Aktuelle Informationen zu Corona / Covid-19 finden Sie hier.

Privacy by design / Privacy by default

Standardmäßiger Datenschutz für mehr Privatsphäre

In Zeiten der Digitalisierung steigt die Menge erfasster Daten sowie datenverarbeitender Anwendungen stetig. Dies führt wiederum dazu, dass die Wahrung eines angemessenen Persönlichkeitsschutzes maßgeblich von der jeweiligen Technikgestaltung abhängt. Im Hinblick auf die Gestaltung von Systemen, angefangen von der Produktentwicklung bis hin zu ihrer Implementierung, wurden daher bereits in der Vergangenheit zunehmend die Ansätze Datenschutz durch Technik („privacy by design“) und datenschutzfreundliche Voreinstellungen („privacy by default“) thematisiert.

Was sagt die Datenschutzgrundverordnung (DSGVO)

Mit dem Inkrafttreten der Datenschutz-Grundverordnung (DSGVO) im Mai 2016 haben diese Gestaltungsprinzipien nun auch ihren gesetzlichen Niederschlag gefunden (vgl. Art. 24, 25 DSGVO). Die Berücksichtigung von "privacy by design" und "privacy by default" ist damit kein Nice-to-have mehr. Vielmehr handelt es sich um eine explizite Anforderung an die Entwicklung und Implementierung von Produkten zur Verarbeitung personenbezogener Daten, mit dem Ziel, das Prinzip der Datenvermeidung und Datensparsamkeit in Verarbeitungssystemen wirksam umzusetzen. Oder anders gesagt: Damit der Datenschutz nicht von der technischen Entwicklung abgehängt wird, sind Produkte/ Systeme frühzeitig um angemessene Datenschutzfunktionen zu ergänzen, so dass das Risiko datenschutzkritischer Entwicklungen, welche unmittelbar aus der Nutzung technischer Systeme resultieren, von vornherein verringert wird (z. B. durch frühzeitige Pseudonymisierung der Daten).

Empfehlungen, inwiefern, d. h. mit welchen Strategien Datenschutz im Wege von „privacy by design“ in Produkten und Systemen verankert werden kann, hat die Europäische Agentur für Netz- und Informationssicherheit (ENISA) im Hinblick auf die DSGVO bereits in einem Bericht vom Dezember 2014 veröffentlicht. Die Umsetzungsmöglichkeiten spiegeln sich dabei in den folgenden acht Strategien wider:

1. MINIMISE

Bei diesem Punkt geht es um die Forderung nach Datensparsamkeit. Es sollen also keine oder zumindest keine unnötigen personenbezogenen Daten gesammelt und ihre Verarbeitung auf ein Minimum beschränkt werden. Wichtig ist daher also immer die Beantwortung der Frage, ob die Verarbeitung personenbezogener Daten zur Erreichung des jeweiligen Zwecks erforderlich ist oder ob dieser nicht auch auf anderem Weg erreicht werden kann.

2. HIDE

Der Grundgedanke dieser Strategie ist es, einem Missbrauch personenbezogener Daten in der Form entgegen zu

wirken, dass diese schlicht nicht mehr zur Kenntnis genommen werden können. Ziel ist dabei die Schaffung von Unverfolgbarkeit, Unbeobachtbarkeit sowie Unverknüpfbarkeit. An dieser Stelle spielen also beispielsweise die Pseudonymisierung und Anonymisierung personenbezogener Daten eine entscheidende Rolle.

3. SEPARATE

Diese Empfehlung bezieht sich auf eine verteilte Datenhaltung, sprich Daten zu einer Person sollen möglichst an verschiedenen Orten gespeichert und verarbeitet werden. So kann die Erstellung umfassender Profile verhindert werden.

4. AGGREGATE

An dieser Stelle geht es darum, dass personenbezogene Daten so früh wie möglich zu Gruppen zusammengefasst werden sollten. Die Rückschlussmöglichkeiten auf einzelne Personen können so minimiert bzw. gänzlich ausgeschlossen werden.

5. INFORM

Dieser Punkt spiegelt den datenschutzrechtlichen Grundsatz der „Transparenz“ wider. Wenn Personen ein System verwenden, so sollen sie darüber informiert werden, welche Daten über sie gesammelt werden, zu welchem Zweck und mit welchen Technologien. Auch sind sie darüber zu informieren, wie die Daten geschützt werden und ob eine Datenweitergabe an Dritte erfolgt. Ferner ist von Bedeutung, dass sie über ihre Datenzugriffsrechte informiert werden und wie sie diese ausüben können.

6. CONTROL

Hier geht es um den Aspekt, dass Personen die Kontrolle über diejenigen Daten behalten sollen, welche über sie gesammelt werden. Faktoren wie z. B. die Bearbeitung von Datenschutzeinstellungen über Benutzeroberflächen sowie eine insgesamt benutzerzentrierte Gestaltung spielen dabei eine maßgebliche Rolle.

7. ENFORCE

Es sollte eine den rechtlichen Anforderungen entsprechende Datenschutzrichtlinie, sprich ein Regelwerk zum Schutz der Privatsphäre der betroffenen Personen vorhanden sein, die auch faktisch umgesetzt wird. Dies impliziert zumindest, dass geeignete technische Schutzmechanismen vorhanden sind, die Verletzungen der Daten verhindern.

8. DEMONSTRATE

Bei dieser Strategie geht es darum, den Nachweis darüber zu führen, wie datenschutzrechtliche Vorgaben effektiv in das IT-System implementiert worden sind. Diese Strategie geht damit also einen Schritt weiter als die ENFORCE-Strategie.

Wurden die datenschutzrechtlichen Anforderungen beim Erwerb von IT-Produkten sowie auch bei werkvertraglichen oder eigenen Individualentwicklungen bislang also eher vernachlässigt, so sind diese nun ausdrücklich zu berücksichtigen. Dies gilt umso mehr, da gegenüber der verantwortlichen Stelle nunmehr ein Bußgeld von bis zu 10.000.000 EUR verhängt werden kann (vgl. Art. 83 Abs. 4 a DSGVO), wenn diese sich trotz der Existenz daten-schutzkonformer Alternativen für den Einsatz datenschutzkritischer IT-Lösungen entscheidet.

PRAXISTIPP

- Beachtung von "privaty by design" und "privaty by default" - Grundsätzen bei Einkauf und Gestaltung von IT-Lösungen

- Bestehende IT-Verfahren überprüfen und ggf. Anpassungen der inhaltlich/technischen Gestaltung vornehmen
- Produktanforderungen mit Datenschutz- und IT-Sicherheitsbeauftragten abstimmen