Was ist Data Protection by Design Data Protection by Default?

Was bedeutet «Data Protection by»?

Grundeinstellungen sollen möglichst datenschutzfreundlich sein und **technische Vorkehrungen** müssen personenbezogene Daten bestmöglich schützen.

Jede Person soll darauf vertrauen können, dass grundsätzliche Massnahmen und Vorkehrungen zum Schutz ihrer Privatsphäre bereits getroffen wurden, selbst dann, wenn sie die Grundeinstellungen nicht ändert.

Wer ist davon betroffen?

Die Anbieter von Betriebssystemen und Anwendersoftware, aber auch die Entwickler von App und CRM-Software sowie die Betreiber von Websites und Online-Shops.

Data Protection by Design

Data Protection by Design (Datenschutz durch Technik) umfasst alle funktionellen (Produktedesign), inhaltlichen (Erklärungen, Hinweise) und technischen (Programmierung) Massnahmen zum Schutz von personenbezogenen Daten. Niemand soll ohne das ausdrückliche Einverständnis einer betroffenen Person deren Daten erheben können.

Mit dem Begriff «Design» ist hier nicht das Aussehen eines Produktes gemeint, sondern das, was Software-Entwickler als Produkte-Design bezeichnen, wenn sie über die funktionellen Eigenschaften eines Produktes reden. Das optische Äussere einer Software nennt man «Interface Design».

Anstelle von «Data Protection by Design» wird auch der Begriff «Privacy by Design» verwendet.

Data Protection by Default

Data Protection by Default (Datenschutzfreundliche Voreinstellungen) bedeutet, dass beim Aufstarten eines Betriebssystems, bei der Installation einer App aber auch beim Öffnen einer Website oder eines Online-Shops keine Massnahmen zum Schutz der eigenen Daten getroffen werden müssen. Die Anwendung ist per se datenschutzfreundlich.

Anstelle von «Data Protection by Default» wird auch der Begriff «Privacy by Default» verwendet.

Was bedeutet das für Websites und Online-Shops?

Auch Websites und Online-Shops müssen mit technischen Schutzmassnahmen versehen sein und mit datenschutzfreundlichen Voreinstellungen überzeugen.

Data Protection by Design (Datenschutz durch Technik)

Damit sind diejenigen Massnahmen zum Schutz von Besuchern einer Internet-Präsenz gemeint, die für Surfende auf ihren Bildschirmen meistens nicht erkennbar sind. Dazu gehören:

- TLS-Zertifikat (verschlüsselte Übertragung der Daten von/zum Webserver)
- Schutz der IP-Adresse der Surfenden (IP-Anonymisierung)
- Schutz vor Tracking-Cookies
- 2-Klick Lösungen bei der Einbettung von Like-/Share Funktionen
- No Cookie-Lösungen bei der Einbettung externer Inhalte (z.B. Videos)
- etc.

Data Protection by Default (Datenschutzfreundliche Voreinstellungen)

Damit sind diejenigen Massnahmen gemeint, die unter die gesetzlichen Regeln der Minimierung, des Zweckbezugs und der Anonymisierung von personenbezogenen Daten fallen. Keine Voreinstellung und keine Funktion sollen gegen Treu und Glauben verstossen und Surfende dazu zwingen oder verleiten, ihre Privatsphäre offen zu legen. Dazu gehören:

- Kurze aber verständlich formulierte Datenschutzhinweise bei der Anmeldung zu einem E-Newsletter, bei Online-Formularen oder beim Check-Out in einem Online-Shops
- Keine Verknüpfung von Leistungen mit Gegenleistungen die eine Offenlegung von personenbezogenen Daten erfordert (z.B. Freebie oder PDF-Download nur bei gleichzeitiger Anmeldung als Empfänger des E-Newsletter möglich)
- Bei Anmeldung zum E-Newsletter: Name und Vorname nicht als Pflichtfelder festlegen
- Einfache Möglichkeit, um die erteilte Erlaubnis zur Bearbeitung von personenbezogenen Daten zu widerrufen.
- Einfache Möglichkeit, um «Mein Konto» zu löschen/löschen zu lassen
- etc.

Dieser Bereich betrifft auch firmeninterne Massnahmen in organisatorischer und technischer Hinsicht, zum Beispiel die Prozesse rund um das CRM Customer Relationship Management.