Die technische Dimension der Datenschutz-Grundverordnung

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

Zur Person

Dipl.-Ing. Dr. iur. Walter Hötzendorfer

- Wirtschaftsinformatiker und Jurist
- **Senior Researcher** und **Senior Consultant**, Research Institute
- OCG-Vorstandsmitglied und Co-Leiter „OCG Forum Privacy“
- (Mit-)Autor mehrerer aktueller Bücher zum Datenschutzrecht
- **Erfahrungen** in:
  - Wissenschaft (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 junges 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 den besten Partnern auf nationaler und internationaler Ebene.

DIE TECHNISCHE DIMENSION DER DATENSCHUTZ-GRUNDVERORDNUNG

- Art 24: „Verantwortung des für die Verarbeitung Verantwortlichen“
- Art 25 und Art 32: Gemeinsamkeiten und Unterschiede
- Art 32: Sicherheit der Verarbeitung
- Art 25 Abs 1: Datenschutz durch Technikgestaltung (Privacy by Design)
- Art 25 Abs 2: Datenschutz durch datenschutzfreundliche Voreinstellungen (Privacy by Default)
- Art 22: Automatisierte Entscheidungen im Einzelfall einschließlich Profiling

Die technische Dimension der Datenschutz-Grundverordnung

- Art 24: „Verantwortung des für die Verarbeitung Verantwortlichen“
- Art 25 und Art 32: Gemeinsamkeiten und Unterschiede
- Art 32: Sicherheit der Verarbeitung
- Art 25 Abs 1: Datenschutz durch Technikgestaltung (Privacy by Design)
- Art 25 Abs 2: Datenschutz durch datenschutzfreundliche Voreinstellungen (Privacy by Default)
- Art 22: Automatisierte Entscheidungen im Einzelfall einschließlich Profiling
- Art 17: Recht auf Löschung
- Art 18: Recht auf Einschränkung der Verarbeitung
- Art 20: Recht auf Datenübertragbarkeit

Art 24: „Verantwortung des für die Verarbeitung Verantwortlichen“

- **Eigenverantwortung** und Haftung des Verantwortlichen
- Risikobasierter Ansatz
- Rechenschafts- und Nachweispflicht
- Pflicht zu technischen und organisatorischen Maßnahmen, um sicherzustellen und den Nachweis zu erbringen, dass die Verarbeitung DSGVO-Konform erfolgt
- Pflicht, diese Maßnahmen zu überprüfen und zu aktualisieren
- Nähere Ausgestaltung dieser Pflichten durch
  - Art 25: *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*
  - Art 32: *Sicherheit der Verarbeitung*
  - Art 35: *Datenschutz-Folgenabschätzung*
- Abs 2: Konkretisierung des Verhältnismäßigkeitsgrundsatzes

Art 25 und Art 32: Gemeinsamkeiten und Unterschiede

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 32 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 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; […]"

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

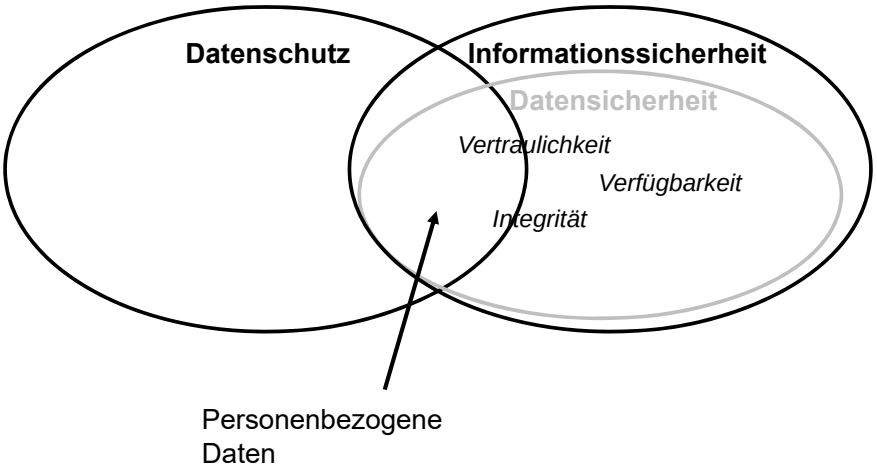
  (vgl Martini in Paal/Pauly (Hrsg), Datenschutz-Grundverordnung, Beck [2017] Art. 25 Rz 39 mwN).
- Es kommt somit auf die praktische Umsetzbarkeit an, nicht aber auf einen bereits weit verbreiteten Einsatz in der Praxis
- Betrifft nicht nur Ausgestaltung einzelner Maßnahmen (zB Auswahl von Verschlüsselungsalgorithmen), 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 32
Sicherheit der Verarbeitung

Verhältnis von Datenschutz und Informationssicherheit



Datensicherheit in der DSGVO

- Sicherheit neu unter den Datenschutzgrundsätzen in Art 5 Abs 1 lit f: „Sicherheit der personenbezogenen Daten“, „Integrität und Vertraulichkeit“
- Wie bisher (§ 14 DSG): Angemessene technische und organisatorische Maßnahmen
- Art 32 nennt ausdrücklich folgende Schutzmaßnahmen:
  - Pseudonymisierung und Verschlüsselung personenbezogener Daten
    - Verpflichtung zur Pseudonymisierung, wenn der konkrete Verarbeitungszweck auch mit pseudonymisierten Daten zu erreichen ist (sofern kein unverhältnismäßig hoher Aufwand)
    - Verpflichtung zur Verschlüsselung der Daten bei Speicherung und Übertragung, außer in begründeten Ausnahmefällen
  - Fähigkeit, folgende Schutzziele auf Dauer sicherzustellen:
    - Vertraulichkeit
    - Integrität
    - Verfügbarkeit
    - Belastbarkeit
  - Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen (Recovery)
  - Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen

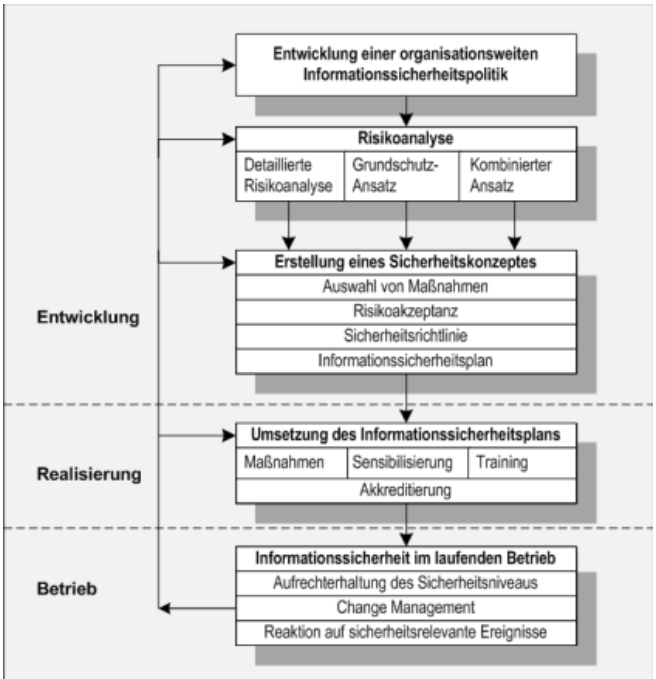
EXKURS: PSEUDONYMISIERUNG

Pseudonymisierung: Von der Option der Privilegierung (DSG: indirekt personenbezogene Daten) zur verpflichtenden Sicherheitsmaßnahme

- Personenbezogene Daten sind zu pseudonymisieren, wenn der konkrete Verarbeitungszweck auch mit pseudonymisierten Daten zu erreichen ist (sofern kein unverhältnismäßig hoher Aufwand)
- Art 4 Z 5:
  „Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten **ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können**, sofern diese **zusätzlichen Informationen gesondert aufbewahrt** werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden“
- Pseudonymisierung ist schwierig: Auch wenn identifizierende Attribute (Name etc.) entfernt werden, kann aus den Daten selbst heraus eine Zuordnung zum Betroffenen möglich sein (zB individuelle medizinische Daten)

INFORMATIONSSICHERHEITS-MANAGEMENT

- „Technische und organisatorische Maßnahmen“: Systematische Organisation erforderlich
- Dokumentation: Teil des Verzeichnisses der Verarbeitungs-tätigkeiten (Art 30 Abs 1 lit g)
- Informationssicherheits-Managementsystem (ISMS) nach ISO/IEC 27000-Normenreihe (ISO/IEC 27001 und 27002)
- ISM als kontinuierlicher Verbesserungsprozess:
  Plan – Do – Check – Act
  (Art 32 Abs 1 lit d), vor allem:
  - Veränderungen des Schutzbedarfs
    - Steigende Datenmengen
    - Neue externe Bedrohungen
  - Veränderungen des Stands der Technik
    - Neue Abwehrmaßnahmen



Quelle: Österreichisches Informationssicherheitshandbuch

Konkrete Maßnahmen (Art 29 Abs 2 DSRL-PJ)

- **Zugangskontrolle**: Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte
- **Datenträgerkontrolle**: Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Entfernens von Datenträgern
- **Speicherkontrolle**: Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten
- **Benutzerkontrolle**: Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte
- **Zugangskontrolle**: Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschließlich zu den ihrer Zugangsberechtigung unterliegenden personenbezogenen Daten Zugang haben
- **Übertragungskontrolle**: Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können
- **Eingabekontrolle**: Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben worden sind
- **Transportkontrolle**: Verhinderung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Daten unbefugt gelesen, kopiert, verändert oder gelöscht werden können
- **Wiederherstellung**: Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können
- **Verfügbarkeit**: Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen, auftretende Fehlfunktionen gemeldet werden
- **Datenintegrität**: Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können

Informationssicherheit: Einige Empfehlungen

- Entscheidend: Feststellen von erfolgten Angriffen (incident detection/intrusion detection)
  - Logs auch tatsächlich auswerten
- Risikofaktor Mensch (Art 32 Abs 4)
  - Verhaltensrichtlinien, Datenverwendung nur wenn für betriebliche Zwecke erforderlich
  - Identity- und Access-Management: Restriktive Zugriffsrechte, jeder soll nur das sehen bzw. ändern können, was notwendig ist
  - Benutzerbezogene Zugriffsprotokollierung (in Einklang mit Arbeitnehmerdatenschutz)
  - Schulungen, Awareness schaffen
- Risikofaktor physischer Zugriff
  - „Gäste“ im Büro
  - Unbeaufsichtigte Geräte in der Öffentlichkeit (auch im Hotelzimmer)
  - „Gefundene“ USB-Sticks nie anstecken
- Einhaltung von Verhaltensregeln (iSv Art 40) und Zertifizierung (iSv Art 42) können als Faktor herangezogen werden, um die Erfüllung nachzuweisen (Art 32 Abs 3)

Art 25 Abs 1
Datenschutz durch Technikgestaltung (Privacy by Design)

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

PRIVACY BY DESIGN BEDEUTET:

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

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

- Gänzlich neue Pflicht (vgl. jedoch bereits die Formulierung in ErwGr 46 DSRL)
- Begriff:
  - DSGVO (EN): „Data Protection by Design“
  - DSGVO (DE): „Datenschutz durch Technikgestaltung“
  - Wissenschaft: „Privacy by Design“
  - eIDAS-VO (EN): „Privacy by Design“
  - eIDAS-VO (DE): „eingebauter Datenschutz“
- **Verhältnismäßigkeitsabwägung** zwischen den Risiken für die Rechte und Freiheiten natürlicher Personen 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

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 seid 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

- 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
- Vision: Privacy by Design als ein standardisierter Prozess im Software Engineering
  Jedoch: Zu ambitioniert und zu pauschal; jedes System ist anders
- Daher: 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.

PRIVACY-DESIGN-STRATEGIEN

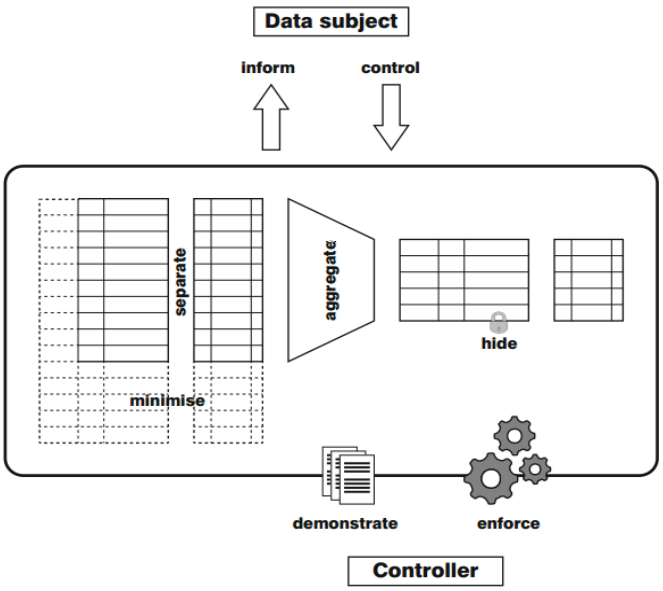
- MINIMISE: Die Menge der verarbeiteten Daten sollte so gering wie möglich sein
- HIDE: Alle personenbezogenen Daten und ihre Zusammenhänge sollten möglichst verborgen bleiben
- SEPARATE: Personenbezogene Daten sollten möglichst verteilt verarbeitet und getrennt gespeichert werden
- AGGREGATE: Personenbezogene 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

PRIVACY-DESIGN-STRATEGIEN

- MINIMISE
- HIDE
- SEPARATE
- AGGREGATE

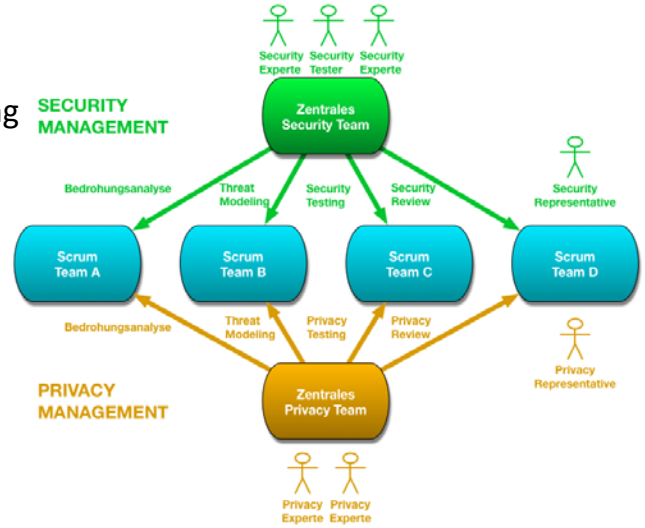
- INFORM
- CONTROL
- ENFORCE
- DEMONSTRATE



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

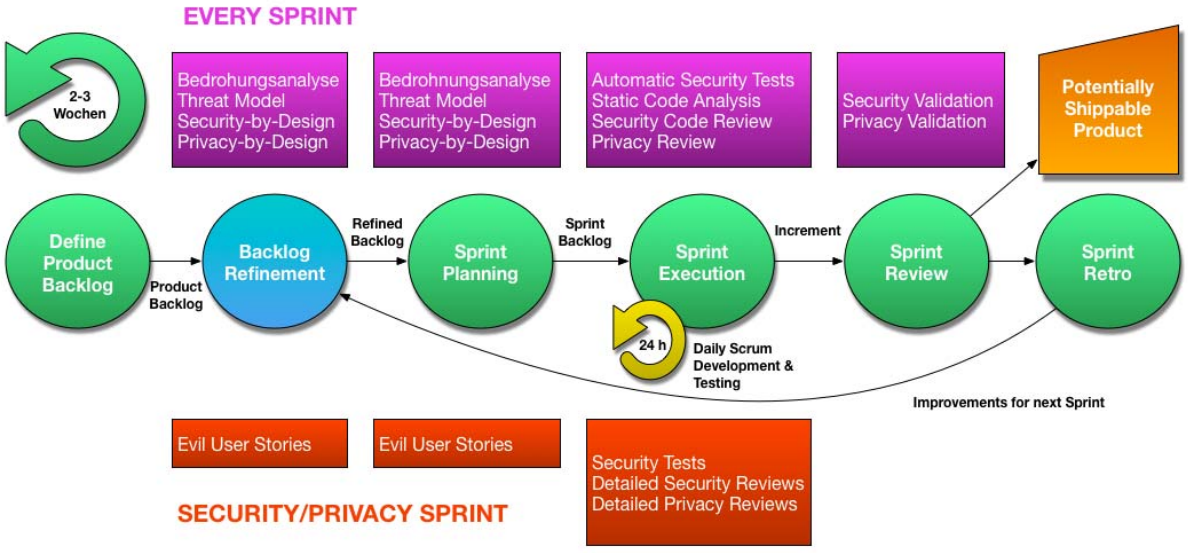
UMSETZUNGSBEISPIEL IN DER SOFTWARE-ENTWICKLUNG

- Ein auf **Scrum** basierender Softwareentwicklungsprozess
- Iterativ-inkrementelle agile Entwicklung
- **Mechanismen zur Umsetzung von Security- und Privacy-Anforderungen:**
  - Abbilden von Privacy- u. Security-Anforderungen
    - Akzeptanzkriterien
    - Definition of Done
    - User Stories
    - Technische User Stories
  - Evil User Stories
  - Statische Code-Analyse
  - Automatisierte Tests
  - Inkrementelle Reviews



Terbu, O., Hötzendorfer, W., Leitner, M., Bonitz, A., Vogl, S., Zehetbauer, S.: Privacy and Security by Design im agilen Softwareentwicklungsprozess. In: *Schweighofer, E., Kummer, F., Hötzendorfer, W., Borges, G.* (Hrsg.): Netzwerke. Tagungsband des 19. Internationalen Rechtsinformatik Symposions IRIS 2016, Österreichische Computer Gesellschaft (OCG), Wien, 2016, 457–464.

UMSETZUNGSBEISPIEL IN DER SOFTWARE-ENTWICKLUNG



Art 25 Abs 2
Datenschutz durch datenschutzfreundliche Voreinstellungen (Privacy by Default)

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 „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

Privacy by Default bedeutet:

Die datenschutzfreundlichsten Einstellungen sind von vornherein ausgewählt, wenn ein Betroffener ein Produkt in Betrieb oder eine Dienstleistung in Anspruch nimmt

Bei Bedarf kann der Betroffene diese Einstellungen dann bewusst ändern

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

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

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 **Prozess**
  - Vor allem auch außerhalb der Rechtsabteilung:
    - IT
    - Entwicklung
    - Beschaffung
  - 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)

Art 22: Automatisierte Einzelentscheidungen/Profiling

- Bisher Art 15 DSRL sowie § 49 DSG
- Definition von Profiling (Art 4 Abs 4):
  - Jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden,
  - um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich
  - Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel
  - dieser natürlichen Person zu analysieren oder vorherzusagen
- Art 22 Abs 1: Die **betroffene Person** hat das Recht, nicht einer **ausschließlich** auf einer **automatisierten Verarbeitung** – einschließlich Profiling – beruhenden Entscheidung unterworfen zu werden, die ihr gegenüber **rechtliche Wirkung entfaltet** oder sie **in ähnlicher Weise erheblich beeinträchtigt**
- Art 22 Abs 2: Ausnahmen
  - Abschluss oder Erfüllung eines Vertrags (zB Pflichten beim Abschluss von Verbraucherkreditverträgen gem Verbraucherkredit-Richtlinie)
  - Ausdrücklich vorgesehen in Rechtsvorschriften der Union oder der Mitgliedstaaten, die angemessene Maßnahmen zur Wahrung der Rechte und Freiheiten sowie der berechtigten Interessen der betroffenen Person enthalten
  - Ausdrückliche Einwilligung der betroffenen Person

Zusammenfassung

- **Eigenverantwortung** und Haftung des Verantwortlichen
- Risikobasierter Ansatz
- Pflicht zu technischen und organisatorischen Maßnahmen, um sicherzustellen und den Nachweis zu erbringen, dass die Verarbeitung DSGVO-Konform erfolgt
- Nähere Ausgestaltung dieser Pflichten durch
  - Art 25: *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*
  - Art 32: *Sicherheit der Verarbeitung*
  - Art 35: *Datenschutz-Folgenabschätzung*
- **Datensicherheit**
  - Neu unter den Datenschutzgrundsätzen in Art 5 Abs 1
  - Art 32 neu gestaltet, aber Anforderungen ähnlich wie bisher
  - Systematische Organisation und Dokumentation erforderlich
  - Verhältnismäßigkeitsabwägung

Zusammenfassung

- Gänzlich neue Pflicht: **Privacy by Design und by Default**
- Verankerung im Unternehmen als **Prozess**
- Einbeziehen von IT, Entwicklung, Beschaffung etc.
- **Privacy by Design:**
  1. Datenschutz bei der Gestaltung von Systemen von Beginn an berücksichtigen
  2. Verhindern der nicht intendierten/nicht zweckkonformen Verwendung des Systems durch technische und organisatorische Maßnahmen
  - Kernelement: **Datenminimierung**
  - **Privacy Engineers** in den Entwicklungsprozess involvieren
  - Umsetzung einiger weniger Grundprinzipien des Datenschutzes
    - von Beginn an
    - individuell auf das jeweilige System und dessen Zweck abgestimmt
- **Privacy by Default:**
  Die datenschutzfreundlichsten Einstellungen sind von vornherein ausgewählt
  - Keine Verhältnismäßigkeitsabwägung

Weiterführende Literatur

- Hörbe/Hötzendorfer, Privacy-by-Design-Anforderungen für das Federated Identity Management, in Jahnel (Hrsg), Jahrbuch Datenschutzrecht [2014], 305–325
- ENISA, Privacy and Data Protection by Design – from policy to engineering, 2014 https://www.enisa.europa.eu/activities/identity-and-trust/library/ deliverables/privacy-and-data-protection-by-design/at_download/full Report
- Gürses/Troncoso/Diaz, Engineering Privacy by Design, Proceedings of Computers, Privacy & Data Protection (CPDP 2011) [2011]
- Spiekermann/Cranor, Engineering Privacy, IEEE Transactions on Software Engineering 2009, 67–82
- Deng et al, A privacy threat analysis framework: Supporting the elicitation and fulfillment of privacy requirements, Requirements Engineering 2011, 3–32
- van Rest et al, Designing Privacy-by-Design, Proceedings of the First Annual Privacy Forum, APF 2012, LNCS, vol 8319 [2014] 55–72;
- Kung, PEARs: Privacy Enhancing ARchitectures, Proceedings of the Second Annual Privacy Forum, APF 2014, LNCS, vol. 8450 [2014] 18–29
- Koops/Leenes, Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law, International Review of Law, Computers & Technology, 28:2 [2014] 159–171
- Hörbe/Hötzendorfer, Privacy by Design in Federated Identity Management, Proceedings of the 2015 IEEE Security and Privacy Workshops [2015] 167–174
- Tsormpatzoudi/Berendt/Coudert, Privacy by Design: From Research and Policy to Practice – the Challenge of Multi-disciplinarity, Proceedings of the Third Annual Privacy Forum, APF 2015, LNCS, vol. 9484 [2016] 199–212

Die technische Dimension der Datenschutz-Grundverordnung

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