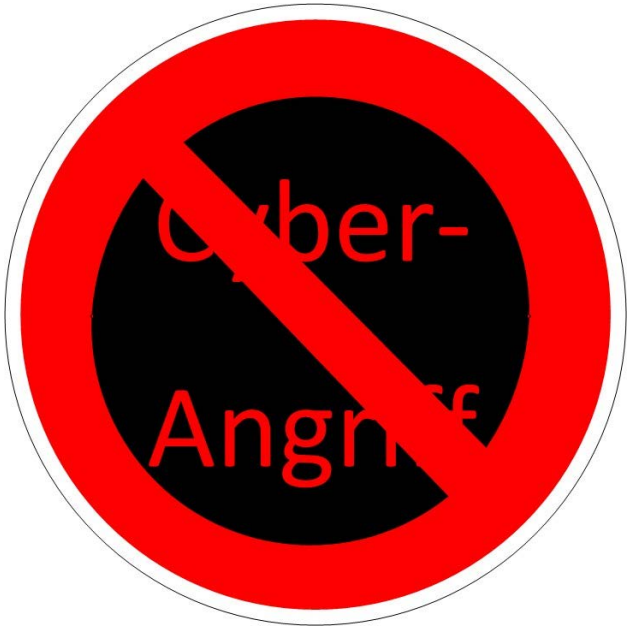

Privacy by Design/Default

Dr. Bernd Schütze

Seminar Datenschutz-Grundverordnung (DS-GVO)

HEALTHCARE SOLUTIONS

Agenda

Worum geht es eigentlich?

- Anforderungen aus Art. 25 DS-GVO
- Stand der Technik
- The 7 Foundational Principles
- Technisch-organisatorische Maßnahmen (TOM)
- Nachweis bzgl. Abwägung Implementierungskosten
- Grundsätzliches Vorgehen

Anforderungen aus Art. 25 DS-GVO

Privacy by Design

Grundsätzliches

- Begriff „Privacy by Design“ wurde 1. Mal von Ann Cavoukian verwendet
- Privacy by Design:
- Konzept, das auf IT-Systeme, Geschäftspraktiken, physikalisches Design und Netzwerkarchitekturen anwendbar ist
- Ziel: Gewährleistung von Datenschutz und die persönliche Kontrolle über die eigenen Daten
- Mittel: Berücksichtigung von Datenschutzaspekten während der Designphase

Art. 25: Privacy by Design/Default

Wer muss sich darum kümmern?

- Normadressat
  - Für die Daten Verantwortliche, nicht Hersteller
- ErwGr. 78

  „[...] sollten die Hersteller der Produkte, Dienste und Anwendungen ermutigt werden, das Recht auf Datenschutz bei der Entwicklung und Auslegung der Produkte, Dienste und Anwendungen zu berücksichtigen“
- Verantwortlicher darf (u.a.) nur Software einsetzen, die Tatbestand erfüllt
  - Keine Pflicht des Auftragsverarbeiters zur Unterstützung
  - Kundenservice?

Art. 25: Privacy by Design/Default

Anforderungen

- Treffen geeigneter technisch-organisatorische Maßnahmen (Art. 25 Abs. 2)
  - zur Umsetzung der Datenschutzgrundsätze

Art. 25: Privacy by Design/Default

Anforderungen: Datenschutzgrundsätze

Artikel 5 „Grundsätze für die Verarbeitung personenbezogener Daten“

- Verarbeitung in nachvollziehbarer Weise
  (= Gewährleistung von Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz)
- Einhaltung der Zweckbindung
- Verarbeitung auf das notwendige Maß beschränken („Datenminimierung“)
- Nur „richtige“ Daten verarbeiten
- Daten löschen, sobald zur Erreichung des Zweckes nicht länger benötigt
  („Speicherbegrenzung“)
- Gewährleistung des Schutzes vor unbefugter oder unrechtmäßiger Verarbeitung sowie vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung („Integrität und Vertraulichkeit“)
- Nachweis der Einhaltung dieser Anforderungen („Rechenschaftspflicht“)

Art. 25: Privacy by Design/Default

Anforderungen

- Treffen geeigneter technisch-organisatorische Maßnahmen (Art. 25 Abs. 2)
  - zur Umsetzung der Datenschutzgrundsätze
  - zur Durchsetzung der Betroffenenrechte
- unter Berücksichtigung (Art. 25 Abs. 1)
  - des Stands der Technik
  - der Implementierungskosten
  - der Art, Umfang, Umstände und Zwecke
  - der Eintrittswahrscheinlichkeiten und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen
- Hinweis: Genehmigtes Zertifizierungsverfahren gemäß Artikel 42 bietet Möglichkeit, Anforderungen nachzuweisen

Art. 25: Privacy by Design/Default

Anforderungen

- [...] 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 [...],
- die dafür ausgelegt sind,
  - die Datenschutzgrundsätze (siehe Art. 5 DS-GVO) [...] 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
- CAVE: Art. 25 enthält im Gegensatz zu Art. 32 keine Beschränkung bzgl. „Angemessenheit“ der Maßnahmen

Art. 25: Privacy by Design/Default

Anforderungen

- „Treffen geeigneter technisch-organisatorische Maßnahmen“

→ Privacy by Design/by Default betrifft sowohl die technische als auch organisatorische Komponenten

→ Anforderung an IT-Systeme

→ Anforderung an die Organisationsabläufe

  - Auch diese müssen entsprechend „designed“ werden

Art. 25: Privacy by Design/Default

Anforderungen

Beschränkung der Verarbeitung durch Voreinstellung auf das Erforderliche:

- Beschränkung auf den oder die Verarbeitungszweck(e)
- Beschränkung der Datenmenge
- Beschränkung des Verarbeitungsumfangs
- Beschränkung der Speicherfristen
- Beschränkung der Zugänglichkeit

Stand der Technik

Stand der Technik

Was versteht man unter „Stand der Technik“?

- Keine Definition bzgl. „Stand der Technik“ in DS-GVO
- Begründung zum IT-Sicherheitsgesetz
  (analog § 3 Abs. 6 Bundes-Immissionsschutzgesetz)
  - „Stand der Technik in diesem Sinne ist der Entwicklungsstand
    - **fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen,**
  - der die **praktische Eignung**
  - einer **Maßnahme zum Schutz der Funktionsfähigkeit** von informationstechnischen Systemen, Komponenten oder Prozessen
  - **gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit** gesichert erscheinen lässt.
  - Bei der Bestimmung des Standes der Technik sind insbesondere einschlägige internationale, europäische und nationale Normen und Standards heranzuziehen, aber auch vergleichbare Verfahren, Einrichtungen und Betriebsweisen, die mit Erfolg in der Praxis erprobt wurden.“

Stand der Technik

Was versteht man unter „Stand der Technik“?

- Bundes-Immissionsschutzgesetz (BImSchG): Überarbeitung 2001 erfolgte, um das Gesetz an geltende europäischen Vorgaben anzupassen
- in § 3 Ziff. 6 BImSchG :„Stand der Technik im Sinne dieses Gesetzes ist der

  Entwicklungsstand fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen, der

  die praktische Eignung einer **Maßnahme**

  zur Begrenzung von [...],

  zur Gewährleistung der Anlagensicherheit,

  zur Vermeidung oder Verminderung von Auswirkungen [...]

  gesichert erscheinen lässt.
- 1:1 Übertragung sicherlich nicht möglich
- Aber man kann ersehen, was der europäische Gesetzgeber mit „Stand der Technik“ adressiert:
  → Im Wesentlichen identisch mit Begründung zum IT-Sicherheitsgesetz

Stand der Technik

Definition

- „fortschrittlicher Verfahren, Einrichtungen oder Betriebsweisen“ mit
- „praktischer Eignung“ bzgl.
- Maßnahmen zum Schutz der Funktionsfähigkeit sowie
- Maßnahmen gegen Beeinträchtigungen der Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit

→ Auch dies adressiert nicht nur technische Komponenten

→ Auch hier werden entsprechende organisatorische Maßnahmen gefordert

Stand der Technik

Normen?

- Normen und Richtlinien: im Prinzip nichts weiter als Empfehlungen privater Vereine (z. B. Deutsches Instituts für Normung, DIN)
- EU-Verordnung 1025/2012 zur europäischen Normung (Art. 2 Nr. 1)
  - Norm: eine von einer anerkannten Normungsorganisation angenommene technische Spezifikation zur wiederholten oder ständigen Anwendung, deren Einhaltung nicht zwingend ist und die unter eine der nachstehenden Kategorien fällt:
    - a) „internationale Norm“: eine Norm, die von einer internationalen Normungsorganisation angenommen wurde
    - b) „europäische Norm“: eine Norm, die von einer europäischen Normungsorganisation angenommen wurde
    - c) „harmonisierte Norm“: eine europäische Norm, die auf der Grundlage eines Auftrags der Kommission zur Durchführung von Harmonisierungsrechtsvorschriften der Union angenommen wurde
    - d) „nationale Norm“: eine Norm, die von einer nationalen Normungsorganisation angenommen wurde

Stand der Technik

Normen?

- Verbindlichkeit der Norm regelt sich durch die Vereinbarung der beteiligten Parteien, für welche die Norm(en) Leistungsgrundlage sein soll
- Normen stellen nicht zwangsläufig eine Regel oder Stand der Technik dar:
  - Anerkannt ist eine Regel dann, wenn Fachleute sie anwenden und sich dabei sicher sind, dass sie dem Stand der Technik entspricht
  - Z. B. kann eine Norm in Deutschland nicht angewendet werden, wenn ein entsprechendes fachliches Gutachten einer qualifizierten Stelle dies begründet
- Ist die Anwendung bestimmter Normen in einem Gesetz vorgeschrieben, so ist deren Einhaltung selbstverständlich auch Pflicht

Stand der Technik

Normen sind hier nicht der Weg ...

„The 7 Foundational Principles“ von Ann Cavoukian, Ph.D.

– Information & Privacy Commissioner
  Ontario, Canada

1) Proactive not Reactive; Preventative not Remedial
2) Privacy as the Default Setting
3) Privacy Embedded into Design
4) Full Functionality – Positive-Sum, not Zero-Sum
5) End-to-End Security – Full Lifecycle Protection
6) Visibility and Transparency – Keep it Open
7) Respect for User Privacy – Keep it User-Centric

The 7 Foundational Principles

The 7 Foundational Principles

1) Proaktiv, nicht reaktiv; als Vorbeugung und nicht als Abhilfe

- Privacy by Design Ansatz ist von proaktiven, nicht von reaktiven Maßnahmen geprägt
- Privacy by Design soll Datenschutzverletzungen verhindern
- Privacy by Design bietet keine Abhilfe, wenn Datenschutzverletzungen eingetreten sind!

The 7 Foundational Principles

2) Datenschutz als Standardeinstellung

- Privacy by Design soll den bestmöglichen Schutz der Privatspäre gewährleisten

→ Zielsetzung

  - Einzelperson muss nichts für den Schutz leisten
  - Schutz ist systemimmanent als Standardeinstellung vorhanden

  → Einzelperson kann den Schutz verringern

The 7 Foundational Principles

3) Datenschutz ist in das Design eingebettet

- Privacy by Design ist in das Design und die Architektur von IT-Systemen und Geschäftspraktiken eingebettet.
- Datenschutz ist ein wesentlicher Bestandteil des Systems, ohne Abstriche bei der Funktionalität.

The 7 Foundational Principles

4) Volle Funktionalität – eine Positivsumme, keine Nullsumme

- Privacy by Design kommt allen berechtigten Interessen und Zielen entgegen
- PbD = Positivsumme: ein zufriedenstellendes Ergebnis für beide Seiten
- **Kein (veralteter) Nullsummenansatz**
  - Datenschutz ist konstruktiver Begleitansatz
  - Datenschutz ist keine Verhinderung!

The 7 Foundational Principles

5) Durchgängige Sicherheit. Schutz während des gesamten Lebenszyklus

- Privacy by Design: von der Ersterfassung bis zum Löschen
- Wirkung von PbD muss den gesamten Lebenszyklus der Daten umfassen!

The 7 Foundational Principles

6) Sichtbarkeit und Transparenz – Für Offenheit sorgen

- Privacy byDesign gibt allen Beteiligten Sicherheit.
- Einzelne Komponenten und Verfahren bleiben sichtbar und transparent; gleichermaßen für Nutzer und Anbieter.

The 7 Foundational Principles

7) Wahrung der Privatsphäre der Nutzer: Für nutzerzentrierte Gestaltung sorgen

- Privacy by Design fordert:
  - Interessen der Einzelpersonen stehen an erster Stelle!

Technisch-organisatorische Maßnahmen (TOM)

Technisch-organisatorische Maßnahmen (TOM)

Berücksichtigung Artt. 5, 32

Wahrung Datenschutzgrundsätze, d. h. per „Voreinstellung“ grundsätzlich nur Verarbeitung

- für den jeweiligen bestimmten Verarbeitungszweck
- nur die Menge an Daten und
- den Verarbeitungsumfang
- unter Beachtung der erforderliche Speicherfrist
- und wahren nur der erforderlichen Zugänglichkeit

→ Anforderungen von Art. 5 einhalten

→ Sicherheit der Verarbeitung gefordert (Art. 32)

Nachweis bzgl. Abwägung Implementierungskosten

Berücksichtigung Implementierungskosten

Nachweispflichten erfordern Begründung

- Art. 25 DS-GVO Abs. 1

  „Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und [...]“
- Maßnahmen zur Gewährleistung der IT-Sicherheit sind bzgl. Wirtschaftlichkeit zu bewerten
  - Controlling der IT-Sicherheit gefordert
- Cave: Es müssen trotzdem „geeignete Maßnahmen“, die den Anforderungen der DS-GVO zu genügen (Art. 25 Abs. 1 DS-GVO)
  - Falls eine Maßnahme auf Grund von Implementierungkosten nicht durchgeführt wird und dadurch den Anforderungen der DS-GVO nicht genügt wird, kann die Verarbeitung nicht durchgeführt werden

Berücksichtigung Implementierungskosten

Return on Security Investment (RoSI)

- Return on Security Investment (RoSI)
  - Kennzahl bzgl. der Rentabilität einer IT-Sicherheitsmaßnahme
- Kosten eines pot. Eintretenden Sicherheitsvorfalls vs. Kosten der IT-Sicherheitsmaßnahme

Berücksichtigung Implementierungskosten

RoSI: Vorgehen

1) Bestimmung des zu erwartenden jährlichen Verlust (Annual Loss Expectancy, ALE)
   - ALE:= Produkt aus der finanziellen Höhe (Loss, L) und der Eintrittswahrscheinlichkeit (Probability, P) des potentiellen Schadens
   - $ALE_{tot} = \sum_{i=1}^{n} L_i \cdot P_i$
   - Finanzieller Verlust, z.B.
     - Umsatzeinbußen, z.B. durch Ausfall eines Shopsystems
     - Produktivitätskosten, wenn beispielsweise durch den Ausfall Produkte nicht weiterentwickelt werden können
     - Wertverlust, z.B. durch Imageschaden
     - Wiederherstellungskosten
     - Schadensersatzleistungen, z.B. gegenüber betroffenen Personen
     - Sanktionsmaßnahmen, wie z.B. von Aufsichtsbehörden verhängte Bußgelder

Beispiel Bestimmung ALE: Ausfall Mail-Gateway bei Denial-of-Service-Attacke (Erwartete Ausfälle pro Jahr: 2)

ALE: Berechnung

Kostenart	Kosten
Wiederherstellungskosten:	
– externer Berater (4 Stunden, Stundensatz 250 Euro)	1.000,00 €
Umsatzeinbußen:	
– 0,5 Aufträge /Stunde Ausfall (pro Auftrag ~ 5.600 Euro)	11.200,00 €
Produktivitätskosten:	
– 12 Beschäftigte im Marketing (Ausfall 4 Stunden, Stundenlohn 18,60 Euro)	892,80 €
– Fax statt Mailbestätigung für eingegangene Aufträge (25 x, Kosten je Fax 0,10 Euro)	2,50 €
Kosten einmaliger Ausfall:	13.095,30 €

Berücksichtigung Implementierungskosten

RoSI: Vorgehen

1) Bestimmung des zu erwartenden jährlichen Verlust (Annual Loss Expectancy, ALE)
2) Bestimmung Kosten für die Implementierung einer Schutzmaßnahme (und Festlegung des Betriebszeitraums)
   - Konzeptionskosten, z.B.
     - Entwicklung bzw. Auswahl der Lösung, Testbetrieb, Anpassungen an die eigene Infrastruktur
   - Investitionskosten, wie beispielsweise
     - Anzuschaffende Hardware, Software, Schulungskosten, Installation/Konfiguration
   - Betriebskosten, Kosten für Support. Lizenzkosten, usw.

Beispiel Bestimmung ALE: Ausfall Mail-Gateway bei Denial-of-Service-Attacke (Schutzmaßnahmen, Betriebszeitraum 3 Jahre)

ALE: Berechnung

Kostenart	Kosten
Konzeptionskosten:	
– Interne Mitarbeiter (40 Stunden, Stundensatz 25 Euro)	2.000,00 €
– externer Berater (4 Stunden, Stundensatz 250 Euro)	
Investitionskosten:	
– 2 Server (je 4.500 Euro)	9.000,00 €
– IDS-Lösung (2.300 Euro)	2.700,00 €
• Schulungskosten (16 Stunden, Stundensatz 25 Euro)	
– Anti-Spam-Lösung incl. Real-Time-Protection (1.800 Euro)	2.200,00 €
• Schulungskosten (16 Stunden, Stundensatz 25 Euro)	
Betriebskosten:	
– IDS	150,00 €
• 150 Euro (Signaturen/Updates)	
– Anti-Spam-Lösung	450,00 €
• 450 Euro für 100 User	

Berücksichtigung Implementierungskosten

RoSI: Vorgehen

1) Bestimmung des zu erwartenden jährlichen Verlust (Annual Loss Expectancy, ALE)
2) Bestimmung Kosten für die Implementierung einer Schutzmaßnahme (und Festlegung des Betriebszeitraums)
3) Berechnung der Gesamtkosten der Sicherheitsmaßnahmen (Total Cost of Ownership, TCO)
   - Einmalkosten werden über den Betriebszeitraum abgeschrieben, d.h.

$$TCO = \frac{Konzeptionskosten + Investitionskosten}{Betriebszeitraum} + Betriebskosten$$

Beispiel Mail-Gateway:

$$TCO = \frac{2.000 + 13.900}{3} + 600 = 5.300 + 600 = 5.900€$$

Berücksichtigung Implementierungskosten

RoSI: Vorgehen

1) Bestimmung des zu erwartenden jährlichen Verlust (Annual Loss Expectancy, ALE)
2) Bestimmung Kosten für die Implementierung einer Schutzmaßnahme (und Festlegung des Betriebszeitraums)
3) Berechnung der Gesamtkosten der Sicherheitsmaßnahmen (Total Cost of Ownership, TCO)
4) Berechnung RoSI
5) Betrachtung ALE-Wert vor und nach Einführung der IT-Sicherheitsmaßnahmen

$$RoSI = \frac{(ALE_{alt} - ALE_{neu}) - TCO}{TCO}$$

Berücksichtigung Implementierungskosten

RoSI: Vorgehen

Ausfall Mail-Gateway bei Denial-of-Service-Attacke
(Schutzmaßnahmen (Betriebszeitraum 3 Jahre)

1) ALE (Alt): 2 Ausfälle je 13.095,30 = 26.190,60 €
2) TCO: 5.900,00 €
3) ALE (Neu): 1 Ausfall je 13.095,30 = 13.095,30

$$RoSI = \frac{(26190{,}60 - 13095{,}30) - 5900{,}00}{5900{,}00} = \frac{7195{,}30}{5900{,}00} \sim 1{,}22$$

Berücksichtigung Implementierungskosten

RoSI: Vorgehen

1) Bestimmung des zu erwartenden jährlichen Verlust (Annual Loss Expectancy, ALE)
2) Bestimmung Kosten für die Implementierung einer Schutzmaßnahme (und Festlegung des Betriebszeitraums)
3) Berechnung der Gesamtkosten der Sicherheitsmaßnahmen (Total Cost of Ownership, TCO)
4) Berechnung RoSI
5) Bewertung:
    a) Erwartete Ersparnis beim ALE-Wert ($ALE_{Alt} - ALE_{neu}$) liegt über den Anschaffungs- und Betriebskosten: wirtschaftlich sinnvoll
    b) Erwartete Ersparnis beim ALE-Wert ($ALE_{Alt} - ALE_{neu}$) liegt unter den Anschaffungs- und Betriebskosten: wirtschaftlich nicht sinnvoll

Privacy by Design: Grundsätzliches Vorgehen

Privacy by Design

Modellvorschlag

Grundgedanke

- Ausrichtung der Verarbeitung am Betroffenen
- Fragen beantworten:
  - Was hat der Betroffene von der Verarbeitung?
  - Welchen Nutzen zieht der Betroffene aus der Verarbeitung?
  - Ist der Nutzen größer als (potentiellen) Schaden?
  - Kann der Betroffene (jederzeit) aktiv agieren? D.h. Einfluss auf die Verarbeitung nehmen?
  - Erfolgt die Verarbeitung transparent?

Privacy by Design

Modellvorschlag

- Auftragsorientiert:
  - Dabei werden Daten explizit für einen bestimmten Zweck erhoben und eine weitere Verarbeitung geschieht nur in dessen Rahmen
  - Zweckbindung wird von Erhebung bis Löschung beibehalten
- Prinzip der Datensparsamkeit umsetzen
  - Nur erforderliche, notwendige Daten verarbeiten
  - Nach Möglichkeit Anonymisieren oder wenigstens pseudonymisieren
  - Nach Möglichkeit nur temporär speichern
- Gesamte Verarbeitung: Wahrung der Verhältnismäßigkeit
  - Verarbeitung für Zweck: geeignet, erforderlich, kein existierendes milderes Mittel

Privacy by Design

Modellvorschlag

- Berechtigungskonzept umsetzen
  - Datenverwaltung/Datenzugriff entsprechend „Need-to-know“
  - Datenminimierung für den jeweiligen Verarbeiter
  - Wenn möglich: Personenbezogenheit der Daten erst bei Eintritt Ereignis
- Wahrung Betroffenenrechte
  - Rechte der Betroffenen beachten
  - Einschränkung der Rechte nur bei entsprechenden Allgemeininteresse
- Datensicherheit gewährleisten
  - Anforderungen Art. 32 DS-GVO aus Sicht des Betroffenen realisieren
- Keine automatisierte Einzelentscheidung

Privacy by Design

Literatur

- Ann Cavoukian: Privacy by Design - The 7 Foundational Principles
  https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
- Ann Cavoukian: Privacy by Design: Strong Privacy Protection - Now, and Well into the Future
  https://www.ipc.on.ca/wp-content/uploads/Resources/PbDReport.pdf
- Federal Trade Commission: Fair Information Practice Principles
  https://web.archive.org/web/20090205180646/http://ftc.gov/reports/privacy3/fairinfo.shtm
- Federal Trade Commission: Privacy Online: Fair Information Practices in the Electronic Marketplace: A Federal Trade Commission Report to Congress
  https://www.ftc.gov/reports/privacy-online-fair-information-practices-electronic-marketplace-federal-trade-commission
- OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data
  http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm;
  Update der Guidelines 2013 unter "OECD work on privacy" (http://www.oecd.org/sti/ieconomy/privacy.htm bzw. The OECD Privcy Framework inkl. Guidelines unter http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf)
- enisa: Privacy Enhancing Technologies (https://www.enisa.europa.eu/topics/data-protection/privacy-enhancing-technologies)
- enisa: Privacy and Data Protection by Design (https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/)
- enisa: Privacy by design in big data (https://www.enisa.europa.eu/publications/big-data-protection/)
- Jaap-Henk Hoepman: Privacy Design Strategies (https://www.cs.ru.nl/J.H.Hoepman/publications/pdp-sec.pdf)
- Jaap-Henk Hoepman: Privacy and Data Protection by Design - from policy to engineering (https://www.cs.ru.nl/J.H.Hoepman/publications/pbd-enisa.pdf)
- Jaap-Henk Hoepman: Privacy by Design - Strategies & Patterns (Presentation, https://www.cs.ru.nl/J.H.Hoepman/presentations/pds-2013.pdf)