Dennis-Kenji Kipker

Privacy by Default und Privacy by Design

Die allgegenwärtige Technisierung führt dazu, dass unser Alltag zunehmend von vernetzten, teils hochkomplexen Informations- und Kommunikationssystemen (IuK) geprägt ist. Nicht nur das vernetzte Automobil, sondern auch „Smart Home" und „Smart Meter" („Smart Grid"), „Data Mining", NFC-gestützte Micropayment-Systeme oder der neue, mit RFID ausgestattete biometrische Reisepass sind Beispiele für die Vielzahl unterschiedlicher Anwendungsfelder, in denen IuK-Systeme zum Einsatz kommen.

Umso wichtiger ist es, dass solche IuK-Systeme, die unseren Alltag bestimmen, datenschutzkonform ausgestaltet sind. Der Nutzer muss darauf vertrauen können, dass die grundsätzlichen Datenschutzanforderungen an ein informationstechnisches System von der ersten Nutzung an gewahrt sind und zwar auch dann, wenn die vorgegebenen Werkseinstellungen zunächst nicht geändert werden bzw. die technische Ausgangskonfiguration genutzt wird. Eine solche datenschutzfreundliche Grundeinstellung wird gemeinhin als „Privacy by Default" bezeichnet.[1]

Privacy by Default wiederum kann am besten durch „Privacy by Design" gewährleistet werden, indem bei einem IuK-System, welches personenbezogene Daten verarbeitet, bereits in der Phase seiner Entwicklung proaktiv die mit der späteren Nutzung verbundenen datenschutzrechtlichen Anforderungen berücksichtigt werden. Durch die Implementierung von Datenschutz- und Datensicherheitstechniken zu einem möglichst frühen Zeitpunkt kann von Anfang an ein stimmiges Gesamtkonzept für den Persönlichkeitsschutz eingerichtet werden, ohne dass es aufwändiger, unvollständiger und möglicherweise fehlerbehafteter Nachrüstungen bedarf, um den Erfordernissen eines angemessenen Datenschutzniveaus gerecht zu werden.[2] Beispiele für Privacy by Design umfassen sichere Nutzer-Authentifizierungslösungen, Anonymisierungs- und Pseudonymisierungstechniken, integrierte Verschlüsselungsmethoden, die Begrenzung der Datenverarbeitung auf das unbedingt notwendige Maß (Datensparsamkeit) und speziell für den Bereich der vernetzten Automobile die Trennung von Identifizierungs- und Inhaltsdaten, zum Beispiel bei der Nutzung ortungsbasierter Dienste.[3]

Aus rechtlicher Perspektive ist ein solches Konzept des Schutzes personenbezogener Daten keineswegs neu. Bereits seit 1990 regelt § 9 BDSG, dass von den datenverarbeitenden Stellen sogenannte technische und organisatorische Maßnahmen (TOM) zu treffen sind, die erforderlich sind, um die Ausführung der Vorschriften des BDSG zu gewährleisten. Verwiesen wird dabei auf die Anlage zu § 9 S. 1 BDSG, welche die allgemeinen, vom Gesetz vorgeschriebenen Datensicherheitsanforderungen konkretisiert. Der dort aufgeführte Maßnahmenkatalog bildet einen Bestandteil des BDSG, sodass die TOM stets nur in Verbindung mit der Anlage gesehen werden können.[4] Hier werden Vorgaben zur Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle aufgestellt, darüber hinaus muss die Zweckbindung der Datenverarbeitung technisch und organisatorisch sichergestellt werden.

Stets ist zu beachten, dass der Maßnahmenkatalog zu § 9 S. 1 BDSG nicht abschließend ist, sondern je nach Art der Datenverarbeitung in seiner Anwendung ggf. zu variieren bzw. zu ergänzen ist. Die Gewährleistungsverpflichtung nach § 9 BDSG umfasst dabei auch eine präventive Komponente, welche die Technik- und Verfahrensgestaltung von Beginn an einbezieht.[5] Letztlich wird mit Privacy by Design somit nur das praktisch umgesetzt, was durch § 9 BDSG ohnehin schon seit langem gesetzlich festgeschrieben und allgemein anerkannt ist.

1 Siehe hierzu beispielsweise auch unter https://digitalcourage.de/blog/2014/privacy-default-datenschutz-darf-keine-ausnahme-bleiben (Stand: 06.04.2015).

2 Zu den Erfordernissen von Privacy by Design und möglichen Anwendungsfeldern auch *Schaar*, Identity in the Information Society, August 2010, Vol. 3, Issue 2, pp. 267-274. Detaillierte Anforderungen an das Konzept aufstellend *Cavoukian*, https://www.privacybydesign.ca/content/uploads/2009/08/7foundationalprinciples-german.pdf (Stand: 06.04.2015). Jüngst auch die ENISA, http://www.enisa.europa.eu/activities/identity-and-trust/library/deliverables/privacy-and-data-protection-by-design/at_download/fullReport (Stand: 06.04.2015).

3 Eine solche Lösung wird beispielsweise durch das „Daimler Vehicle Backend" verfolgt, siehe http://www.mercedes-benz.com/de/mercedes-benz/fahrzeuge/personenwagen/s-klasse/die-mercedes-benz-apps-und-live-traffic-information/ (Stand: 06.04.2015).

4 Vgl. *Gola/Klug/Körffer*, in: Gola/Schomerus, BDSG, § 9, Rn. 2.

5 Vgl. *Ernestus*, in: Simitis, BDSG, § 9, Rn. 16.