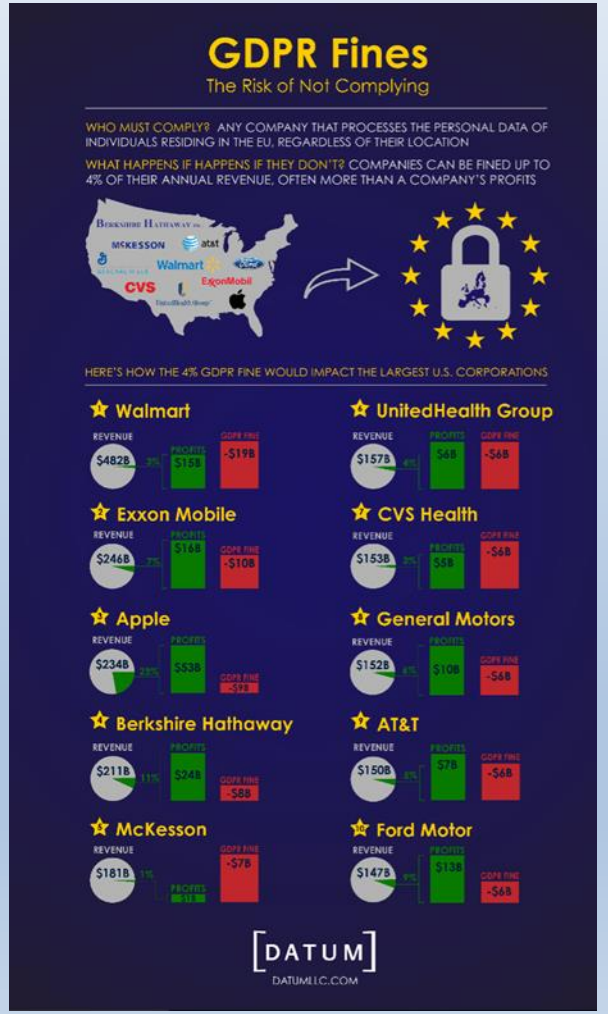
Agenda

- Intro:
  - Worum geht`s?
  - verschärfter Sanktionsrahmen
  - Bußgelder
  - EU-DSGVO
- Zentrale Säule: Risikobasierter Ansatz der DS-GVO
  - Vorherige Regelungen (DSG 2000)
  - Datenschutz und Datensicherheit
  - Von „systemisch“ zu „faktisch“
  - Art. 32 DS-GVO
  - Änderungen
  - Schutzvorkehrungen nach der EU-DSGVO
- Was heißt das nun für mich?
  - Sicherheitsarchitektur
  - Grundeinstellungen
  - Verschlüsselungsgrad
  - Zugriffsrechte
  - Risiko- und Notfallmanagement…

cyberlegal

Intro

Worum geht`s?



Verschärfter Sanktionsrahmen

Im Rahmen der EU-DSGVO ist der Strafrahmen deutlich erweitert worden:

Verstöße gegen Pflichten der verantwortlichen Stelle bzw. des Auftragnehmers sind nach Art. 83 Abs. 4 lit. a der EU-DSGVO mit **Geldbußen von bis zu 10 Mio. € bzw. von bis zu 2 % des weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres fällig. Das betrifft u.a.:

- Missachtung von Privacy by Design / Default (Art. 25)
- Nichteinhaltung von Auflagen zur Auftragsdatenverarbeitung (Art. 28)
- Unvollständiges Verzeichnis von Verarbeitungstätigkeiten (Art. 30)
- Unzureichende Maßnahmen zur Sicherheit der Verarbeitung (Art. 32)
- Unzureichende Meldungen von Verletzungen des Schutzes personenbezogener Daten (Art. 33 + 34)
- Unzureichende Datenschutz-Folgenabschätzung (Art. 35)
- Nichtbenennung eines Datenschutzbeauftragten (Art. 37 bis 39)
- Fehlerhafte Zertifizierungen (Art.42+43)

→ Unzureichender technischer Datenschutz strafbewährt!

Bußgelder

Im Rahmen der EU-DSGVO ist der Strafrahmen deutlich erweitert worden:

Folgende Verstöße sind nach Art. 83 Abs. 5 der EU-DSGVO mit **Geldbußen von bis zu 20 Mio. € bzw. von bis zu 4 % des weltweit erzielten Jahresumsatzes** des vorangegangenen Geschäftsjahres fällig:

- **Verstöße gegen die Grundsätze für die Verarbeitung** (einschließlich der Bedingungen für die Einwilligung!) nach Art. 5, 6, 7 & 9 (also auch einer unzureichenden Handhabung von besonderen Kategorien personenbezogener Daten)
- **Verstöße gegen die Betroffenenrechte** nach Art. 12 bis 22
- **Unzulässige Übermittlung von Daten in Drittstaaten** nach Art. 44 bis 49
- Nichteinhaltung der Vorschriften für besondere Verarbeitungssituationen nach Art. 85 bis 91 gemäß den Rechtsvorschriften der Mitgliedsstaaten
- Behinderung der Aufsichtsbehörden

→ **Unzureichende Rechtmäßigkeit der Verarbeitung strafbewährt!**

→ Gleiches gilt für die Nichtbefolgung von Anweisungen der Aufsichtsbehörde

EU-DSGVO

- Ziel: europaweite Vereinheitlichung des Datenschutzes
- gilt als Verordnung in jedem Mitgliedsstaat unmittelbar
- Prinzipien:
  - Marktort-Prinzip
  - One-Stop-Shop
- Massiv erhöhte Bußgelder
- Vorgaben für vertragliche Vereinbarungen zw. Verantwortlichem und Auftragsverarbeiter
- Regelungen zur Übermittlung an Drittstaaten
- Möglichkeit d. Mitgliedsstaaten Verbandsklagen zuzulassen (in Deutschland bereits umgesetzt)
- Abrufbar in allen EU-Sprachen unter: http://eur-lex.europa.eu/legal-content/de/TXT/?uri=CELEX%3A32016R0679

cyberlegal

zentrale Säule: risikobasierter Ansatz

Vorherige Regelung

§ 14 DSG 2000

- Organisationskontrolle
  (DSB/ Datengeheimnis/Aufsichtsbehörde **/ …**)
- Technisch- organisatorische Maßnahmen (TOMs) beim Umgang mit personenbezogenen Daten
- Systemischer Datenschutz des DSG 2000
- Datenschutzseitige Zuverlässigkeit in § 11 DSG 2000
- „……“

cyberlegal

zentrale Säule: risikobasierter Ansatz

Datenschutz und Datensicherheit

Grundlagen des Datenschutzes		Grundlagen der IT-Sicherheit	
	Geschichte des Datenschutzes		Anforderungen zur IT-Sicherheit
	Datenschutzrechtliche Prinzipien		Mehrseitige IT-Sicherheit
	Technischer Datenschutz		Risiko-Management
	Kundendatenschutz		Konzeption von IT-Sicherheit

- Begriffsklärung: Daten, personen-bezogene Daten & Informationen, Sicherheit, Datensicherung, Datensicherheit
- technische & organisatorische Maß-nahmen (nach DSG 2000 & EU-DSGVO), Datenschutzkonzept
- Standard-Datenschutzmodell
- Risikobasierter Ansatz im Datenschutzrecht

- Vorabkontrolle zu Datenschutzrisiken
- Bestimmung von Datenschutzrisiken
- Datenschutz-Folgenabschätzung nach der EU-DSGVO
- Privacy Impact Assessment
- Datenschutzrisiken bei der Auftragsdatenverarbeitung
- Datenschutzfördernde Techniken
- Privacy by Design / Default

cyberlegal

Datenschutz und Datensicherheit

Von „systemisch“ zu „faktisch“

Artikel 4

►M2 Sicherheit der Verarbeitung ◄

(1) Der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes muss geeignete technische und organisatorische Maßnahmen ergreifen, um die Sicherheit seiner Dienste zu gewährleisten; die Netzsicherheit ist hierbei erforderlichenfalls zusammen mit dem Betreiber des öffentlichen Kommunikationsnetzes zu gewährleisten. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der Kosten ihrer Durchführung ein Sicherheitsniveau gewährleisten, das angesichts des bestehenden Risikos angemessen ist.

cyberlegal

zentrale Säule: risikobasierter Ansatz

Art. 32 DS-GVO

Sicherheit der Verarbeitung

(1)Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten; diese Maßnahmen schließen unter anderem Folgendes ein:

a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten; 4.5.2016 L 119/51 Amtsblatt der Europäischen Union DE

b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;

c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

d) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

(2)Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung verbunden sind, insbesondere durch — ob unbeabsichtigt oder unrechtmäßig — Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.

(3)Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 oder eines genehmigten Zertifizierungsverfahrens gemäß Artikel 42 kann als Faktor herangezogen werden, um die Erfüllung der in Absatz 1 des vorliegenden Artikels genannten Anforderungen nachzuweisen.

(4)Der Verantwortliche und der Auftragsverarbeiter unternehmen Schritte, um sicherzustellen, dass ihnen unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur auf Anweisung des Verantwortlichen verarbeiten, es sei denn, sie sind nach dem Recht der Union oder der Mitgliedstaaten zur Verarbeitung verpflichtet.

cyberlegal

zentrale Säule: risikobasierter Ansatz

Art. 32 DS-GVO

Erwägungsgründe:

"(66) Zur Aufrechterhaltung der Sicherheit und zur Vorbeugung gegen eine gegen diese Verordnung verstoßende Verarbeitung sollte der für die Verarbeitung Verantwortliche oder der Auftragsverarbeiter die mit der Verarbeitung verbundenen Risiken ermitteln und Maßnahmen zu deren Eindämmung ergreifen. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der dabei anfallenden Kosten ein Schutzniveau gewährleisten, das den von der Verarbeitung ausgehenden Risiken und der Art der zu schützenden personenbezogenen Daten angemessen ist. Die Kommission sollte bei der Festlegung technischer Standards und organisatorischer Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung die technologische Neutralität, die Interoperabilität sowie Innovationen fördern und gegebenenfalls mit Drittländern zusammenarbeiten."

cyberlegal

zentrale Säule: risikobasierter Ansatz

Änderungen

Art. 32 DS-GVO	§ 14 DSG 2000
Art. 32 Abs. 1 lit. a: Pseudonymisierung personenbezogener Daten	-/-
Art. 32 Abs. 1 lit. a: Verschlüsselung personenbezogener Daten	-/-
Art. 32 Abs. 1 lit. b: ... Vertraulichkeit, ... im Zusammenhang mit der Verarbeitung auf Dauer sicher-zustellen	• Zutrittskontrolle • Zugangskontrolle • Zugriffskontrolle • Weitergabekontrolle • Auftragskontrolle • Zweckbindung

cyberlegal

zentrale Säule: risikobasierter Ansatz

Änderungen

Art. 32 DS-GVO	§ 14 DSG 2000
Art. 32 Abs. 1 lit. b: ... Integrität, ... im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	• Eingabekontrolle • Auftragskontrolle
Art. 32 Abs. 1 lit. b: ... Verfügbarkeit ... im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	• Verfügbarkeitskontrolle
Art. 32 Abs. 1 lit. b: ... Belastbarkeit ... im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen	-/-
Art. 32 Abs. 1 lit. c: Beschreibung des Verfahrens zur Gewährleistung den Zugang zu den personenbezogenen Daten bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen	-/-

zentrale Säule: risikobasierter Ansatz

Änderungen

Art. 32 DS-GVO	§ 14 DSG 2000
Art. 32 Abs. 1 lit. d: Beschreibung der Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung	-/-

zentrale Säule: risikobasierter Ansatz

Schutzvorkehrungen nach der EU-DS-GVO

Nach Art. 32 Abs. 1 der EU-DSGVO gilt, dass **geeignete** technische und organisatorische Maßnahmen zu treffen sind unter Berücksichtigung von

- Stand der Technik
- Implementierungskosten
- Art, Umfang, Umstände & Zwecke der Verarbeitung
- sowie unterschiedliche Eintrittswahrscheinlichkeit & Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Dabei ist ein **dem Risiko angemessenes Schutzniveau** zu gewährleisten.

Die Maßnahmen sind nach Art. 24 Abs. 1 erforderlichenfalls zu **überprüfen und aktualisieren.**

cyberlegal

zentrale Säule: risikobasierter Ansatz

Schutzvorkehrungen nach der EU-DS-GVO

Zu treffende Maßnahmen schließen u.a. Folgendes ein (nach Art. 32 Abs. 1):

- **Pseudonymisierung und Verschlüsselung** personenbezogener Daten
- Fähigkeit zur **Sicherstellung von**
- **Vertraulichkeit**
- **Integrität**
- **Verfügbarkeit**
- **Belastbarkeit**

der Systeme & Dienste im Zusammenhang mit der Verarbeitung auf Dauer.

Fähigkeit zur **raschen (!) Wiederherstellung**

- der Verfügbarkeit personenbezogener Daten
- und des Zugangs zu diesen Daten
- **bei** einem physischen oder technischen **Zwischenfall**
- Verfahren zur regelmäßigen **Überprüfung, Bewertung & Evaluierung**
- **der Wirksamkeit dieser Maßnahmen**

cyberlegal

zentrale Säule: risikobasierter Ansatz

Schutzvorkehrungen nach der EU-DS-GVO

Nach Art. 32 Abs. 2 der EU-DSGVO sind bei der Beurteilung des angemessenen Schutzniveaus **insbesondere die Risiken** zu berücksichtigen, die **mit der Verarbeitung verbunden** sind; insbesondere hinsichtlich

- Vernichtung bzw. Verlust (ob unbeabsichtigt oder unrechtmäßig)
- Veränderung (ob unbeabsichtigt oder unrechtmäßig)
- unbefugte Offenbarung von bzw. unbefugter Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet werden

Genehmigte Verhaltensregeln (nach Art. 40) oder genehmigte Zertifizierungsverfahren (nach Art. 42) können nach Art. 32 Abs. 3 als **Nachweis für die Erfüllung der Anforderungen** herangezogen werden.

Ausführende Personen, die Zugang zu personenbezogenen Daten haben, dürfen diese Daten nach Art. 32 Abs. 4 nur auf Anweisung der verantwortlichen Stelle verarbeiten, sofern sie nicht durch geltendes Recht zur Verarbeitung verpflichtet sind.

zentrale Säule: risikobasierter Ansatz

Einheitliche Gewährleistungsziele

Am 1. Oktober 2015 haben die deutschen Aufsichtsbehörden zum Datenschutz ein Konzept zur Datenschutzberatung und -prüfung auf der Basis **einheitlicher Gewährleistungsziele** verabschiedet. Danach sind folgende Gewährleistungsziele zu verfolgen (unter Angabe von zugehörigen Maßnahmen):

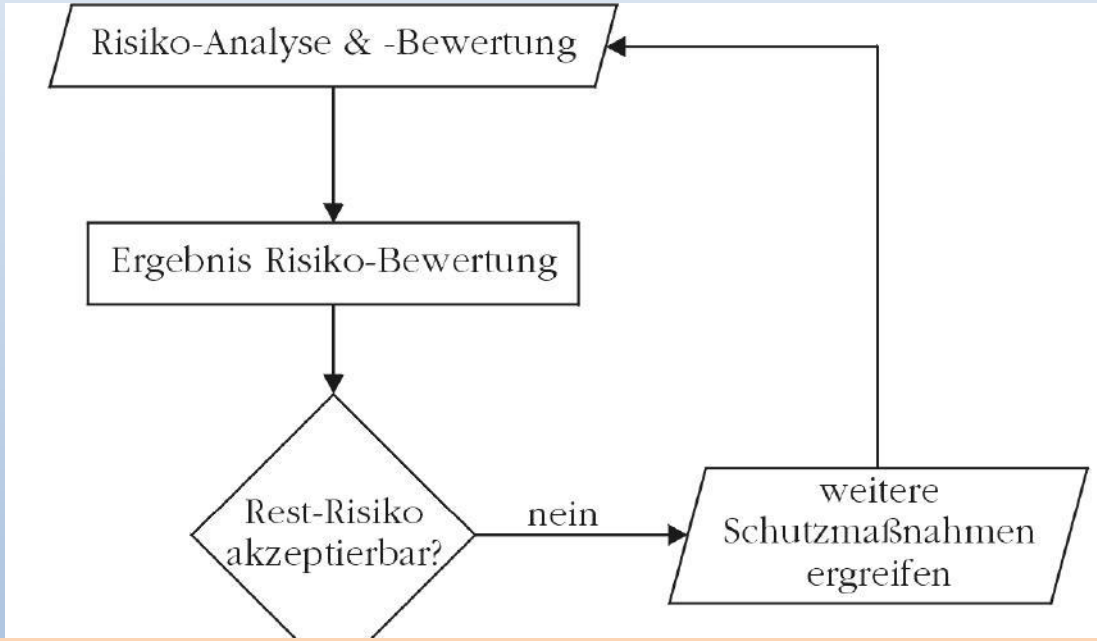
- Datensparsamkeit (grundlegend übergeordnet)
- Verfügbarkeit
- Integrität
- Vertraulichkeit
- Nichtverletzbarkeit
- Transparenz
- Intervenierbarkeit

Die grünen Gewährleistungsziele zählen zu den „klassischen“ Gewährleistungszielen der Datensicherheit, die blauen Gewährleistungsziele sind dagegen am Schutzbedarf von Betroffenen ausgerichtet.

(siehe:https://www.bfdi.bund.de/DE/Datenschutz/Themen/Technische_Anwendungen/TechnischeAnwendungenArtikel/Standard-Datenschutzmodell.html)

zentrale Säule: risikobasierter Ansatz

Schutzmaßnahmen und Datenschutzkonzept



Dokumentation fehlt, insbesondere wenn eine Verarbeitung trotz Risiko durchgeführt wird.

Summe ergriffener Schutzmaßnahmen = Datenschutzkonzept

Was heißt das nun für mich?

Allgemein

- erhöhter gesetzlicher Dokumentationszwang
- Interne Audits Evaluation
- „Sign Off“ Verfahren
- Neu-Zertifizierungen/Audits nötig
- Risikobewertungen
- Beschaffung von Hardware und Software möglichst mit Zertifizierung
- Verschlüsselung
- …….

cyberlegal

Was heißt das nun für mich?

Sicherheitsarchitektur

- Strikte Trennung der Kunden auf allen Ebenen
- Sicherheit des eigenen Rechenzentrums und der eigenen IT-Systeme
- Maßnahmen gegen Missbrauch der Ressourcen

Überprüfung

- Sind alle Voreinstellungen auf dem aktuellen Stand der Technik?
- Ist der Verschlüsselungsgrad auf dem aktuellen Stand der Technik?
- Sind die Zugriffsrechte noch aktuell und entsprechen den tatsächlich notwendigen Zugriffsmöglichkeiten?
- Ist das Risiko- und Notfallmanagement funktionsfähig?

cyberlegal

Was heißt das nun für mich?

Grundeinstellungen

- Privacy-by-design
- Privacy-by-default

-> Programme und Systeme müssen schon Datenschutzkonform erstellt und konzipiert sein (zB Zero-Knowledge-Prinzip)

- Einsatz zertifizierter Produkte verringert die Haftung
  - Datenschutz-Gütesiegel
  - EuroPriSe

cyberlegal

Bei Fragen:

RA Robert Niedermeier +49 171 2440099 oder mail@legislator.de

Quellen:

Grundlagen des Datenschutzes, Vorlesung im Sommersemester 2016 an der Universität Ulm von Bernhard C. Witt

Das neue Datenschutzrecht in der betrieblichen Praxis, Laue & Philip

EU-Datenschutz-Grundverordnung im Unternehmen: Praxisleitfaden (Kommunikation & Recht), Wybitul, Tim