Privacy wird zum gesetzlich vorgeschriebenen Design-Prozess

Was tun für die EU-DSGVO geforderte Technikgestaltung?

Dr. Thomas Liedtke, Kugler Maag CIE GmbH

Am 25. Mai 2018 tritt die neue EU-Datenschutz-Grundverordnung [EU-DSGVO] in Kraft. Datenschutz ist dann europaweit gesetzlich einheitlich geregelt. Präambel 78, Artikel 25 und andere der neuen EU-DSGVO fordern explizit „Datenschutz durch Technikgestaltung" und „datenschutzfreundliche Voreinstellungen". Insbesondere werden Data Protection by Design und Data Protection by Default gefordert. Der Einsatz von Datenschutz-Maßnahmen wie z.B. Pseudonymisierung und Anonymisierung personenbezogener Daten werden verpflichtend vorgegeben. Der Stand der Technik bei der Entwicklung und Gestaltung von technischen Produkten ist im gesamten Entwicklungslebenszyklus sicherzustellen. Dieses Paper gibt einen Überblick über verschiedene Prinzipien und Methoden in unterschiedlichen Projekt-Entwicklungsphasen. Privacy by Design (PbD), Privacy Principles und Privacy Enhancing Techniques (PETs) werden erläutert. Zur Berücksichtigung des Datenschutzes sind Privacy-spezifische Schutzziele (Predictability, Manageability, Disassociability) zu erfüllen. Diese Schutzziele leiten sich nicht unbedingt aus den klassischen Schutzzielen der Security ab. Am Ende des Papers werden Standards zur Durchführung von Privacy Risiko Analysen vorgestellt.

Motivation und neue Verordnungen

Um Entwicklungsziele Safety, Security und Privacy für Produkte und Systeme zu erreichen, sind – trotz Ähnlichkeiten - zur Entwicklungszeit unterschiedliche Methoden und Maßnahmen anzuwenden.

Das bzgl. Privacy wichtigste einzuhaltende Gesetz ist die ab 25. Mai 2018 europaweit (Marktortprinzip) geltende EU Datenschutzgrundverordnung (kurz: EU-DSGVO, im englischen GDPR (General Data Protection Regulation)) [EU-DSGVO]. Im Erwägungsgrund 78, sowie in mehreren Artikeln (z.B. Artikel 25: *Technikgestaltung*, Artikel 32: *Sicherheit der Verarbeitung*, Artikel 24: *Verantwortung des für die Verarbeitung Verantwortlichen*) werden dazu Anforderungen an die Gestaltung technischer Systeme gestellt. Wesentliche Forderungen sind:

- *Privacy by Default* (PbD): Datenschutzfreundliche Voreinstellungen/ sichere Konfigurationen
- Kontextabhängige Berücksichtigung des „Stand der Technik"
- Mitverantwortung des Herstellers technischer Systeme

Zeitgleich wird das Bundesdatenschutzgesetz [BDSG] durch seine neue Fassung, das Datenschutz-Anpassungs- und -Umsetzungsgesetz EU [DSAnpUG-EU] ersetzt.

Gleichzeitig soll eine inhaltlich noch in Diskussion befindliche ePrivacy-Verordnung über Privatspähre und elektronische Kommunikation wirksam werden [ePrivacy]. Auch das IT-Sicherheitsgesetz [IT-SIG] mit der BSI-KritisVerordnung [BSI-KritisV] wird in den nächsten Jahren das Thema Privacy mehr und mehr in den Blickpunkt bei der Entwicklung Daten- und Informations-getriebener Systeme und Anwendungen rücken. Die Verantwortung bzgl. der Einhaltung von Datenschutz-Vorgaben hat nicht mehr alleine der Anwender.

Die EU-DSGVO formuliert in mehreren Artikeln das wie folgt: *„… Entwicklung… unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art des Umfangs, der Umstände und der Zwecke der Verarbeitung der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen…“*.

Eine Bedeutung der Formulierung *Stand der Technik* findet man z.B. beim Bundesverband IT Sicherheit e.V. 2016 [TTT16].

Schon 1973 wurden sogenannte FIPPs (Fair Information Practice Principles) [DoH73] zur Wahrung von Bürgerinteressen bei der rechnergestützten Speicherung personenbezogener Daten aufgestellt.

Diese noch heute gültigen und in Standards häufig berücksichtigten Prinzipen sind: Zugriff und Änderungsmöglichkeiten für Betroffene, Verantwortlichkeit, Befugnis, Minimierung der Speicherung personenbezogener Daten auf das gesetzlich Notwendige und nur zu den gesetzlich vorgesehenen Zwecken, Qualität und Integrität der Daten, Einbezug der Betroffenen, Zweckbestimmung und Nutzungslimitierung, Schutz vor unautorisierten Zugriff und Transparenz.

Privacy Enhancing Techniques

Ann Couvokian beschrieb 2011 [Cav11, Hoe14] sieben „*foundational Principles*“ für die Berücksichtigung von Privacy, die wie die FIPPs in vielen Gesetzen und Standards zu finden sind:

- *Proaktiv statt reaktiv*: Datenschutzanforderungen müssen von Entwicklungsbeginn an (proaktiv) berücksichtigt werden.
- *Datenschutz als Standard (PbD)*: sichere Standardkonfigurationen, keine Standardzugänge, opt-in statt opt-out, …
- *Einbettung des Datenschutzes im Design,* nicht als „Add-on“
- *Keine Nullsumme sondern volle Funktionalität*: Die Einhaltung des Datenschutzes muss die Funktionalität einer Anwendung erhalten, sie darf ihr nicht entgegen wirken

- *Schutz über den gesamten Lebenszyklus.* Wichtiger Teil heutiger Standards und Regelungen.

- *Sichtbarkeit und Transparenz*: Ermöglicht die Ausübung von Rechten der Benutzer.

- *Respekt:* vor dem Datenschutz von Nutzern, Anwendern und Betroffenen

Die ENISA beschreibt entsprechende Strategien [ENISA14] in ihrem *Privacy und Data Protection by Design Report* und unterscheidet in Daten- und Prozessorientierte Strategien.

Ein weiterer Schlüsselfaktor bzgl. des Designs eines Systems ist die Annahme über das Vertrauen. Beispiele sind *Blind Trust, Verifiable Trust, Verified Trust Amounts* und *Distributed Trust*.

Beispiele für Datenorientierte Strategien sind:

- *Minimise: select before you collect; anonymisation and use pseudonyms:* Die Menge personenbezogener Daten die erhoben, gespeichert und verarbeitet wird, muss auf ein Minimum beschränkt und auf den Zweck der Verarbeitung limitiert werden. Das anlasslose Sammeln personenbezogener Daten ohne vorherige Zweckbestimmung und Zweckbindung und ohne Abwägung des Erforderlichkeitsgrundsatzes widerspricht der informationellen Selbstbestimmung der Betroffenen und damit dem Datenschutz.

- *Hide: encryption of date; mix networks; unlink certain related events; anonymisation; pseudonyms:* zielt auf das Schutzziel Vertraulichkeit (Confidentiality) ab.

- *Separate:*Daten müssen getrennt gehalten werden, Tabellen über mehrere Datenbanken verteilt werden. Auf ID's ist zu verzichten, Datenverarbeitung soll lokal erfolgen. Über die Zwecke hinausgehende Auswertungen personenbezogener Daten sollen nicht ermöglicht werden

- *Aggregate: aggregation over time; dynamic location granularity; k-anonymity; differential privacy; …:* Wann immer einzelne Daten zur Zweckerfüllung nicht (mehr) benötigt werden, müssen diese z.B. zeitlich (s. Streamingdaten/ Smart Meter) oder ortsgebunden (s. Staumeldungen) zusammengefasst werden. Die Verarbeitung erfolgt auf oberster Verdichtungsebene bei geringstmöglicher Detailtiefe

Beispiele für Prozessorientierte Strategien sind:

- *Inform: privacy preferences platform P3P; data breach notifications, …:* betrifft sowohl die Transparenz der Verarbeitung bzgl. Art der

Information (Zweck, welche Mittel) als auch den Informationsschutz wie der Zugriff Dritter

- *Control: User-centric identity management; end-to-end encryption support control:* Ist das Gegenstück zu *Inform*. Rechte können nur bei entsprechender Transparenz eingefordert werden.
- *Enforce: access control; Datenschutzmanagement; Digitales Rechtemanagement; Lizenzen.*
- *Demonstrate: Datenschutzmanagementsysteme; Protokolle; Audits.*

Privacy Enhancement Techniques (sog. PETs) sind Datenschutz-fördernde (datenschutzfreundliche) Techniken, die den Datenschutz in Informations- und Kommunikationssystemen soweit wie möglich fördern und durchsetzen, zumindest aber unterstützen.

„Privacy Enhancing Technologies are a coherent system of ICT measures that protects privacy [...] by eliminating or reducing personal data or by preventing unnecessary and/or undesired processing of personal data; all without losing the functionality of the data system.“ (Wikipedia)

Eine nicht abschließende Sammlung wichtiger PETs findet sich ebenfalls im ENISA-Report [ENISA14]:

- *Authentifizierung*: Client-Server-Authentifizierung, Ende-zu-Ende-Authentifizierung, Identity Access Management, Single Sign On
- *Attribute Based Credentials:* anonymous credentials, ABC
- *Sicherung privater Kommunikation:* Kryptorafie, Ende-zu-Ende-Verschlüsselung, …
- *Datenschutz beim Speichern:* Verschlüsselung (FDE, FSE, FPE, …)
- *Datenschutz erhaltendes Verarbeiten:* Homomorphic Encryption (PH, RSA, FHE, SHE, ElGamal, …)
- *Anonymität und Pseudonymität:* Kritisch sind z.B. anfallende Metadaten aus denen tatsächliche Identitäten ermittelt werden können. Dies betrifft sowohl Sender als auch Empfänger: Proxies, VPN, Onion Routing, …
- *Datenschutz in Datenbanken:* Verhinderung der Re-Identifikation von Betroffenen. Keine Offenlegung von Abfrageergebnissen, Verhinderung von Profiling und Re-Identifikation in interaktiven Abfragen von Benutzern
- *Statistical Disclosure Control (SDC):* Datenschutz von Betroffenen bei statistischen Auswertungen (Attribut & Identität)

- *Datenschutzkonformes Data Mining (PPDB):* Keine Rückschlüsse aus Analyseergebnissen [GIL16]. Kryptografie, PPDM Protokoll, Knowledge Hiding

- *Private Informatoin Retrieval (PIR):* Standalone Relaxations, Multi-Party Relaxations: anonymes Routing,

- *Transparancy Enhancing Techniques:* Verständnis der Betroffenen, welche Daten über sie gespeichert sind und wie sie genutzt werden. Siegel und Logos.

- *Interveniability Enhancing Techniques:* Möglichkeit für Betroffene einzugreifen. Kontrollierbarkeit. Vertrauensbildung.

Zielkonflikte | Privacy Risikobegriff

Privacy-Schutzziele sind keine Untermenge von den Security-Schutzzielen. Das NIST [NIST8062] definiert hierzu eigene Privacy-Schutzziele:

- *Predictability*: Betroffene, Eigentümer und Betreiber können verlässliche Vorhersagen über personenbezogene Daten und ihre Verarbeitung durch das System machen

- *Manageability*: Fähigkeit personenbezogene Daten granular zu administrieren (ändern, löschen, lesen, …)

- *Dissaciability*: Verarbeitung von personenbezogenen Daten ohne Assoziierung zu Betroffenen über die operationalen Anforderungen des Systems hinaus

Es gibt Security Issues die nichts mit Privacy zu tun haben, genauso umgekehrt Privacy Issues, die nichts mit Security zu tun haben. Während der Verlust von Security und seinen wichtigsten Schutzzielen (z.B. Confidentiality, Integrity, Availability) ursächlich durch unauthorisiertes Systemverhalten hervorgerufen wird, wird der Verlust von Privacy und seinen oben genannten Schutzzielen (z.B. Dissaciability) als Nebenprodukt autorisierter Verarbeitung verursacht. Privacy kann hierbei sowohl zu Safety als auch Security im Zielkonflikt stehen.

Es gibt eine ganze Reihe von Standards in Bezug auf Security und Privacy Risikoanalysen wie z.B. die BSI [BSI200-3]. Auf Privacy speziell ausgerichtet ist die ISO29134 [ISO29134] *Privacy Impact Assessment*, welche im Wesentlichen mit der Vorabkontrolle des BDSG vergleichbar ist. Eine zur ISO 27005 [ISO27005] und IEC 62443 [IEC62443-3-2] sehr ähnliche Vorgehensweise ist in der NIST 8062 [NISTIR8062]: *An introduction to Privacy Engineering and Risk Management* beschrieben.

Das Risiko wird hier als Funktion von Auswirkung – wenn ein Ereignis auftritt – und der Wahrscheinlichkeit seines Auftretens definiert. Während bei einer Security

Risiko Analyse Bedrohungen (die durch ihre Angreifbarkeit ausgenutzt werden können) betrachtet werden, sind es in der Privacy Risiko Analyse problematische Daten Aktionen, welche Bedrohungen darstellen. Problematische Datenaktionen können hierbei sein: sammeln, aufbewahren, analysieren, transformieren, offenlegen, zusammenführen, …

Summary

Die Berücksichtigung von Privacy-Belangen bei der Entwicklung technischer Systeme wird durch die EU-DSGVO und ePrivacy gesetzlich vorgeschrieben. *Privacy by Design*, *Privacy Enhancing Techniques*, *Privacy Engineering* sind von Entwicklungsbeginn an anzuwenden. Verschiedene Standards geben Prozesse für Privacy Risiko-Analysen vor.

Privacy wird zum Attribut von technischen Systemen.

Literatur

[BDSG] *Bundesdatenschutzgesetz.* Link: https://www.gesetze-im-internet.de/bdsg_1990/

[BSI-KritisV] *Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz* (BSI-Kritisverordnung). Link https://www.gesetze-im-internet.de/bundesrecht/bsi-kritisv/gesamt.pdf

[BSI200-3] BSI-Standard 200-3: *Risikoanalyse auf der Basis von IT-Grundschutz*

[Cav11] *Privacy by Design - The 7 Foundational Principles*; Ann Cavoukian. Published January 2011 by the Information and Privacy Commissioner of Ontario. Link: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf

[DoH73] *Records Computers and the rights of Citizens*; Report of the Secretary‘s Advisory Committee on Automated Personal Data Systems. U.S. Department of Health, Education & Welfare. July 1973. https://www.justice.gov/opcl/docs/rec-com-rights.pdf

[DSAnpUG-EU] *Datenschutz-Anpassungs- und –Umsetzungsgesetz*, Gesetzesentwurf Drucksache 110/17 02.02.2017. Link: http://www.bundesrat.de/SharedDocs/drucksachen/2017/0101-0200/110-17.pdf?__blob=publicationFile&v=5

[ePrivacy] *Verordnung über Privatsphäre und elektronische Kommunikation*. Link: https://ec.europa.eu/digital-single-market/en/news/proposal-regulation-privacy-and-electronic-communications

[ENISA14] *Privacy and Data Protection by Design – from policy to engineering*; December 2014 by European Union Agency for Network and Information

Security. Link: https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design

[EU-DSGVO] *EU-Datenschutzgrundverordnung*; Amtsblatt der Europäischen Union L 119. Link: http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=OJ:L:2016:119:FULL&from=DE

[GIL16] *Data-Mining, Privacy Preserving – Einleitung;* GI-Informatiklexikon; eingesehen 13.07.2016; Link: https://www.gi.de/service/informatiklexikon/detailansicht/article/data-mining-privacy-preserving.html

[Hoe14] *Privacy Design Strategies*; Jaap-Henk Hoepmann, 29th IFIP TC 11 International Conference, SEC 2014 Marrakech, Marocoo, June 2-4, 2014 Proceedings p446-459.

[IEC-62443-3-2] *Security for industrial automation and control systems; Security risk assessment for system design*

[ISO27005] *Information Technology – Security Techniques – Information Security Risk Management*

[ISO29134] *Information technology -- Security techniques -- Guidelines for privacy impact assessment*

[IT-SIG] Gesetz zur Erhöhung der Sicherheit informationstechnischer Gesetze vom 17. Juli 2015. Link: https://www.bgbl.de/xaver/bgbl/start.xav?startbk=Bundesanzeiger_BGBl&jumpTo=bgbl115s1324.pdf#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl115s1324.pdf%27%5D__1482241057975

[NISTIR 8062] *An Introduction to Privacy Engineering and Risk Management in Federal Systems*. Information Security U.S. Department of Commerce. Link: http://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf

[TTT16] *Handreichung zum „Stand der Technik" im Sinne des IT-Sicherheitsgesetzes (ITSIG).* TeleTrusT – Bundesverband IT-Sicherheit e.V., 2016 https://www.teletrust.de/publikationen/broschueren/stand-der-technik/

Autor

Dr. rer. nat. Thomas Liedtke (geb. 1966) ist Process Director bei der Kugler Maag CIE GmbH. Seine Hauptarbeitsgebiete sind Projektmanagement, Safety, Security und Privacy, theoretisch, praktisch und in der Lehre. Er ist SCRUM Master, IT-SiBe, bDSB, Mitglied bei der ZVEI Automotive Cybersecurity, VDA Cybersecurity und leitet die GI-AG Privacy-by-Design.

Kontakt

Internet: www.kuglermaag.de
E-Mail: Thomas.Liedtke@kuglermaag.com