Privacy by Design

Privacy by Design ist ein Konzept für die Entwicklung von Produkten, Diensten und Systemen, bei denen die Privatsphäre des Einzelnen von Anfang an im Vordergrund steht. Dabei werden Überlegungen zum Datenschutz in den Entwurfs- und Entwicklungsprozess integriert, anstatt den Datenschutz als nachträglichen Gedanken zu behandeln.

Das Konzept des „Privacy by Design“ wurde erstmals in den 1990er Jahren von der kanadischen Datenschutzbeauftragten Dr. Ann Cavoukian vorgestellt und wird seitdem von Datenschutzbehörden auf der ganzen Welt aufgegriffen. Die Datenschutz-Grundverordnung (GDPR) verlangt von Organisationen ausdrücklich, geeignete technische und organisatorische Maßnahmen zu ergreifen, um sicherzustellen, dass die Verarbeitung personenbezogener Daten unter Berücksichtigung des Stands der Technik, der Implementierungskosten sowie der Art, des Umfangs, des Kontexts und der Zwecke der Verarbeitung datenschutzgerecht gestaltet wird.

Zu den wichtigsten Grundsätzen des Privacy by Design gehören:

- Proaktiv statt reaktiv: Proaktiv potenzielle Datenschutzrisiken erkennen und angehen, anstatt auf Datenschutzvorfälle zu reagieren, nachdem sie eingetreten sind. Dies kann durch den Einsatz von Risikobewertungen, Folgenabschätzungen und anderen Instrumenten erreicht werden, um potenzielle Datenschutzrisiken frühzeitig zu erkennen.
- Datenschutz als Standardeinstellung: Schutz der Privatsphäre von Anfang an in Produkten, Diensten und Systemen, anstatt von den Menschen zu verlangen, dass sie sich für den Datenschutz entscheiden. Das bedeutet, dass der Datenschutz die Standardeinstellung sein sollte und nicht eine optionale Funktion, für deren Aktivierung sich der Einzelne entscheiden muss.
- Datenminimierung(Vgl. auch Art. 5 Abs. 1 lit. c DSGVO): Nur so viele personenbezogene Daten erheben und verarbeiten, wie für die Erfüllung ihrer Zwecke erforderlich sind. Das bedeutet, dass Organisationen die Menge der von ihnen erhobenen und gespeicherten personenbezogenen Daten auf ein Minimum reduzieren und nur dann personenbezogene Daten erheben oder speichern sollten, wenn dies für ihre rechtmäßigen Zwecke unbedingt erforderlich ist.
- Sicherheit(Vgl. Art. 32 DSGVO): Der Grundsatz des „eingebauten Datenschutzes“ verlangt von Organisationen, dass sie geeignete Sicherheitsmaßnahmen ergreifen, um personenbezogene Daten vor unbefugtem Zugriff, unbefugter Nutzung oder Offenlegung zu schützen. Dazu können Maßnahmen wie Verschlüsselung, Zugangskontrollen und sichere Speichersysteme gehören.
- Transparenz(Vgl. auch Art. 5 Abs. 1 lit. a und Art. 12 DSGVO): Datenschutz durch Technik erfordert, dass Organisationen ihre Datenverarbeitungsaktivitäten transparent machen und Einzelpersonen klare und präzise Informationen darüber geben, wie ihre personenbezogenen Daten verwendet werden.

Artikel, 2023