Mehr Datenschutz durch Technik?

Die Umsetzung der technikbezogenen DS-GVO-Bestimmungen in der Praxis

«Privacy by design», «Privacy by default», oder das Recht auf «Vergessen werden» sind Kernelemente der Datenschutzgrundverordnung. Ihre technische Umsetzung in der Praxis ist aber nicht einfach.

Vorsprung durch Technik?

Die neue Datenschutzgrundverordnung (DS-GVO) soll helfen, den europäischen Datenschutz an die Realitäten des 21. Jahrhunderts anzupassen. Als die aktuell geltende Datenschutzdirektive 95/46/EC Anfang der Neunziger Jahre konzipiert wurde, steckte das World Wide Web noch in den Kinderschuhen: gerade einmal knapp 3000 Web Sites zählte man 1994[1] – seit März 2016 sollen es weit über 1 Milliarde sein. Ähnliche Fortschritte gab es seitdem auch bei den Mobiltelefonen: das erste internetfähige Mobiltelefon wurde erst 1996 vorgestellt (der Nokia Communicator 9000), heute werden weltweit über 6 Exabytes (6 Millionen Terabytes) pro Monat per Mobiltelefon bewegt.[2] Und nicht zuletzt wurde das Zeitalter der «Apps» erst 2007 mit dem iPhone eingeläutet, heute gibt es jeweils über 2 Millionen mobile Applikationen auf den beiden populärsten Plattformen[3] (iOS und Android). Grund genug, bei der Revision des europäischen Datenschutzes nicht nur der rasanten technologischen Entwicklung Rechnung zu tragen, sondern sich auch die Entwicklungen beim technikbezogenen Datenschutz, also dem «Datenschutz *durch* Technik» (statt «Datenschutz trotz Technik») direkter als bisher einzubeziehen. So finden sich in der finalen Version der DS-GVO eine Vielzahl an Referenzen auf entweder neue technische Herausforderungen an den Datenschutz, als auch auf neue Möglichkeiten, durch Technik Datenschutz zu unterstützen. Somit stellen sich zwei Arten von Fragen: Inwieweit sind die Antworten, die die DS-GVO auf die neuen technologischen Herausforderungen bietet, praktikabel? Und wie weit können heutige Technologien helfen, Datenschutz praktisch umzusetzen?

Datenschutz durch Technik: PETs

Die Idee, dass dank Technologie ein besserer Datenschutz möglich sein kann, wurde im Oktober 1995 – nur wenige Tage vor der Veröffentlichung der EU Datenschutzdirektive – erstmals präsentiert. John Borking, damals Mitarbeiter des holländischen Datenschutzbeauftragen, erläuterte an der 17. Konferenz der Datenschutzbeauftragten in Kopenhagen in seinem Vortrag «Back to Anonymity – Privacy Enhancing Technologies» die Vision einer nicht nur datenschutzfreundlichen, sondern datenschutz*ermöglichenden* Technik. Damit begründete Borking eine völlig neue Forschungsrichtung, eben die der «Privacy Enhancing Technologies», oder kurz «PETs», deren Flagschiff-Konferenz – das im Jahr 2000 gegründete «Privacy Enhancing Technologies Symposium» – in diesem Jahr bereits zum 17. Mal stattfinden wird.

Privacy-Enhancing Technologies

Borkings Ursprungsidee einer Privacy Enhancing Technology war sein «Identity Protector» (Borking 1998) – ein System, welches

[1] http://www.internetlivestats.com/total-number-of-websites/

[2] https://www.statista.com/statistics/271405/global-mobile-data-traffic-forecast/

[3] https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/

Marc Langheinrich (2017). Mehr Datenschutz durch Technik? Die Umsetzung der technikbezogenen DS-GVO-Bestimmungen in der Praxis. Digma. 17. Jahrgang, Heft 1, März 2017, pp. 14-19

es Nutzern ermöglichte, bei der Interaktion mit digitalen Diensten auf «Pseudoidentitäten» zurückzugreifen. Statt seiner wahren (bzw. vollständigen) Identität würde ein Nutzer einen Dienst jeweils mit einem Pseudonym nutzen, welches es dem Dienst verunmöglicht, den Nutzer zu identifizieren. Der Protector erstellte dabei Pseudoidentitäten dynamisch und nutzte sie in transparenter Weise, d.h. der Nutzer bemerkte davon idealerweise nichts.

Das Konzept des Identity Protectors demonstriert eines der Kernanliegen von PETs: Datenminimisierung und Anonymität. Weitere PET-Themen sind beispielsweise Transparenz (z.B. der P3P-Standard, Cranor et al. 1999), Datenbanken (z.B. Zugriffskontrolle, Datenaggregation), Daten-Lifecyclemanagement (z.B. «Sticky Policies», Mont et al. 2003) und vermehrt auch die Nutzbarkeit von Datenschutztechnik.

Von PET zu Privacy by Design (PbD)

Mitherausgeber von Borkings an der Kopenhagener Konferenz vorgestellten Studie war Ann Cavoukian, die damalige Datenschutzbeauftragte des Staates Ontario in Kanada. Aus Borkings Ansatz heraus entwickelte Cavoukian später die Idee des «Privacy by Design» (Cavoukian, 2009). Sieben Grundsätze sollten es Unternehmen ermöglichen, die personenbezogenen Daten ihrer Kunden datenschutzfreundlich zu verwenden:

1. Proactive not reactive; preventive, not remedial
2. Privacy as default setting
3. Privacy embedded into design
4. Full functionality
5. End-to-end security – full lifecycle security
6. Visibility and transparency – keep it open
7. Respect for user privacy – keep it user-centric

Während Cavoukian's holistischer Ansatz, der neben dem IT Systemen selbst auch Geschäftspraktiken sowie das Design von Geräten bzw. Applikationen miteinschliesst, durchaus erahnen lässt, welche Aspekte für eine von Cavoukian angestrebte «win-win / positive-sum» Entwicklung im Datenschutz wichtig sind, so bleibt die Aufzählung konkrete Lösungsansätze jedoch schuldig. Wie lässt sich «full functionality» ohne Einbussen am Datenschutz konkret umsetzen? Was bedeuted «user-centric privacy»? Und wie integriert man «privacy» in der Praxis in das Design eines Systems?

Technik und DS-GVO

Die neue Datenschutzgrundverordnung will «Datenschutz durch Technik» viel konkreter in die Gesetzgebung mit einbeziehen. In ihren 99 Artikeln und 173 Erwägungsgründen finden sich eine Vielzahl von direkten und indirekten Referenzen auf «Privacy Enhancing Technologies» bzw. «Privacy by Design». Doch wie leicht lassen sich diese Anforderungen in der Praxis umsetzen? Exemplarisch seien im Folgenden fünf Artikel herausgegriffen.

Artikel 25: «Privacy by Design»

Unter Artikel 25 verlangt die DS-GVO einen «Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen» (im Englischen «Privacy by Design and privacy-aware defaults»). Doch Cavoukian's «Privacy-by-Design» lässt sich nur schwer direkt umsetzen. Eine praktischere Anleitung wurde 2015 von der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) entwickelt (Danezis et al. 2015). Die Autoren identifizieren acht Kernstrategien:

1. Minimize – die Menge an gesammelten personenbezogenen Daten sollte so gering wie möglich sein.
2. Hide – personenbezogene Daten sollten nicht direkt zugreifbar sein («not in plain view»).
3. Separate – personenbezogene Daten sollten wann immer möglich verteilt (d.h. in getrennten Datencontainern) bearbeitet werden.
4. Aggregate - personenbezogene Daten sollten auf einem höchstmöglichen Aggregationsniveau bearbeitet werden, d.h. mit so wenig Detail wie möglich.
5. Inform – Datensubjekte sollten ausreichend informiert werden.
6. Control – Datensubjekte sollten Kontrolle («agency») über die Bearbeitung ihrer personenbezogenen Daten behalten.

7. Enforce – eine rechtlich einwandfreie Datenschutzerklärung sollte vorhanden und umgesetzt werden.
8. Demonstrate – die Einhaltung des Datenschutzes sollte für Datensubjekte überprüfbar sein («demonstrate compliance»)

Die acht Grundsätze lassen sich mehr oder weniger direkt in korrespondierende PETs übersetzen. So bieten Identitätsmanagementsysteme (z.B. PrimeLife[4]) eine verbesserte Kontrolle, während «Privacy Labels» (Kelley et al. 2009) bzw. «Sticky Policies» jeweils die Präsentation und automatisierte Umsetzung von Datenschutzregeln ermöglichen. Dennoch bleiben zwei Kernprobleme: zum einen gibt es eine Vielzahl von PETs aber kaum etablierte bzw. standardisierte Verfahren, zum anderen sind viele der Technologien kaum ausserhalb einzelner Forschungsprojekte erprobt und sind daher nur selten im grossen Rahmen einsetzbar.

Darüber hinaus ist unklar, wer für das Vorantreiben von «Privacy by Design» überhaupt verantwortlich ist. Entwickler von Datenverarbeitungssystemen selbst sehen sich gemäss Umfragen kaum in der Pflicht (Lahlou et al. 2005, Szegely 2013), während im betriebswirtschaftlich orientierten Management oft nur ein minimales Bewusstsein in Bezug auf die technischen Anforderungen und Möglichkeiten besteht. Nicht zuletzt fehlt in aktuellen Softwareentwicklungsprozessen eine klare Verortung des «Privacy-by-Design» Prozesses – auch wenn einige Veröffentlichungen zum «Privacy Engineering» in den letzten Jahren dieses Problem zu adressieren versuchen (z.B. Oliver 2014, Dennedy et al. 2014, Bowman et al. 2015).

Artikel 20: Recht auf Datenübertragung

Artikel 20 erteilt Datensubjekten das Recht, ihre personenbezogenen Daten in einem «strukturierten, gängigen und maschinenlesbaren Format» zu erhalten. Die Idee ist, dass Nutzer so leicht ihren Dienstanbieter wechseln können (z.B. von Facebook zu Google «zügeln»). Absatz (2) des Artikels verlangt sogar, dass Anbieter diesen Wechsel direkt anbieten, d.h. ohne Umweg (Download und anschliessender Upload) des Nutzers, «soweit dies technisch machbar ist».

«Technisch machbar» ist dies prinzipiell sehr wohl. «Gängige maschinenlesbare Formate» gibt es zuhauf: eine einfache Textdatei (oft mit der Endung .txt gekennzeichnet) würde diesem bereits entsprechend, ebenso Bilddateien (z.B. im Jpeg Format), HTML-Seiten, oder auch sogenannte «CSV-Dateien» (Comma Separated Values). Doch genügt dies bereits, um die gewünschte Datenportabilität zu gewährleisten? Bereits heute können interessierte Nutzer sich eine digitale Kopie ihres gesamten Facebook Datensatzes herunterladen – als ein Archiv (ZIP) mehrer HTML Seiten, die in Tabellen die vom Nutzer eingestellten Informationen (Texte und Bilder im JPG-Format) beinhalten. Doch wie soll man diese Daten nun auf einen Konkurrenzdienst, sagen wir Google Plus oder auch eine Diaspora[5] Installation, heraufladen? Zu unstrukturiert sind die von Facebook zur Verfügung gestellten Daten, zu verschieden die jeweiligen Informationsfelder der konkurrierenden Dienste.

Um eine reibungslose Datenportabilität zu ermöglichen benötigt es standardisierte Austauschformate, wie es sie z.B. im Gesundheitswesen hat (Stichwort: electronic medical record, EMR). Doch selbst bei so grundsätzlichen Informationen wie Patientendaten gibt es eine Vielzahl konkurrierender Standards (z.B. openEHR[6], SMART[7], xDT[8]) die trotz ihrer relativ klar definierten Informationsmenge untereinander nicht kompatibel sind. Welche Chancen mag hier z.B. eine Standardisierung von «Social Network Data» haben? Sind es nicht gerade die Unterschiede, die es einem Konkurrenzdienst erlauben, Nutzer zum Wechsel zu bewegen? Wie importiere ich meine Facebook «Pokes» in Google Plus? Am Ende bleibt wohl nur der «kleinste gemeinsame Nenner» zum Export/Import übrig (z.B. Name und Geschlecht des Nutzers).

Auch der automatische Datenaustausch, der auf den ersten Blick einfach umsetzbar scheint, wird in der Praxis wahrscheinlich Probleme bereiten. Zwar gibt es auch hier

[4] http://primelife.ercim.eu/
[5] https://www.joindiaspora.com/
[6] http://www.openehr.org/
[7] http://smarthealthit.org/
[8] https://en.wikipedia.org/wiki/XDT

eine grosse Zahl von etablierten Verfahren (Programmierschnittstellen/APIs zur Datenserialisierung), wie zwei unterschiedliche Dienste direkt Daten austauschen können (z.B. Google's «Protocol Buffers»[9], Apache's «Avro»-Format[10], oder die Web Services Description Language WSDL[11] des W3Cs), doch werden direkte Konkurrenten am Markt sich wohl kaum bemühen, ihre Daten für den jeweils anderen Dienst zugreifbar zu machen – wer kann schon sagen, ob dies «technisch machbar» ist? Im besten Falle werden Drittanbieter hier eine Marktnische finden, zwischen verschiedenen Diensten diesen Datenaustausch zu ermöglichen. Schon heute gibt es zahlreiche «Web2.0»-orientierte Firmen, die es Nutzern ermöglichen, verschiedenste Services zu kombinieren (z.B. Zapier[12]).

Artikel 17: «Recht auf Vergessenwerden»

Das infolge des Urteils des Europäischen Gerichtshofs (EuGH)[13] vom 13. Mai 2014 bestehende Recht auf Löschung von Verweisen (Links) auf «veraltete» personenbezogene Informationen findet in der DS-GVO in Artikel 17 «Recht auf Löschung ('Recht auch Vergessenwerden')» seine Entsprechung. Der Artikel etabliert zum einen in Absatz 1 einen Löschanspruch für personenbezogene Daten (nicht nur Verweise darauf), sofern die Daten nicht mehr notwendig sind, zum anderen in Absatz 2 eine Informationspflicht des Verantwortlichen, sofern die zu löschenden personenbezogenen Daten öffentlich gemacht wurden. In diesem Falle muss der Verantwortliche all diejenigen über den Löschanspruch informieren, die einen Link auf bzw. eine Kopie der Daten selbst besitzen.

Die Löschung personenbezogener Daten sollte bei der Verwendung moderner Datenbanktechnologie leicht zu implementieren sein. Integrierte «Privacy Management» Systeme können hier eine feingranulare Handhabung der Löschanfrage ermöglichen, indem jeweils nur jene Daten gelöscht werden, die für den jeweiligen (nicht mehr notwendigen) Zweck erhoben wurden. Etwas schwieriger mag sich die in Absatz 2 verlangte Informationspflicht gestalten. Sollten die Daten z.B. auf einer Webseite veröffentlich worden sein, so scheint es nahezu unmöglich, zum Zeitpunkt der Löschanfrage herauszufinden, wer möglicherweise noch Kopien dieser Daten bereithält. Ein Wissen um diejenigen, die eine Kopie der personenbezogenen Daten haben könnten, bedingt praktisch eine nichtöffentliche (d.h. registrierungspflichtige) Bereitstellung. Diese ist jedoch nicht von Absatz 2 erfasst. Einzig ein «passives» Informieren ist denkbar, indem beim erneuten Abrufen der nun gelöschten personenbezogenen Daten z.B. ein «410 Gone» HTTP-Fehlercode[14] gesendet wird. Dies kann jedoch nur diejenigen informieren, die die nun gelöschten Daten zum ersten Mal bzw. erneut abrufen.

Artikel 16: Sachliche Richtigkeit

Das Recht auf Berichtigung (Artikel 16) ist nicht neu: auch die bisher geltende EU Datenschutzdirektive 95/46 EC räumt Betroffenen Berichtigungsrechte ein (Artikel 10 und 11). Die Umsetzung dieses Rechts wird allerdings in Zukunft immer schwieriger werden. Dies liegt an der zunehmenden Sammlung und Nutzung von sogenannten «hochdimensionalen» Datensätzen. Während in den frühen 90er Jahren personenbezogene Datensätze meist lediglich einige dutzend Merkmale einer Person erfassten (z.B. Name, Adresse, Geburtsdatum, Einkommen), so brachte die Nutzung von Webdiensten bereits eine Explosion des Datenvolumens in Form von individuellen Webseiteninteraktionen. Schnell konnten bei einem kurzen Besuch einer Webseite tausende von «Klicks» in einem persönlichen Nutzerkonto anfallen. Heutige Technik erlaubt es hingegen, pro Nutzer hunderte von Merkmalen (z.B. Puls, Ortsinformation, aktuelles Lied) mit jeweils tausenden von Werten pro Tag aufzuzeichnen. Würde man z.B. jene Merkmale, gesammelt über die letzten 12 Monate, einem Nutzer zur Berichtigung falscher Werte vorlegen, wäre es kaum vorstellbar,

[9] https://github.com/google/protobuf
[10] http://avro.apache.org/
[11] https://www.w3.org/TR/wsdl20/
[12] https://zapier.com/
[13] http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-05/cp140070de.pdf
[14] https://de.wikipedia.org/wiki/HTTP-Statuscode#4xx_.E2.80.93_Client-Fehler

hier eine seriöse Prüfung vorzunehmen. Ohne Computeralgorithmen, die solche Zeitreihen-Rohdaten auf Anomalien oder Regelmässigkeiten hin untersuchen, ist eine Fehlerprüfung praktisch nicht möglich. Erst wenn ein solcher Algorithmus beispielsweise einen schlanken Nutzer aufgrund seiner Pulsuhrdaten als übergewichtig klassifiziert, mag es auffallen, dass das jeweilige Gerät seit mehreren Wochen inkorrekte Werte liefert. Komplexere Inferenzen, welche z.B. auf «Deep Learning» Algorithmen beruhen, lassen womöglich gar nicht mehr erkennen, aufgrund welcher Daten eine bestimmte Klassifizierung vorgenommen wurde. Und wie würde der Nutzer den Verantwortlichen von der Unrichtigkeit der erhobenen Daten überzeugen können? Was bei einer falschen Adresse oder einem inkorrekten Betreibungseintrag recht eindeutig nachzuweisen ist, stellt z.B. bei Telemetriedaten einer im Auto eines Junglenkers eingebauten Black Box eine juristische Herausforderung dar: wie kann ich beweisen, dass die von der Box gemeldeten Beschleunigungswerte zu hoch sind?

Selbst wenn es einem Nutzer gelingt, fehlerhafte Zeitreihendaten erst zu identifizieren und anschliessend den Verantwortlichen davon zu überzeugen, dass diese tatsächlich fehlerhaft sind, bleibt kaum die Möglichkeit einer Korrektur: fehlerhaft aufgezeichnete Daten sind verlorene Daten. Niemand kann nachträglich sagen, wie hoch meine tatsächliche Beschleunigung bzw. mein tatsächlicher Puls war, sollte ein Sensor fehlerhaft sein. Hier scheint eine Löschung der Daten der einzige Ausweg – womöglich kann dies aber Nachteile für den Nutzer bringen, sollte das Sammeln der Daten belohnt werden (z.B. Versicherungsrabatte für verantwortungsbewusstes Fahren über einen längeren Zeitraum hinweg).

Artikel 5.c: Datenminimierung

Ein auch im Privacy-by-Design wichtiger Grundsatz ist die Datenminimierung: was nicht erst gesammelt wird, kann auch nicht zum Problem werden. Dies spielt vor allem bei Randdaten (d.h. Metadaten, wie z.B. Telefonverbindungsdaten) eine grosse Bedeutung. Diese fallen quasi automatisch als technisches Nebenprodukt moderner Informationstechnologie an und werden von den meisten Kommunikationsanbietern intensiv zur Wartung und Optimierung der technischen Infrastruktur aufbewahrt. Um hier dem Datenschutzgrundsatz der Datensparsamkeit Genüge zu tun, ohne auf das Wartungspotenzial dieser Daten verzichten zu müssen, kommen oft Anonymisierungsverfahren zur Anwendung. So werden beispielsweise IP Adressen oft durch ein zufälliges Pseudonym ersetzt. Auch medizinischen Datenbanken, die oft zum Zwecke der medizinischen Forschung anonym veröffentlich werden, werden durch das Entfernen personenbezogener Daten (Name, Adresse) oft anonymisiert, ohne aber beispielsweise Details zu Diagnose und Wohnort zu entfernen.

Was auf den ersten Blick anonym wirkt kann womöglich aber nachträglich de-anonymisiert werden. In 2002 analysierte MIT Doktorandin Latanya Sweeney eine anonymisierte medizinische Datenbank der GIC-Gruppe im US-amerikanischen Bundestaat Massachusetts. Durch Abgleich der anonymisierten Daten mit einem öffentlichen Wählerverzeichnis konnte sie jedoch die medizinischen Daten des damaligen Gouverneurs von Massachusetts eindeutig darin identifizieren. Dieses grundlegende Prinzip – der Abgleich von anonymisierten Daten mit einer kleinen, nicht-anonymisierten Datenmenge – kann prinzipiell jede mehr oder weniger detaillierte Datensammlung de-anonymisieren. So konnte de Montjoye et al. (2015) mit Informationen von nur drei Kreditkarteneinkäufen die gesamte Kreditartenhistorie aus einem anonymisierten Datensatz von über 1 Millionen Konsumenten mit über 90%iger Sicherheit reidentifizieren. Ebenso gelang es de Montjoye et al. (2013), mit lediglich vier ungefähren «Sichtungen»[15] eines Natelnutzers, dessen gesamte Bewegungshistorie aus einem anonymen Datensatz von über 1.5 Millionen Nutzern herauszufiltern. Andere erfolgreich de-anonymisierte öffentliche Datensätze sind

[15] D.h. dem Wissen um vier Orte, an denen sich ein Nutzer zu einer bestimmten Zeit ungefähr aufhielt.

z.B. der pseudonymisierte Netflix Datensatz aus 2008 (Narayanan und Shmatikov 2008) oder die anonymisierten 173 Millionen Fahrten von Taxifahrern in New York City[16]. Experten bezweifeln inzwischen, ob sich Daten grundsätzlich anonymisieren lassen (Ohm 2009, Narayanan et al. 2015).

Fazit

Auch wenn die DS-GVO zeitgemässer als die vor über 20 Jahren verabschiedete EU Datenschutzdirektive ist, so ist ihre Umsetzung in der Praxis keineswegs trivial. Zwar nimmt die DS-GVO viele Möglichkeiten der aktuellen Technik auf und zwingt Datenverarbeiter so, das allgemeine Datenschutzniveau auf das heute «technisch machbare» anzuheben. Doch damit sich dies auch wirklich in knapp einem Jahr praktisch umsetzen lässt, ist noch viel Vorarbeit nötig.

Herausforderungen

Die Kernherausforderungen liegen in vor allem beim Umsetzen effektiver Entwicklungsprozesse, die «Privacy-by-Design» technisch und organisatorisch umsetzen können. Auch mangelt es trotz intensiver Forschung auf dem Gebiet der PETs an Standards und «Best Practices», die den Einsatz von komplexen Lösungen, die über Kommunikations- und Datenverschlüsselung hinausgehen (z.B. «Sticky Policies» oder Identitätsmanagement), für Datenverarbeiter praktisch ermöglichen. Gerade im Zeitalter von «Big Data» und «Open Data» ist es beunruhigend, dass die Wissenschaft noch keine Klarheit hat, welche Daten sich wann und wie dauerhaft anonymisieren lassen.

Implikationen für Verantwortliche und Datenverarbeiter

Verantwortliche und Datenverarbeiter müssen schnellstmöglich Prozesse anstossen, um ihre Datenverarbeitung an einem «Privacy-by-Design»-Prozess zu orientieren. Die in Artikel 35 DS-GVO geforderte Datenschutz-Folgenabschätzung («Privacy Impact Assessment») ist hier ein wichtiger erster Schritt, für den bereits umfassende Dokumentation sowie breite praktische Erfahrung existieren (Wright 2012). Eine Schulung von Management und IT-Mitarbeitern im «Privacy Engineering» (z.B. Bowman et al. 2015) ist wohl ebenfalls unabdinglich, selbst ohne eigene Softwareentwicklung.

Implikationen für Betroffene

Zwar räumt die DS-GVO Nutzern umfassende Informations- und Partizipationsrechte ein, doch wann (ob?) hier etwas «technisch machbar» ist, wird von aussen nur schwer abzuschätzen sein. Es bleibt zu hoffen, dass vor allem Anbieter von Softwarelösungen (z.B. CRM-Software) und Onlinediensten (z.B. Google, Facebook) hier bald direkt nutzbare Lösungen im Programm haben werden. Womöglich können auch Drittanbieter hier eine Nische finden, indem sie Nutzer bei dem Zugriff und der Visualisierung/Analyse ihrer von Datenverarbeitern gesammelten Daten unterstützen.

Kurz & bündig

Vieles was in der neuen Datenschutzgrundverordnung gefordert wird, scheint «technisch möglich», doch in der Praxis gestaltet sich deren Umsetzung womöglich schwierig. Das Konzept des «Privacy-by-Design» ist schwer fassbar und noch kaum in organisatorischen bzw. entwicklungstechnischen Prozessen verankert. Auch sind viele der in der Wissenschaft vorgeschlagenen technischen Datenschutzansätze noch kaum in der Praxis erprobt. Verantwortliche und Datenverarbeiter müssen gut abschätzen, welche Aspekte sie wie organisatorisch und technisch umsetzen. Nutzer werden die umfangreichen Informations- und Partizipationsrechte der DS-GVO wohl erst nutzen können, wenn Software- und Onlineserviceindustrie erste mit technischem Datenschutz integrierte Produkte anbieten können.

[16] https://tech.vijayp.ca/of-taxis-and-rainbows-f6bc289679a1#.1741sm9x4

Literatur

- BORKING, J. Einsatz datenschutzfreundlicher Technologien in der Praxis. Datenschutz und Datensicherheit, 11, 1998, pp. 636-640.
- BOWMAN, M., GESHER, A., GRANT, J.K., SLATE, D. The Architecture of Privacy: On Engineering Technologies that Can Deliver Trustworthy Safeguards. O'Reilly, 2015
- DANEZIS, G., DOMINGO-FERRER, J., HANSEN, M., HOEPMAN, J.-H., LE METAYER, D., TIRTEA, R., SCHIFFNER, S. Privacy and Data Protection by Design - from policy to engineering, 2015. http://doi.org/10.2824/38623
- DENNEDY, M., FOX, J., FINNERAN, T. The Privacy Engineer's Manifesto: Getting from Policy to Code to QA to Value. Apress, 2014
- KELLEY, P., BRESEE, J., CRANOR, L., REEDER, R.. A "Nutrition Label" for Privacy. SOUPS 2009
- LAHLOU, S., LANGHEINRICH, M., RÖCKER, C. Privacy and trust issues with invisible computers. Comm. of the ACM, 48(3), 59–60, 2005. DOI:10.1145/1047671.1047705
- MONT, M.C., PEARSON, S., BRAMHALL, P. Towards accountable management of identity and privacy: Sticky policies and enforceable tracing services. Proceedings – Intl. Workshop on Database and Expert Systems Applications, DEXA, 377–382, 2003. DOI:10.1109/DEXA.2003.1232051
- DE MONTJOYE Y.-A., RADAELLI L., SINGH V. K., PENTLAND A. S. Unique in the shopping mall: On the reidentifiability of credit card metadata. Science 347 (6221), 536-539. DOI:10.1126/science.1256297, 2015
- NARAYANAN, A., HUEY, J., FELTEN, E. W. A Precautionary Approach to Big Data Privacy, 1–28, 2015. DOI:10.1007/978-94-017-7376-8
- OHM, P. Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization. Imagine (Vol. 57), 2009.
- OLIVER, I. Privacy Engineering. A dataflow and ontological approach. CreateSpace Independent Publishing, 2014
- SZEKELY, I. What Do IT Professionals Think About Surveillance? In C. Fuch et al. (Eds.), Internet and Surveillance. The Challenge of Web 2.0 and Social Media. (pp. 198–219). Routledge, 2011.
- WRIGHT D., DE HERT P. Introduction to privacy impact assessment. In: Privacy Impact Assessment 2012 (pp. 3-32). Springer Netherlands.

Autor

Marc Langheinrich, Prof. Dr., Universität der italienischen Schweiz (USI), Lugano, marc.langheinrich@usi.ch