Datenschutz-Folgenabschätzung / Privacy by design & default

Dipl.-Ing. Dr. iur. Walter Hötzendorfer
Senior Researcher | Senior Consultant

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte
Smart.Rights.Consulting

Annagasse 8/1/8
1010 Wien

E-Mail: walter.hoetzendorfer@researchinstitute.at
Web: http://www.researchinstitute.at

Dipl.-Ing. Dr. iur. Walter Hötzendorfer

- Wirtschaftsinformatiker und Jurist
- **Senior Researcher** und **Senior Consultant**, Research Institute – Zentrum für digitale Menschenrechte
- Autor des Buches „**Datenschutz und Privacy by Design im Identitätsmanagement**“ und Mitautor zweier aktueller Bücher zur Datenschutz-Grundverordnung
- Vorstandsmitglied der Österreichischen Computer Gesellschaft (**OCG**) und Co-Leiter **OCG Forum Privacy**
- Mitglied in der ASI-AG 001 18, die derzeit einen Datenschutz-Management-Standard ausarbeitet
- Vortragender im In- und Ausland
- **Erfahrungen** in:
  - Wissenschaft (RI, Uni Wien, Arbeitsgruppe Rechtsinformatik)
  - Rechtsberatung
  - Software Engineering
  - Prozessmanagement
- **Forschungsschwerpunkte**:
  - Technische und organisatorische Aspekte des Datenschutzrechts
  - Privacy Engineering, Privacy by Design, Datensicherheit/NIS
  - Identity Management
  - Telekommunikationsrecht
  - Öffentliche Sicherheit

RESEARCH INSTITUTE AG & CO KG

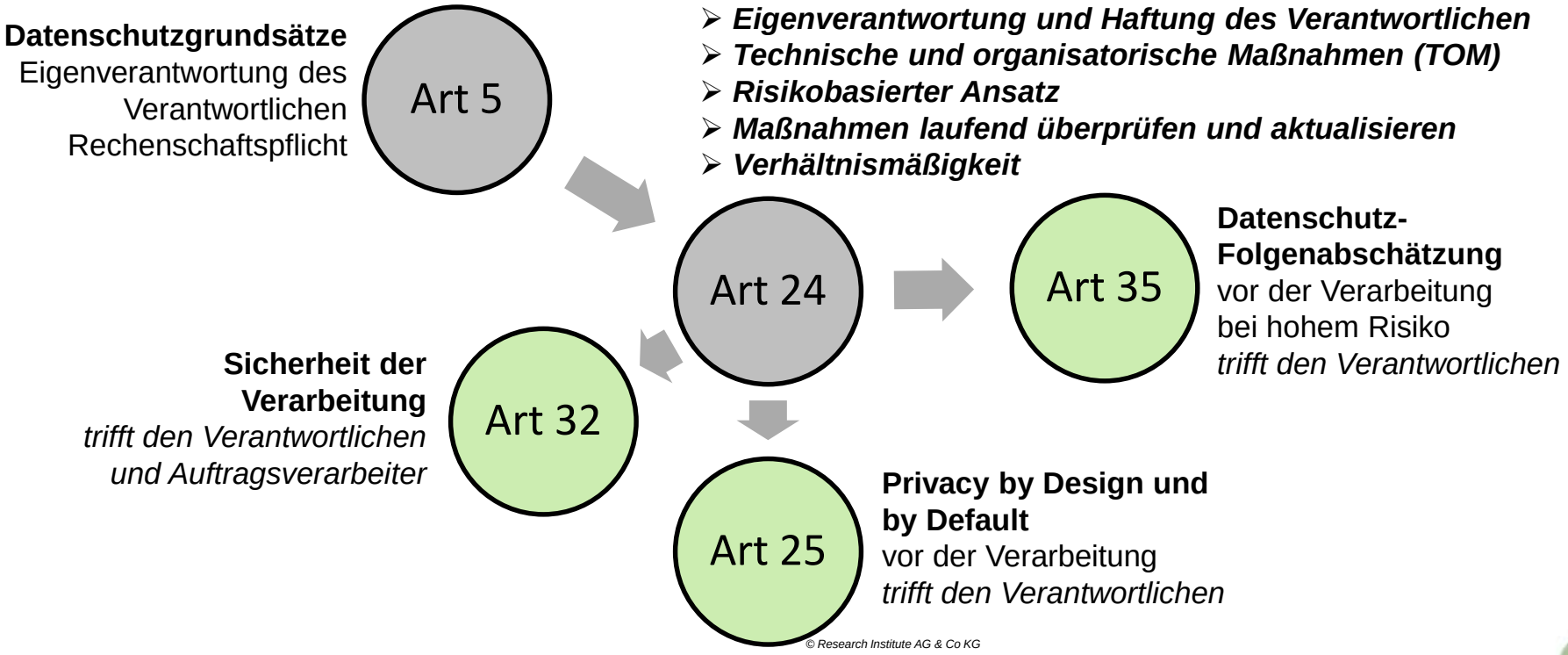
ZENTRUM FÜR DIGITALE MENSCHENRECHTE

Das **Research Institute (RI)** ist ein Forschungszentrum an der Schnittstelle von **Technik, Recht** und **Gesellschaft**, das sich aus multi- und interdisziplinärer Perspektive mit der Bedeutung der Menschenrechte im digitalen Zeitalter beschäftigt.

Portfolio:

- **Forschung zu technischen** und **rechtlichen** Aspekten von **Datenschutz** und **Datensicherheit, Cybercrime, Technikfolgenabschätzung** und **Netzpolitik**
- **Smart.Rights.Consulting:** Beratung in datenschutzrechtlichen Fragen
- **Schulungen** für Privatpersonen und Mitarbeiter von Unternehmen/Organisationen
- **Maßgeschneiderte technische Lösungen** zur praktischen Umsetzung der Compliance-Prozesse (in Zusammenarbeit mit Software-Entwicklern)
- **Konzeption und Durchführung individueller und multidisziplinärer Projekte** mit renommierten Partnern auf nationaler und internationaler Ebene.

ÜBERBLICK UND ZUSAMMENHÄNGE



research institute

DATENSCHUTZ-FOLGENABSCHÄTZUNG
ART 35 DSGVO

Datenschutz-Folgenabschätzung: Intentionen des Gesetzgebers

- DSGVO ersetzt Meldepflicht und Genehmigungspflicht (ErwGr 89: „bürokratisch“) durch
  - Eigenverantwortung des Verantwortlichen und
  - risikobasierten Ansatz
- Intensive Befassung mit jenen Verarbeitungsvorgängen, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen mit sich bringen
  => Prüfen, ob ein hohes Risiko besteht, und ggf.
  Datenschutz-Folgenabschätzung durchführen
  oder dokumentieren, warum nicht
- Die damit verbundenen Abwägungen und Einschätzungen muss der Verantwortliche treffen
- Keine Pflichtverletzung, wenn auf Basis des zum Zeitpunkt der Prognose verfügbaren Wissens deren Unrichtigkeit nicht abzusehen war

Datenschutz-Folgenabschätzung: Motivation

- Wenn eine Datenverarbeitung „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 hat, führt man eine Datenschutz-Folgenabschätzung durch, zwecks
  - Erkennen und Analyse der Risiken für die Betroffenen aufgrund der geplanten Verarbeitung
  - Ergreifen von Gegenmaßnahmen
  - Steigerung der Rechtssicherheit
  - Verringerung des (wirtschaftlichen) Risikos nachträglicher Anpassungen

Artikel 35

Datenschutz-Folgenabschätzung

(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. Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden.

(2) Der Verantwortliche holt bei der Durchführung einer Datenschutz-Folgenabschätzung den Rat des Datenschutzbeauftragten, sofern ein solcher benannt wurde, ein.

(3) Eine Datenschutz-Folgenabschätzung gemäß Absatz 1 ist insbesondere in folgenden Fällen erforderlich:

a) systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;

b) umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Artikel 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 oder

c) systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

(4) Die Aufsichtsbehörde erstellt eine Liste der Verarbeitungsvorgänge, für die gemäß Absatz 1 eine Datenschutz-Folgenabschätzung durchzuführen ist, und veröffentlicht diese. Die Aufsichtsbehörde übermittelt diese Listen dem in Artikel 68 genannten Ausschuss.

(5) Die Aufsichtsbehörde kann des Weiteren eine Liste der Arten von Verarbeitungsvorgängen erstellen und veröffentlichen, für die keine Datenschutz-Folgenabschätzung erforderlich ist. Die Aufsichtsbehörde übermittelt diese Listen dem Ausschuss.

(6) Vor Festlegung der in den Absätzen 4 und 5 genannten Listen wendet die zuständige Aufsichtsbehörde das Kohärenzverfahren gemäß Artikel 63 an, wenn solche Listen Verarbeitungstätigkeiten umfassen, die mit dem Angebot von Waren oder Dienstleistungen für betroffene Personen oder der Beobachtung des Verhaltens dieser Personen in mehreren Mitgliedstaaten im Zusammenhang stehen oder die den freien Verkehr personenbezogener Daten innerhalb der Union erheblich beeinträchtigen könnten.

(7) Die Folgenabschätzung enthält zumindest Folgendes:

a) eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;

b) eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;

c) eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und

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.

(8) Die Einhaltung genehmigter Verhaltensregeln gemäß Artikel 40 durch die zuständigen Verantwortlichen oder die zuständigen Auftragsverarbeiter ist bei der Beurteilung der Auswirkungen der von diesen durchgeführten Verarbeitungsvorgänge, insbesondere für die Zwecke einer Datenschutz-Folgenabschätzung, gebührend zu berücksichtigen.

(9) Der Verantwortliche holt gegebenenfalls den Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung unbeschadet des Schutzes gewerblicher oder öffentlicher Interessen oder der Sicherheit der Verarbeitungsvorgänge ein.

(10) Falls die Verarbeitung gemäß Artikel 6 Absatz 1 Buchstabe c oder e auf einer Rechtsgrundlage im Unionsrecht oder im Recht des Mitgliedstaats, dem der Verantwortliche unterliegt, beruht und falls diese Rechtsvorschriften den konkreten Verarbeitungsvorgang oder die konkreten Verarbeitungsvorgänge regeln und bereits im Rahmen der allgemeinen Folgenabschätzung im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung erfolgte, gelten die Absätze 1 bis 7 nur, wenn es nach dem Ermessen der Mitgliedstaaten erforderlich ist, vor den betreffenden Verarbeitungstätigkeiten eine solche Folgenabschätzung durchzuführen.

(11) Erforderlichenfalls führt der Verantwortliche eine Überprüfung durch, um zu bewerten, ob die Verarbeitung gemäß der Datenschutz-Folgenabschätzung durchgeführt wird; dies gilt zumindest, wenn hinsichtlich des mit den Verarbeitungsvorgängen verbundenen Risikos Änderungen eingetreten sind.

FÄLLE, IN DENEN EINE DSFA JEDENFALLS DURCHZUFÜHREN IST (ABS 3)

- Systematische und umfassende **Bewertung persönlicher Aspekte** natürlicher Personen, die sich auf **automatisierte Verarbeitung einschließlich Profiling** gründet und die ihrerseits als Grundlage für Entscheidungen dient, die **Rechtswirkung** gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen
- Umfangreiche Verarbeitung **besonderer Kategorien von personenbezogenen Daten** gemäß Art 9 Abs 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art 10
  => Ab welchem Umfang ist eine Verarbeitung „umfangreich“?
  - Menge der Daten
  - Zahl der Betroffenen: Richtwert > 5000 binnen 12 Monaten
  - Nicht aber Patienten eines einzelnen Arztes oder Mandanten eines einzelnen Rechtsanwalts (ErwGr 91)
- Systematische umfangreiche **Überwachung** öffentlich zugänglicher Bereiche

Fälle, in denen eine DSFA jedenfalls durchzuführen ist (ErwGr 91)

- Verarbeitungsvorgänge, die potenziell eine **große Zahl von Personen** betreffen, ein **hohes Risiko** mit sich bringen und bei denen entsprechend dem jeweils aktuellen Stand der Technik in großem Umfang eine **neue Technologie** eingesetzt wird
- Verarbeitungsvorgänge, die ein **hohes Risiko** mit sich bringen, und betroffenen Personen die **Ausübung ihrer Rechte erschweren**
- Verarbeitungsvorgänge, bei denen personenbezogene Daten für das **Treffen von Entscheidungen in Bezug auf bestimmte natürliche Personen** im Anschluss an die Verarbeitung **besonderer Kategorien von personenbezogenen Daten**, von biometrischen Daten oder von Daten über strafrechtliche Verurteilungen und Straftaten sowie damit zusammenhängende Sicherungsmaßregeln verarbeitet werden
- Verarbeitungsvorgänge, die ein **hohes Risiko** mit sich bringen, weil sie die betroffenen Personen an der **Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern**
- Verarbeitungsvorgänge, die ein **hohes Risiko** mit sich bringen, weil sie **systematisch in großem Umfang** erfolgen

Art-29-Datenschutzgruppe: Kriterien für hohes Risiko

Faustregel: Ein hohes Risiko besteht jedenfalls, wenn mindestens zwei der folgenden Kriterien erfüllt sind.

- Profiling/Scoring natürlicher Personen
- Automatisierte Entscheidungen, die rechtliche oder vergleichbare Wirkung gegenüber natürlichen Personen entfalten
- Systematische Überwachung
- Sensible Daten
- Datenverarbeitung in großem Umfang
- Verknüpfung verschiedener Datenbestände
- Daten schutzbedürftiger natürlicher Personen
- Neue Technologien oder neuartiger Einsatz von Technologien
- Datenübermittlung in Drittländer
- Datenverarbeitungen, die Betroffene an der Ausübung eines Rechts oder der Nutzung einer Dienstleistung bzw. Durchführung eines Vertrags hindern

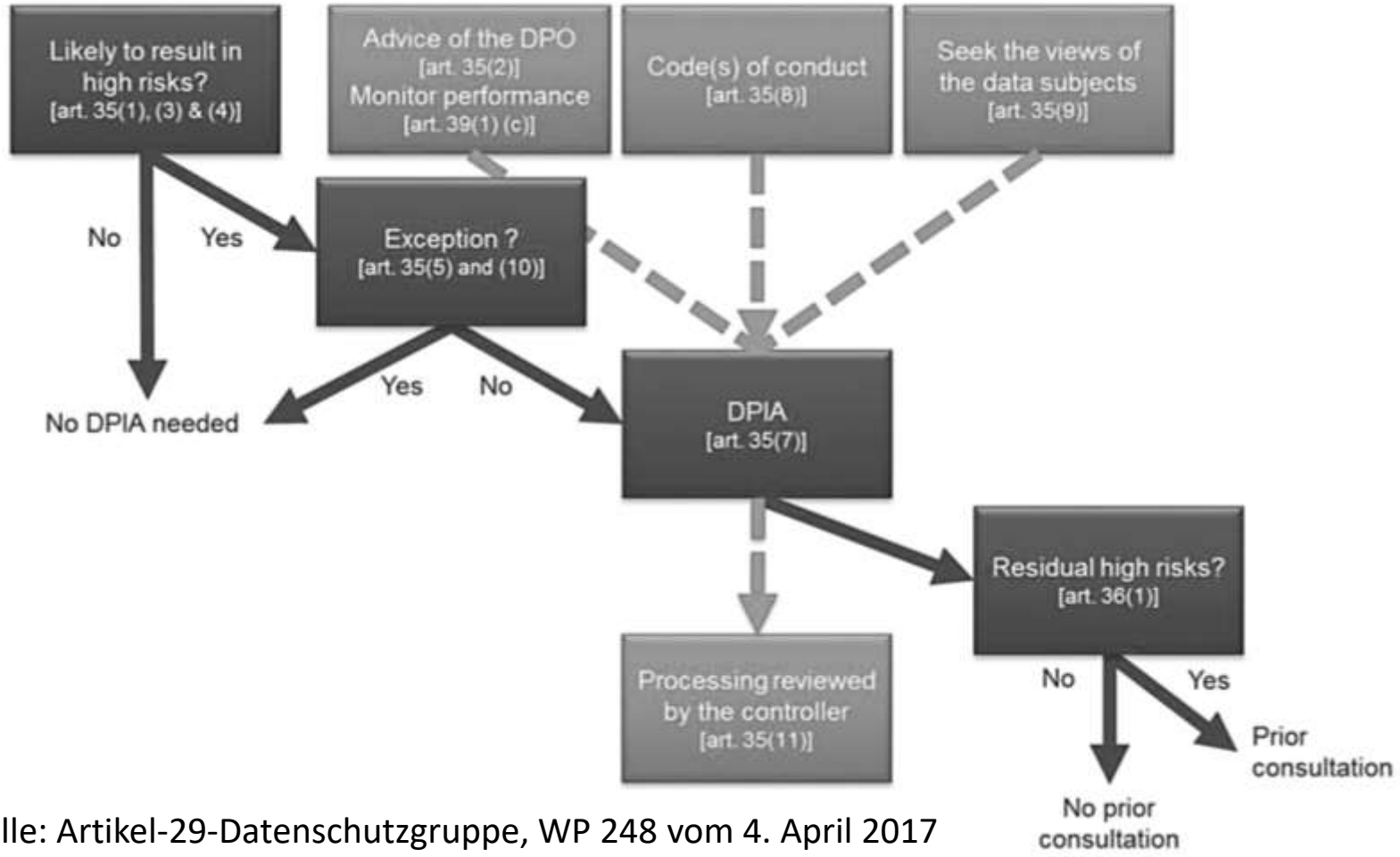
Positivliste und Negativliste

- Die Aufsichtsbehörde *hat* eine Liste der Verarbeitungsvorgänge zu erstellen, für die eine Datenschutz-Folgenabschätzung durchzuführen ist (Positivliste).
- Die Aufsichtsbehörde *kann* eine Liste der Arten von Verarbeitungsvorgängen erstellen, für die keine Datenschutz-Folgenabschätzung durchzuführen ist (Negativliste).
- Kohärenzverfahren (Art 63) zur Koordinierung dieser Listen zwischen den Aufsichtsbehörden betreffend Arten von Verarbeitungsvorgängen, die Auswirkungen auf mehrere Mitgliedstaaten haben, zwecks einheitlicher Anwendung der DSGVO

Ausnahme bei gesetzlicher Grundlage (Abs 10)

- Beruht die Verarbeitung auf einer nationalen oder unionsrechtlichen Rechtsgrundlage nach
  - Abs 1 lit c (Verpflichtung des Verantwortlichen zu bestimmten Verarbeitungen) oder
  - Abs 1 lit e (Verarbeitungserfordernisse durch öffentliche Stellen bzw. im öffentlichen Interesse)
- und wurde bereits im Zusammenhang mit dem Erlass dieser Rechtsgrundlage eine Datenschutz-Folgenabschätzung durchgeführt,
- besteht keine Pflicht zur Datenschutz-Folgenabschätzung,
- es sei denn, der Mitgliedstaat ordnet diese nach seinem Ermessen dennoch an

PRÜFSCHEMA DATENSCHUTZ-FOLGENABSCHÄTZUNG (DSFA)



Quelle: Artikel-29-Datenschutzgruppe, WP 248 vom 4. April 2017

Durchführung der Datenschutz-Folgenabschätzung (Abs 7)

1. Aufsetzen des Projekts:
   - Zusammenstellung des Teams: Fachabteilung, Juristen, Techniker, ggf. Datenschutzbeauftragter, ggf. externe Berater
   - Zeit- und Ressourcenplanung
   - Commitment des Managements
2. Beschreiben der geplanten Verarbeitung inkl. ihrer Zwecke (im Kontext)
3. Einholen der Standpunkte der betroffenen Personen oder ihrer Vertreter (Abs 9)
   - Verpflichtung, wenn ein solcher Standpunkt vorliegt oder abzusehen ist
   - Impliziert auch die Information der Betroffenen
4. Zulässigkeitsprüfung inkl. Bewertung der Notwendigkeit und Verhältnismäßigkeit
5. Identifizieren, Analysieren und Bewerten der Risiken für die Betroffenen:
   - Eintrittswahrscheinlichkeit
   - Auswirkungen der Risikoverwirklichung
6. Identifizieren von Maßnahmen zum Umgang mit den nicht tragbaren Risiken
7. Dokumentation der Datenschutz-Folgenabschätzung (Bericht) mit Nachweisen, wie die Anforderungen der DSGVO eingehalten werden
8. Laufende Überprüfung, ob die bei der Datenschutz-Folgenabschätzung getroffenen Annahmen und Prognosen richtig waren und die Verarbeitung gemäß (den Vorgaben) der Datenschutz-Folgenabschätzung durchgeführt wird

Beispiel einer Risikomatrix als Grundlage der Risikobewertung

BEISPIEL EINER RISIKOBEURTEILUNG (VEREINFACHT)

Identifiziertes Risiko (Beschreibung)	Auswirkungen (Schwere)	Eintrittswahrscheinlichkeit	Risikograd	Maßnahmen (TOM)	Finaler Risikograd
Bekanntwerden medizinischer Diagnosen durch Datendiebstahl auf dem Übertragungsweg	sehr schwer	mittel	hoch	Ende-zu-Ende-Verschlüsselung der Daten	mittel
Missbräuchliche Leistungsbeurteilung der Mitarbeiter auf Basis elektronischer Ausweiskarten (Bewegungsdaten)	schwer (da jeder Mitarbeiter seinen Ausweis täglich im Schnitt 12x benützen muss)	mittel	mittel	4-Augen-Prinzip bei der Auswertung (by Design); Protokollierung und regelmäßige Auswertung der Zugriffe auf die Bewegungsdaten mit dem Betriebsrat	niedrig

Datenschutz-Folgenabschätzung bei bestehenden Verarbeitungen?

Ist für Datenverarbeitungen, die bei In-Geltung-Treten der DSGVO schon in Betrieb sind, ebenfalls eine Datenschutz-Folgenabschätzung durchzuführen?

- Abschätzung ist grds *vorab* durchzuführen
- Differenzierte Meinung der *Art-29-Datenschutzgruppe* in WP248 rev.01*:
  - Folgenabschätzung nicht erforderlich, wenn eine bestehende Verarbeitung im Zuge der Vorabkontrolle (dh in Österreich: von der DSB) geprüft wurde und diese unverändert geblieben ist
  - Folgenabschätzung jedenfalls dann erforderlich, wenn sich die Umstände der Verarbeitung geändert haben und sich ein hohes Risiko ergeben könnte

*aktualisiert aufgrund des Erscheinens von WP248 rev.01 am 13.10.2017

Sonstige Bestimmungen

- Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohen Risiken kann eine einzige Abschätzung vorgenommen werden (Abs 1)
  - Sinnvoll auch zur Betrachtung eines allfälligen Gesamtrisikos und ggf. auch aus wirtschaftlichen Gründen
  - Auch Verarbeitungen verschiedener Verantwortlicher (wichtig: klare Zuordnung der Pflichten)
  - Beispiel (ErwGr 92): „wenn Behörden oder öffentliche Stellen eine gemeinsame Anwendung oder Verarbeitungsplattform schaffen möchten“
  - Praxisbeispiele: Videoüberwachung in mehreren Kommunen oder in mehreren Bahnhöfen
  - Hersteller eines Produkts kann eine Abschätzung durchführen und so den Verwendern des Produkts (die weiterhin verpflichtet bleiben) deren Abschätzung erleichtern
- Durchführung durch interne oder externe Personen
- Bei Durchführung ist Rat des Datenschutzbeauftragten (sofern vorhanden) einzuholen
- Die Pflicht trifft nur Verantwortliche, nicht auch Auftragsverarbeiter. Diese haben allerdings gemäß Art 28 Abs 3 lit f die Verantwortlichen bei der Erfüllung der aus Art 35 erwachsenden Pflichten zu unterstützen

EMPFEHLUNGEN

- Dokumentation aller Entscheidungen, insbesondere warum ggf. keine Datenschutz-Folgenabschätzung durchgeführt wurde
- Im Zweifel Durchführung einer Datenschutz-Folgenabschätzung
- Einbeziehung der internen und externen Betroffenen
- Heranziehen von Mustern, Best Practices und ggf. ähnlichen, bereits durchgeführten Datenschutz-Folgenabschätzungen
- Veröffentlichen der Datenschutz-Folgenabschätzung
  - Insbesondere durch öffentliche Stellen
  - Zeigt Datenschutz-Bewusstsein und schafft Vertrauen

- Literatur: *Kastelitz/Hötzendorfer/Riedl*, Ausgewählte Fragen der Durchführung einer Datenschutz-Folgenabschätzung gemäß Art 35 DSGVO, in: Jahnel (Hrsg.), Jahrbuch Datenschutzrecht 2017, *erscheint im November 2017*

research institute

PRIVACY BY DESIGN & DEFAULT
ART 25 DSGVO

Privacy by Design: Motivation

- Vollzugsdefizit: Im Datenschutz scheint **retrospektive Regulierung** besonders schlecht zu funktionieren
  - Verstöße passieren meist auf nicht einsehbaren Systemen und sind schwer nachzuweisen
  - Funktionsweise im Detail nur für Experten erfassbar
  - Durchsetzung schwierig
  - Wiedergutmachung häufig unmöglich
- Das menschliche Handeln wird nicht nur durch das Recht, sondern auch durch die Systeme selbst bestimmt und beschränkt – *Code is Law (Lessig)*
- **Prospektive Regulierung**: Durch die Gestaltung der Systeme können nicht intendierte Datenverwendungen auf faktischer Ebene von vorn herein ausgeschlossen werden
- Daher: Datenschutz in der Gestaltung von Systemen von Beginn an berücksichtigen

Was bedeutet Privacy by Design?

1. Datenschutz bei der Gestaltung von Systemen von Beginn an berücksichtigen,

sodass die Verwirklichung der Datenschutzgrundsätze bereits in den Systemen angelegt ist

2. Verhindern der nicht intendierten/nicht zweckkonformen Verwendung des Systems durch technische und organisatorische Maßnahmen

Technik als Mittel zur Durchsetzung des Datenschutzes

Privacy by Design wirkt sich sowohl auf die Architektur als auch auf viele Detailaspekte der Gestaltung von Systemen aus

Zentrale Maßnahme: **Datenminimierung**

ART 25 ABS 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 der mit der Verarbeitung verbundenen **Risiken** für die Rechte und Freiheiten natürlicher Personen 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 — trifft, 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 25 ABS 1

- Gänzlich neue Pflicht (vgl jedoch bereits die Formulierung in ErwGr 46 Datenschutzrichtlinie)
- Begriff:
  - DSGVO (EN): „Data Protection by Design“
  - DSGVO (DE): „Datenschutz durch Technikgestaltung“
  - Wissenschaft: „Privacy by Design“ (PbD)
  - eIDAS-VO (EN): „Privacy by Design“
  - eIDAS-VO (DE): „eingebauter Datenschutz“
- **Verhältnismäßigkeitsabwägung** zwischen den Risiken für die Rechte und Freiheiten natürlicher Personen (siehe ErwGr 75) und der wirtschaftlichen Belastung des Verantwortlichen durch die Maßnahmen unter Berücksichtigung
  - des Stands der Technik
  - der Implementierungskosten
  - der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung
- Zugleich: Risiko für den Verantwortlichen, eigenverantwortlich diese Abwägung angemessen zu treffen

Zum Begriff „Stand der Technik“

- Maßnahmen, die
  - aktuell technisch realisierbar sind
  - auf gesicherten Erkenntnissen der Wissenschaft und Technik beruhen
  - und in ausreichendem Maße zur Verfügung stehen

  (vgl Martini in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung, Beck [2017] Art 25 Rz 39 mwN)
- Es kommt somit auf die praktische Umsetzbarkeit an, nicht aber auf einen bereits weit verbreiteten Einsatz in der Praxis
- Betrifft nicht nur Ausgestaltung einzelner Maßnahmen (zB Auswahl von Verschlüsselungsalgorithmen), sondern auch vorgelagerte Auswahl der Arten von Maßnahmen

Zu den Implementierungskosten

- Die Implementierungskosten sind mit den Risiken für die Rechte und Freiheiten natürlicher Personen und nicht mit dem voraussichtlichen wirtschaftlichen Nutzen der Datenverarbeitung für den Verantwortlichen abzuwägen
- Datenschutz ist Grundrechtsschutz, d.h.
  - Grundsatz der Verhältnismäßigkeit (Art 52 Abs 2 GRC): Es sind keine Maßnahmen zu treffen, deren Implementierungskosten im Verhältnis zur Steigerung des Schutzniveaus unverhältnismäßig hoch sind
  - Ein unzureichendes Schutzniveau kann aber nicht mit wirtschaftlichen Erwägungen gerechtfertigt werden
- Wenn ein risikoadäquates Schutzniveau mit einem dem Nutzen der Verarbeitung angemessenen Aufwand nicht hergestellt werden kann, ist es unzulässig, das Schutzniveau aus diesem Grund abzusenken
- Begriff:
  - Art 25 und Art 32 DSGVO: Genannt sind nur die Implementierungskosten, nicht auch Folgekosten bzw. laufende Kosten
  - Art 17 Abs 1 DSRL: Genannt sind nur die bei der Durchführung der Maßnahmen entstehenden Kosten

Art 25 Abs 1: Weitere Fragen

- **Privacy by Design bei bestehenden Systemen:**
  - Eine Einschränkung der Verpflichtung auf neu zu entwickelnde Systeme ist nicht ersichtlich, sodass Privacy by Design grundsätzlich auch in bestehenden Systemen umzusetzen ist
  - ErwGr 171: Bestehende Verarbeitung sollten bis 25. Mai 2018 mit der DSGVO in Einklang gebracht werden
  - Es sei denn, dies würde im Sinne der Verhältnismäßigkeitsabwägung (Risiko und Implementierungskosten) einen unverhältnismäßig hohen Aufwand verursachen
- Normadressat des Art 25 ist nur der Verantwortliche, nicht auch der Auftragsverarbeiter (anders im Falle des Art 32)
- ErwGr 78: **Faktische Wirkung auf Hersteller von Produkten**, denn Verantwortliche sind dazu verpflichtet, solche Produkte zu erwerben, die die Vorgaben des Art 25 erfüllen

Praktische Umsetzung von Privacy by Design im Unternehmen

- Häufige Kritik: PbD sei zu wenig konkret
- Zentrale Maßnahme: **Datenminimierung** (auch „Datensparsamkeit“) – Reduktion der Verarbeitung personenbezogener Daten auf das Unvermeidbare; zahlreiche Dimensionen:
  - Art der Daten (zB nicht Geburtsdatum, wenn Alter oder Geburtsjahr ausreicht)
  - Umfang der Daten
  - Speicherdauer
  - Kreis der Zugriffsberechtigten
- Etablieren von **Privacy by Design als Mentalität** im Unternehmen: Privacy by Design ist vor allem eine Einstellung, wie man an Dinge herangeht
- **Schaffung von Prozessen**:
  - Entwicklung oder Beschaffung neuer Systeme darf nicht genehmigt werden, wenn man sich nicht über den Datenschutz Gedanken gemacht hat
  - Dokumentation, dass man bei der Planung von Systemen („zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung“) eine Abschätzung der Datenschutzrisiken durchgeführt und entsprechende Maßnahmen getroffen hat
  - Beschaffte Software muss Privacy by Design entsprechen: Hersteller und Auftragsverarbeiter in die Pflicht nehmen

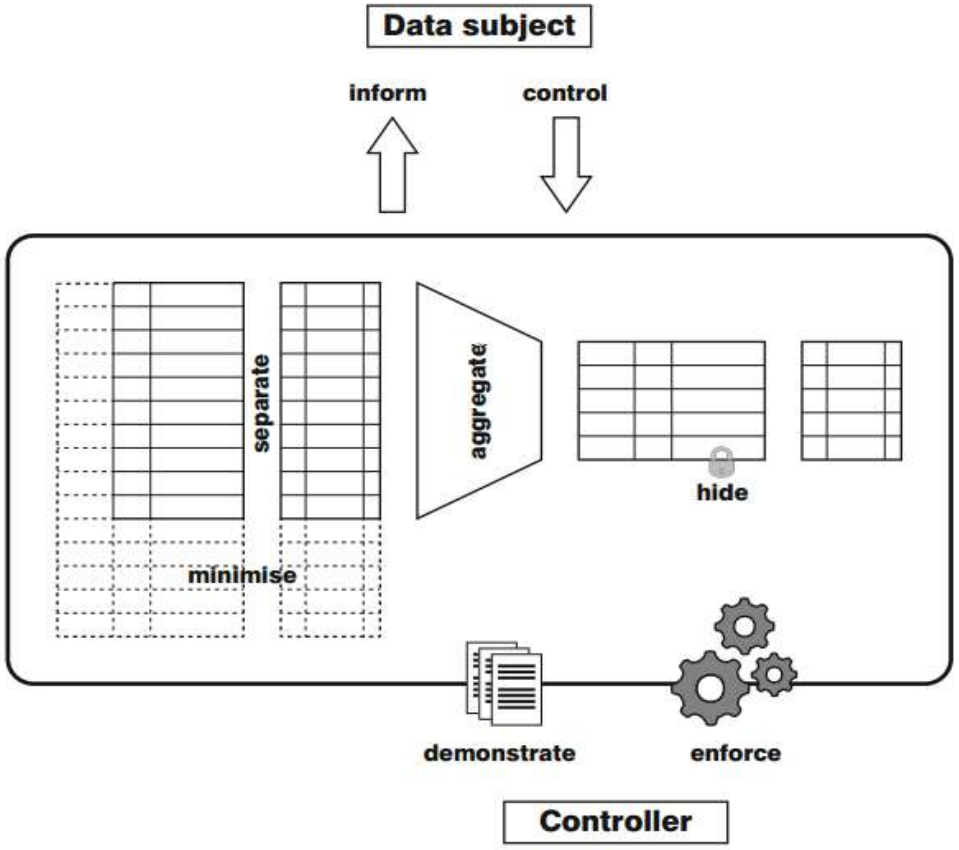
Praktische Umsetzung von Privacy by Design im Software Engineering

- Privacy by Design ist die Umsetzung einiger weniger Grundprinzipien des Datenschutzes
  - von Beginn an
  - individuell auf das jeweilige System und dessen Zweck abgestimmt
  - durch Design-Strategien, Design Patterns und Privacy-Enhancing Technologies (PETs)
  - unter Einbeziehung von Wissen über häufige Fehler, die Rechtslage, aktuelle Bedrohungen und Angriffsmethoden etc.
- Involvieren von „**Privacy Engineers**“ in den Software-Design- und -entwicklungsprozess von Beginn an, die die Grundprinzipien des Datenschutzes auf das jeweilige individuelle System umlegen
  - Kenntnisse des Datenschutzes und technische Kenntnisse
  - Privacy Engineering als neue Disziplin
  - Community
- Beispiele:
  - Daten wenn möglich beim Nutzer verschlüsseln und nicht erst auf dem Server
  - „Durchlaufstelle“ nach TKG-Datensicherheitsverordnung als kontrollierte Schnittstelle zwischen Sicherheitsbehörden und Telekommunikationsanbietern
- Weitere Beispiele: https://privacypatterns.org/

PRIVACY-DESIGN-STRATEGIEN

- MINIMISE
- HIDE
- SEPARATE
- AGGREGATE

- INFORM
- CONTROL
- ENFORCE
- DEMONSTRATE



Quelle: ENISA, Privacy and Data Protection by Design – from policy to engineering, 2014

PRIVACY-DESIGN-STRATEGIEN

- MINIMISE: Die Menge der verarbeiteten Daten sollte so gering wie möglich sein
- HIDE: Alle personenbezogenen Daten und ihre Zusammenhänge sollten möglichst verborgen bleiben
- SEPARATE: Personenbezogene Daten sollten möglichst verteilt verarbeitet und getrennt gespeichert werden
- AGGREGATE: Personenbezogene Daten sollten im höchsten Aggregationsniveau und mit dem niedrigsten Detailgrad verarbeitet werden, in dem sie (noch) ihren Zweck erfüllen
- INFORM: Betroffene sollten angemessen informiert werden, wann immer ihre personenbezogenen Daten verarbeitet werden
- CONTROL: Betroffene sollten Kontrolle über die Verarbeitung ihrer personenbezogenen Daten erhalten
- ENFORCE: Mit den rechtlichen Anforderungen in Einklang stehende Datenschutzregeln sollten vorhanden sein und durchgesetzt werden
- DEMONSTRATE: Der Verantwortliche sollte dazu in der Lage sein, die Einhaltung der Datenschutzregeln und aller gesetzlichen Bestimmungen nachzuweisen

Quelle: ENISA, Privacy and Data Protection by Design – from policy to engineering, 2014

WAS BEDEUTET PRIVACY BY DEFAULT?

Wenn ein Betroffener ein Produkt in Betrieb oder eine Dienstleistung in Anspruch nimmt, sind die datenschutzfreundlichsten Einstellungen von vornherein ausgewählt, mit denen der Verarbeitungszweck gerade noch erreicht werden kann

Bei Bedarf kann der Betroffene diese Einstellungen dann bewusst ändern

Tut er dies nicht, ist er im Rahmen der Einstellungsmöglichkeiten bestmöglich geschützt

Hintergrund: „Privacy Paradox“/Überforderung/Unwissen/Trägheit

Insbesondere sicherstellen, dass personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen der Person einer unbestimmten Zahl von natürlichen Personen zugänglich gemacht werden (Abs 2 Satz 2)
Z.B. Hochladen eines Fotos auf Facebook: Voreinstellung muss gewährleisten, dass das Foto nur einem beschränkten Personenkreis zugänglich wird

Privacy by Default kann auch als **Bestandteil von Privacy by Design** angesehen werden: Eine Funktion ist zwar nicht gänzlich ausgeschlossen, aber im Standardfall deaktiviert

Art 25 Abs 2

- Geeignete **technische und organisatorische Maßnahmen**, die sicherstellen, dass **durch Voreinstellung** grundsätzlich **nur personenbezogene Daten**, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck **erforderlich** ist, verarbeitet werden
  - Kein Verweis auf „Stand der Technik“
  - Keine Verhältnismäßigkeitsabwägung
  - Keine Einschränkung der Verpflichtung auf neu zu entwickelnde Systeme ersichtlich
  - Schaffung neuer Einstellungsmöglichkeiten in bestehender Software? Wenn, dann im Zuge der allgemeinen Anpassung an die DSGVO erforderlich
- Diese Verpflichtung gilt für
  - die Menge der erhobenen personenbezogenen Daten,
  - den Umfang ihrer Verarbeitung,
  - ihre Speicherfrist und
  - ihre Zugänglichkeit
- Die Bestimmung hat Systeme vor Augen, die vom Betroffenen selbst bedient werden
- Verpflichtung nur für Verantwortliche

Privacy by Design und by Default: Einige Empfehlungen

- So früh als möglich prüfen, was Privacy by Design und vor allem die uneingeschränkte Pflicht zu Privacy by Default für die eigenen Produkte und Dienstleistungen bedeutet
- Verankern von Privacy by Design und by Default im Unternehmen als Mentalität und in Form von Prozessen
  - Vor allem außerhalb der Rechtsabteilung:
    - IT
    - Entwicklung
    - Beschaffung (mittelbare Auswirkungen für Softwarehersteller und Auftragsverarbeiter)
  - Dokumentation der Maßnahmen und Entscheidungen
- Involvieren von „**Privacy Engineers**“ in den Software-Design- und -entwicklungsprozess von Beginn an, die die Grundprinzipien des Datenschutzes auf das jeweilige individuelle System umlegen
  - Kenntnisse des Datenschutzes und technische Kenntnisse
  - Privacy Engineering als neue Disziplin
  - Community
- Zertifizierung (iSv Art 42) kann als Faktor herangezogen werden, um die Erfüllung nachzuweisen (Art 25 Abs 3)

Datenschutz-Folgenabschätzung / Privacy by design & default

Dipl.-Ing. Dr. iur. Walter Hötzendorfer
Senior Researcher | Senior Consultant

Research Institute AG & Co KG
Zentrum für digitale Menschenrechte
Smart.Rights.Consulting

Annagasse 8/1/8
1010 Wien

E-Mail: walter.hoetzendorfer@researchinstitute.at
Web: http://www.researchinstitute.at