Umsetzung der DSGVO

Handlungsbedarf aus technisch-organisatorischer Sicht

Ingrid Schaumüller-Bichl
Information Security Compliance Center (ISCC)
FH Oberösterreich
iscc@fh-ooe.at

Inhalte

- Motivation
- Sicherheit der Verarbeitung
- Gütesiegel, Zertifizierungen und Codes of Conduct
- Verzeichnis von Verarbeitungstätigkeiten
- Integration von Datenschutzanforderungen in die Prozesse der Institution
- Data Protection by Design und by Default
- Datenschutz-Folgenabschätzung

Motivation

- Datenschutz braucht nicht nur rechtliche Vorgaben,
  sondern auch praktische Maßnahmen zur Gewährleistung des Schutzes der personenbezogenen Daten

- Dazu braucht es einen Mix aus organisatorischen, personellen, baulichen und (IT-)technischen Maßnahmen.
  „Technische und/oder organisatorische Maßnahmen“, TOMs

- Schon bisher (DSG 2000): Forderung nach risikogerechten, angemessenen Maßnahmen; Stand der Technik

- Die EU DSGVO stellt noch höhere Anforderungen an die technische und organisatorische Sicherheit als das DSG 2000:
  - erhöhte Selbstverantwortung der Unternehmen:
    weniger Meldepflichten, Vorabkontrollen, Genehmigungen;
    dafür mehr Dokumentationspflichten, Nachweise bei Anforderungen
  - mehr Informationspflichten (Info an Betroffene, Data Breach Notification)
  - verstärktes Augenmerk auf Informationssicherheit / technische Lösungen (TOMs, PETs,…)
  - vermehrter Einsatz von Zertifizierungen und Gütesiegeln
  - Datenschutz als integraler Bestandteil von Verarbeitungen (Data Protection by Design und by Default)
  - deutlich höhere Geldbußen (bis zu 20 Mio € oder 4% des Konzernumsatzes)

Sicherheit der Verarbeitung (Artikel 32)

Artikel 32(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 („including inter alia as appropriate“):

a) die **Pseudonymisierung und Verschlüsselung** personenbezogener Daten;
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.

ISCC Information Security Compliance Center der fhoö

Sicherheit der Verarbeitung cont'd

- Wichtige Anforderungen
  - erweiterte Schutzziele: Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit
  - Schutz von Systemen, Applikationen und Daten!
  - angemessenes Schutzniveau
  - risikobasierte Maßnahmen
  - regelmäßige Überprüfung und Bewertung der Wirksamkeit
  - verstärkt Zertifizierungen und Gütesiegel

- ISMS ist nicht explizit gefordert, aber in der Praxis sehr hilfreich
  z.B. nach ISO/IEC 27001

ISCC Information Security Compliance Center der fhoö

Zertifizierung (Artikel 42, 43)

- Die Mitgliedsstaaten und die EU-Kommission fördern den Einsatz von datenschutzspezifischen Zertifizierungen und Datenschutzsiegeln.
- Eine Zertifizierung muss immer freiwillig und transparent sein.
- Aufsichtsbehörden erstellen eine Liste der möglichen Zertifizierungsschemata (Vorschlag für Guidelines der WP 29 voraussichtlich im Februar 2018)

- Achtung: Zertifizierung stellt keinen „Freibrief“ dar, Verantwortung bleibt

  `Eine Zertifizierung gemäß diesem Artikel mindert nicht die Verantwortung des Verantwortlichen oder des Auftragsverarbeiters für die Einhaltung dieser Verordnung …`

  aber: bei Bemessung von Geldbußen „gebührend zu berücksichtigen“ (Artikel 83 (2j))

Verhaltensregeln (Codes of Conduct)

(Artikel 40, 41)

- Ausarbeitung von Verhaltensregeln für einzelne Verarbeitungsbereiche
- durch Berufsverbände, Interessensvertretungen, …(z.B. WKO)
- Präzisierungen für branchen- oder berufsspezifische Verarbeitungen
- Vorlage bei der Aufsichtsbehörde, Genehmigung erforderlich; national oder EU-weit

Inhalte: Präzisierung der Anwendung der DSGVO z.B. in folgenden Bereichen

- berechtigte Interessen des Verantwortlichen in bestimmten Zusammenhängen
- Erhebung personenbezogener Daten
- Unterrichtung der Öffentlichkeit und der betroffenen Personen
- die Maßnahmen und Verfahren zu Privacy by Design und Privacy by Default
- Maßnahmen für die Sicherheit der Verarbeitung gemäß Artikel 32
- Übermittlung personenbezogener Daten an Drittländer oder an internationale Organisationen

Verzeichnis von Verarbeitungstätigkeiten (Artikel 30)

› Meldepflicht gemäß § 17 DSG 2000 idgF (DVR) fällt weg, dafür muss jeder Verantwortliche und Auftragsverarbeiter (**und** ggfs. deren Vertreter) ein **Verzeichnis aller Verarbeitungstätigkeiten** führen.

Gilt NICHT für: Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen und folgende drei Bedingungen erfüllen (Artikel 30 (5)):

- die vorgenommene Verarbeitung stellt kein Risiko für Rechte und Freiheiten der Betroffenen dar,
- die Verarbeitung erfolgt nur gelegentlich (Achtung – Übersetzungsfehler in deutscher Ausgabe der DSGVO, Corrigendum)
- die Verarbeitung schließt keine personenbezogenen Daten besonderer Kategorien bzw. Daten über strafrechtliche Verurteilungen und Straftaten ein

› Das „Verzeichnis von Verarbeitungstätigkeiten" …

- ist ab dem 25. Mai 2018 zu führen,
- ist schriftlich zu führen (auch in elektronischem Format möglich),
- muss nicht öffentlich für jedermann zugänglich sein,
- ist auf Anfrage der Aufsichtsbehörde zur Verfügung zu stellen.

Inhalt des Verzeichnisses (Artikel 30 (1))

Verantwortliche

- Name und Kontaktdaten
  - des Verantwortlichen
  - ggfs. Name und Kontaktdaten des mit ihm gemeinsam Verantwortlichen
  - ggfs. Vertreter des Verantwortlichen
  - ggfs. Datenschutzbeauftragte
- Zweck der Verarbeitung
- Beschreibung
  - der Kategorien betroffener Personen
  - der Kategorien personenbezogener Daten
- Kategorien von Empfängern
  - denen personenbezogenen Daten offengelegt wurden oder noch werden (Zugriffsberechtigungen)
  - dazu gehören auch Empfänger in Drittländern oder internationalen Organisationen

Inhalt des Verzeichnisses (Artikel 30 (1))

cont'd

Verantwortliche

- ggfs. Übermittlungen von personenbezogenen Daten
  - an ein Drittland oder an eine internationale Organisation
  - inkl. Angabe des betreffenden Drittlandes oder der internationalen Organisation
  - die Dokumentierung geeigneter Garantien bei der Datenübermittlung

- wenn möglich, die vorgesehenen Fristen für die Löschung verschiedener Datenkategorien
  - ev. Gesamt-Löschkonzept

- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung (Artikel 32 (1))
  - ev. Gesamt-Sicherheitskonzept plus
  - spezielle Sicherheitsmaßnahmen für einzelne Verarbeitungen, z.B.
    Verschlüsselung (verschlüsselte Datenbanken, Festplatten-Verschlüsselung, verschlüsselte Datenübertragung, …)
    Pseudonymisierung
    feingranulares Berechtigungskonzept

Inhalt des Verzeichnisses (Artikel 30 (1))

cont'd

Auftragsverarbeiter

› Auch Auftragsverarbeiter müssen ein Verzeichnis führen, anzugeben sind:

- Name und Kontaktdaten
  des Auftragsverarbeiter und der Verantwortlichen, in deren Auftrag der Auftragsverarbeiter tätig ist
- Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden
- ggfs. Übermittlungen von personenbezogenen Daten an Drittland, mit Detailinfo
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung (Artikel 32 (1))

› Genaue vertragliche Regelung zwischen Verantwortlichem und Auftragsverarbeiter erforderlich! (s. Artikel 28)

› Der Auftragsverarbeiter ermöglicht Überprüfungen — einschließlich Inspektionen –, die vom Verantwortlichen oder einem anderen von diesem beauftragten Prüfer durchgeführt werden

Allgemeines zum Verzeichnis

- Unabdingbar für die Erstellung des Verzeichnisses sind:
  - Detailkenntnisse über die einzelnen Verfahren
  - Zusammenarbeit → in einer größeren Organisation kann eine einzelne Person das Verzeichnis unmöglich erstellen
- Pflege des Verzeichnisses:
  - Verzeichnis muss aktuell gehalten werden
  - Prozesse sind zu definieren, dass Änderungen/Ergänzungen von Verarbeitungstätigkeiten an die jeweils verantwortliche Stelle kommuniziert werden
  - **Bewusstsein für Datenschutz im gesamten Unternehmen / in der gesamten Behörde ist essentiell**
- Das Verzeichnis ist eine wichtige Grundlage für die Erfüllung der Informations-, Auskunfts-, Lösch-, …-pflichten
- Die Prinzipien des Datenschutzes müssen in die Aufbau- und Ablauforganisation des Verantwortlichen integriert sein.

Das „Verzeichnis von Verarbeitungstätigkeiten“ wird DAS zentrale Dokument für die Datenschutzdokumentation sein.

Integration in die Prozesse

Betroffenenrechte, Informationspflichten, Meldepflichten

- Artikel 12: Transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Person
- Artikel 13 und 14: Informationspflicht bei der Erhebung von personenbezogenen Daten
- Artikel 15: Auskunftsrecht der betroffenen Person
- Artikel 16: Recht auf Berichtigung
- Artikel 17: Recht auf Löschung („Recht auf Vergessenwerden“)
- Artikel 18: Recht auf Einschränkung der Verarbeitung
- Artikel 19: Mitteilungspflicht im Zusammenhang mit Berichtigung oder Löschung oder Einschränkung der Verarbeitung
- Artikel 20: Recht auf Datenübertragbarkeit
- Artikel 21: Widerspruchsrecht
- Artikel 22: Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
- Artikel 33: Meldung von Verletzungen des Schutzes personenbezogener Daten (Data Breach Notification) (an die Aufsichtsbehörde)
- Artikel 34: Benachrichtigung (des Betroffenen) bei Verletzung des Schutzes personenbezogener Daten (Data Breach Communication)
- .....

Integration in die Prozesse

Betroffenenrechte, Informationspflichten, Meldepflichten

- Um den Informations- und Meldepflichten nachzukommen und die Einhaltung der Betroffenenrechte zu gewährleisten, müssen entsprechende Prozesse in der Behörde / im Unternehmen vorgesehen sein
  - Wer ist verantwortlich?
  - Wer entscheidet?
  - Wie sind die Melde-/Eskalationswege?
  - Vorgehensweise
  - Dokumentation

- Beispiel Auskunftserteilungen:
  - Identifikation/Authentifikation des Antragssteller (Welche Nachweise werden verlangt - Passkopie?, elektronische Signatur?, persönliches Erscheinen?, …)
  - Wer prüft die Legitimität?
  - Wie werden die konkreten personenbezogen Daten zum Betroffenen ermittelt
  - Wer gibt die Antwort?
  - Wie wird Antwort übermittelt (RSa-Brief, verschlüsselt, …)?

- Entweder in bestehende Prozesse anpassen (vieles ist It, DSG2000 auch schon gefordert) oder neue Prozesse definieren (Recht auf Datenübertragbarkeit)

Data Protection by Design und by Default

(Artikel 25)

Verantwortliche

NEU: Integration von Datenschutz in die Systeme und Applikationen

- Datenschutz durch Technikgestaltung „Data Protection by Design“ (Artikel 25(1))
  - Der Verantwortliche muss **geeignete technische und organisatorische Maßnahmen** treffen, um die **Datenschutzgrundsätze** (z.B. Datenminimierung) wirksam umzusetzen
  - daten- oder prozessorientierte Maßnahmen
  - Privacy Enhancing Techniques (PETs) - Verschlüsselung, Anonymisierung, … https://www.enisa.europa.eu/topics/data-protection
  - **wirtschaftliche Verhältnismäßigkeit**

- datenschutzfreundliche Voreinstellungen „Data Protection by Default“ (Artikel 25(2))
  - Der Verantwortliche muss geeignete technische und organisatorische Maßnahmen treffen, um sicherzustellen, dass **durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen Zweck erforderlich ist, verarbeitet werden.**
  - Verpflichtung betrifft die Menge der Daten, den Umfang der Verarbeitung, die Speicherfristen und die Zugänglichkeit der Daten.
  - Ev. müssen auch Einstellungsmöglichkeiten geschaffen werden!
  - **Immer erforderlich!**

Datenschutz-Folgenabschätzung

Data Protection Impact Assessment, DPIA (Artikel 35)

Verantwortliche

NEU in der DSGVO

Art. 35(1):
Hat eine Form der Verarbeitung, **insbesondere bei Verwendung neuer Technologien**, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung **voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen** zur Folge, so führt der **Verantwortliche vorab** eine **Abschätzung der Folgen** der vorgesehenen Verarbeitungsvorgänge für den Schutz personenbezogener Daten durch. …

- Datenschutz-Folgenabschätzung ist auf jeden Fall erforderlich bei
  - systematischer und umfassender Bewertung persönlicher Aspekte natürlicher Personen (z.B. Profiling), die als Grundlage für rechtswirksame Entscheidungen dienen…
  - umfangreicher Verarbeitung „sensibler“ Daten oder Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10
  - systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche

Datenschutz-Folgenabschätzung

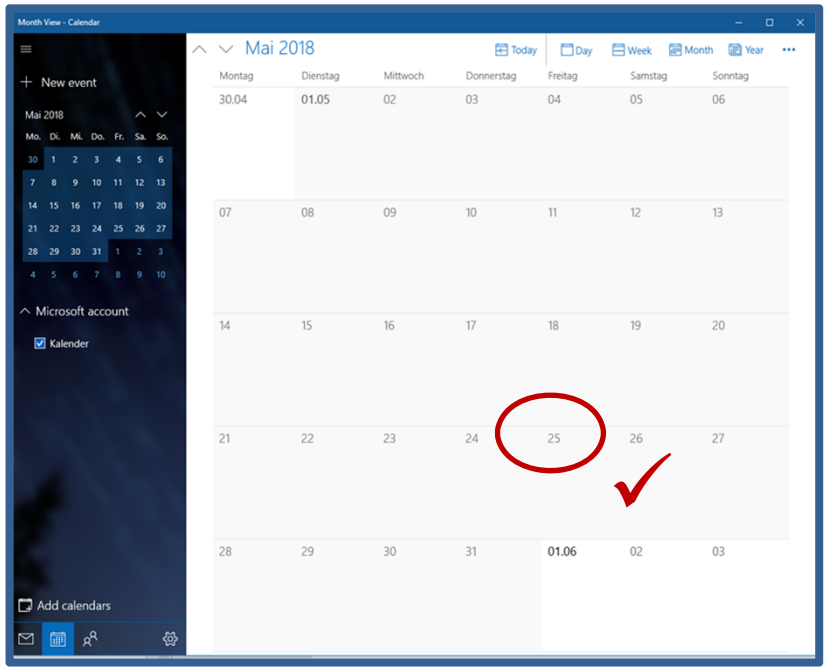
Data Protection Impact Assessment, DPIA (Artikel 35 (7))

Verantwortliche

- Mindestinhalte der Datenschutz-Folgenabschätzung:
  - systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung
  - Beschreibung der berechtigten Interessen
  - Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge
  - **Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen**
  - die zur Bewältigung der Risiken geplanten **Abhilfemaßnahmen**, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren

- Vorherige Konsultation (Artikel 36):
  - Falls die DPIA ergibt, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft, ist **vor Aufnahme der Verarbeitung** die Aufsichtsbehörde zu konsultieren.
  - Wurde das Risiko nicht ausreichend ermittelt oder nicht ausreichend abgedeckt:
    - Aufsichtsbehörde gibt schriftliche Empfehlungen (Frist 8 Wochen),
    - Ausübung der Befugnisse lt. Artikel 58 (Warnungen, Anweisungen, Beschränkungen / Verbot von Verarbeitungen, Verhängung von Strafen,…)

- Black-/Whitelist der Aufsichtsbehörde



Vielen Dank für Ihre Aufmerksamkeit!

ISCC Information Security Compliance Center der fhoö