

Privacy by Design

Datenschutz beginnt mit der Produkt- und Software-Entwicklung

Nicht erst seit PRISM. ist Datenschutz in aller Munde. Die Europäische Union hatte schon seit 2012 eine Reform zur Anpassung und Stärkung des Datenschutzes mit europaweiter Vereinheitlichung geplant, die unter anderem das Konzept Privacy by Design (PbD) zum Schutz personenbezogener Daten vorsieht.

Definition

Viele Unternehmen sehen Datenschutz (Privacy) primär als juristisches und organisatorisches Thema und wählen einen Top-Down Ansatz, um Compliance zu gültigen Gesetzen zu erreichen. Privacy by Design sieht vor, Datenschutz vor allem auch dort zu implementieren, wo personenbezogene Daten gespeichert und verarbeitet werden. Dort, wohin Top-Down-Ansätze häufig noch nicht konsequent vordringen: im Produkt- und Software-Design. So sollen Datenschutz-Probleme in der Praxis verhindert werden. Denn Datenschutz-Vorfälle passieren letztlich durch unsichere Anwendung und Lücken in IT-Systemen und Arbeitsprozessen.



Das Konzept Privacy by Design sieht daher sieben Grundprinzipien vor, die zum Teil bereits implizit im Bundesdatenschutzgesetz enthalten und in der folgenden Abbildung dargestellt sind.

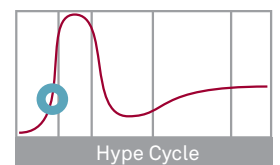
Grundprinzipien Privacy by Design
Proactive, not reactive
Privacy as the Default Setting
Privacy Embedded into Design
Full Functionality and Privacy as a Positive-Sum, not Zero-Sum
End-to-End Security – Full Lifecycle Protection
Visibility and Transparency – Communicated Usage of data
Respect for User Privacy – User is in charge of his/her data

Vor allem das Einbetten von Datenschutz im Produkt- bzw. Systemdesign, Datenschutz als Default-Einstellung und echte, für den Laien verständliche Transparenz und Mitbestimmungsmöglichkeit für Anwender sind zentrale Aspekte von Privacy by Design.

Reifegrad

Privacy by Design wird bislang nur in wenigen Produkten und Systemen konsequent umgesetzt. Vielen Unternehmen fehlen in den Entwicklungsbereichen die nötigen Mitarbeiter mit dem entsprechenden Datenschutzwissen. Die Verantwortung für den Datenschutz wird oft auf Kunden und Anwender übertragen oder der wirtschaftliche Vorteil der Auswertung und Nutzung umfangreicher Personendaten überwiegt.

Daher ist das Thema noch in einer sehr frühen Phase im Hype-Cycle angesiedelt. Der Entwurf der neuen EU-Datenschutz-Grundverordnung beinhaltet bereits Vorgaben für Privacy by Design und wird voraussichtlich ab 2016 für alle Unternehmen verbindlich sein.



Marktübersicht



Privacy by Design ist hauptsächlich durch organisatorische Maßnahmen im Entwicklungsprozess umzusetzen. Unterstützende Technologien und Methoden dafür sind beispielsweise Verschlüsselung, Zugriffs- und Zugangskontrolle, Anonymisierung bzw. Pseudonymisierung und automatisierte Datenlöschung nach einer vereinbarten Frist.

Alternativen

Wirkliche Alternativen zu Privacy by Design gibt es nicht, vorausgesetzt man will „Datenschutzfreundliche“ Produkte und Software entwickeln. Für existierende Systeme kann ein Privacy by Redesign durchgeführt werden. Aus unternehmerischer Sicht sind die Risikoakzeptanz eines Gesetzesverstößes mit Strafzahlungen beim Absehen von Privacy by Design oder u. U. vertragliche Regelungen mit Dritten mögliche Alternativen.

Referenzszenario

Das Konzept Privacy by Design wurde maßgeblich durch die kanadische „Datenschutzbeauftragte“ (Privacy Commissioner) von Ontario, Dr. Ann Cavoukian, mit beeinflusst und entwickelt (siehe auch privacybydesign.ca).

Praxis-Beispiele für Privacy by Design sind die Suchmaschine ixquick, die keine IP-Adressen von Benutzern speichert, oder auch Data Warehouse Systeme, die z. B. Data Mining nicht bis auf Einzelperson-Ebene ermöglichen, sondern nur bis auf Cluster mit mehr als zehn Personen, und zusätzlich auch keinen Export von Listen mit Einzelpersonen erlauben.

Business Impact

Die EU sieht vor, mit Inkrafttreten der neuen Datenschutz-Grundverordnung (voraussichtlich 2016) Strafen von bis zu 2 Prozent des weltweiten Unternehmensumsatzes bei vorsätzlichen Datenschutz-Verstößen einzuführen. Jedoch wird sich noch herausstellen, in wie weit dies in vollem Umfang auch für Verstöße gegen Privacy by Design zutrifft, da ein gewisser Interpretationsspielraum bleibt. Dennoch kann langfristig der Schutz personenbezogener Daten zu einem echten Wettbewerbsvorteil für alle Unternehmen werden, weil Kunden und Anwender beginnen, Datenschutzfreundliche Produkte zu fordern und Datensammelwütigen Unternehmen den Rücken zuzukehren.

Pro	Contra
Echte Reduktion des Risikos von rufschädigenden Datenschutzvorfällen	Fehlendes Datenschutz-Wissen und -Bewusstsein bei Managern, IT-Leitern und Entwicklern
Das Vertrauen der Kunden wird gestärkt – somit entsteht ein Wettbewerbsvorteil	Das Geschäftsmodell von datenanalysierenden Unternehmen wie Facebook und Google ist gefährdet
Compliance zu Gesetzen und Regulierungen	Aufwand und Kosten, ohne kurzfristig ersichtlichen Nutzen

msg systems ag

Robert-Bürkle-Straße 1 | 85737 Ismaning/München
 Telefon: +49 89 96101-0 | Fax: +49 89 96101-1113
www.msg-systems.com | info@msg-systems.com

