□□ Datenschutz

Durch Datenschutz wird das Grundrecht auf die Achtung der Privatsphäre und auf informationelle Selbstbestimmung gewahrt. Zu diesem Zweck definiert das Datenschutzrecht, auf welche Weise personenbezogene Daten – d. h. Daten, durch die Personen identifiziert werden können, wie Namen oder E-Mail-Adressen – verarbeitet werden dürfen.

Datenschutz in der Softwareentwicklung

Das europäische Datenschutzrecht verpflichtet nicht diejenigen, die Software entwickeln und bereitstellen, sondern diejenigen, die personenbezogene Daten mithilfe von Software verarbeiten bzw. für ihre Zwecke verarbeiten lassen. Bei der Entwicklung eines neuen Softwareprojekts ist Datenschutz dennoch von Anfang an wichtig. Denn Software hat nur dann eine Chance eingesetzt zu werden, wenn eine datenschutzkonforme Verarbeitung damit technisch möglich ist.

Entwicklungsprinzipien

Um datenschutzkonforme Software zu entwickeln, sollten zwei Grundprinzipien beachtet werden.

- **Privacy by Design:** Datenschutz durch Technikgestaltung ist ein Designprinzip für die Entwicklung von Software und Hardware, bei der Datenschutzaspekte berücksichtigt werden. Das Ziel ist, dass Software und Hardware von Beginn an alle technischen Voraussetzungen dafür bieten, datenschutzkonform genutzt zu werden, um später zeit- und kostenaufwändige Anpassungen zu vermeiden.
- **Privacy by Default:** Eine besonders wichtige Funktion, die in Software umgesetzt sein sollte, sind datenschutzfreundliche Voreinstellungen. Der Umfang, in dem personenbezogene Daten verarbeitet werden, sollte standardmäßig so gering wie möglich sein und zusätzliche Verarbeitung optional und granular durch Nutzende selbst aktivierbar.

In der Praxis sind folgende Grundsätze und entsprechende Maßnahmen besonders wichtig:

- Datenminimierung:
  Personenbezogene Daten dürfen nur für festgelegte Zwecke und in dafür notwendigem Umfang verarbeitet werden (Art. 5 Abs. 1 lit. b) u. c) DSGVO). Für das Softwaredesign bedeutet das:
  - Software sollte soweit wie möglich **ohne personenbezogene Daten** funktionieren und diese ansonsten, wenn möglich, **lokal speichern**.
  - Im Zweifel sollte die **Verarbeitung optional aktivierbar** sein.
- Speicherbegrenzung:
  Personenbezogene Daten dürfen nur gespeichert werden, so lange sie für den Zweck ihrer

Erhebung benötigt werden (Art. 5 Abs. 1 lit. e) DSGVO). Für das Softwaredesign bedeutet das:
    - Software muss über eine **Löschfunktion** und ggf. eine **Anonymisierungsfunktion** verfügen.
- Richtigkeit, Integrität und Vertraulichkeit:
  Es muss sichergestellt sein, dass personenbezogene Daten sachlich richtig und auf neuestem Stand sind und dass sie vor unbefugter oder unrechtmäßiger Verarbeitung sowie Verlust geschützt sind (Art. 5 Abs. 1 lit. d) u. f) DSGVO). Für das Softwaredesign bedeutet das:
    - Software sollte über **Funktionen für die Aktualisierung und für Backups** von personenbezogenen Daten verfügen.
    - Sie sollte eine **Funktion zur Protokollierung von Änderungen** und **Berechtigungskonzept** anbieten, durch das sich der der Zugriff auf personenbezogene Daten kontrollieren lässt.
    - Eine wirksame Maßnahme, um Integrität und Vertraulichkeit sicherzustellen, ist außerdem die Implementierung von **Verschlüsselung**.
- Betroffenenrechte:
  Personen, deren Daten verarbeitet werden, haben eine Reihe von Rechten. Dazu gehört u. a. das Recht auf Auskunft über die sie betreffende Datenverarbeitung (Art. 15 DSGVO) sowie das Recht auf Datenübertragbarkeit (Art. 20 DSGVO). Für das Softwaredesign bedeutet das:
    - **Transparenz der Verarbeitung** personenbezogener Daten sollte im Vordergrund stehen.
    - Für Nutzendenprofile und damit verbundene Daten sollte eine **Exportfunktion** eingebaut sein.

Relevante Gesetze

Menschenrechte: Ihre Grundlage haben Datenschutzgesetze in den Menschenrechten, die durch die Europäische Menschenrechtskonvention, die Charta der Grundrechte der Europäischen Union und das Grundgesetz garantiert sind.

Datenschutzgrundverordnung (DSGVO): Die DSGVO definiert Grundsätze für die Verarbeitung personenbezogener Daten, die EU-weit unmittelbar gelten.

Bundesdatenschutzgesetz (BDSG): Das BDSG ergänzt die DSGVO in Deutschland und enthält zusätzliche Bestimmungen insbesondere zum Beschäftigtendatenschutz.

Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG): Das TDDDG setzt in Deutschland die ePrivacy-Richtlinie um und regelt unter anderem den Zugriff auf Daten, die auf Geräten von Endnutzenden gespeichert sind, z. B. über das Setzen von Cookies.

Wichtige Organisationen

Datenschutzbehörden: Für die Durchsetzung der DSGVO und des BDSG sind in Deutschland die Datenschutzbehörden zuständig. Die Bundesdatenschutzbeauftragte überwacht die Einhaltung der gesetzlichen Vorgaben bei Bundesbehörden und Telekommunikationsunternehmen, die Landesdatenschutzbeauftragten sind für öffentliche Stellen der Bundesländer und den nicht-öffentlichen Bereich, z. B. Privatunternehmen oder Vereine, zuständig.

Europäischer Datenschutzausschuss (EDSA): Im EDSA kommen die nationalen Datenschutzbehörden zusammen, um die einheitliche Anwendung der DSGVO sicherzustellen. Dazu gibt das Gremium regelmäßig Leitlinien, Empfehlungen und Best Practices zur Umsetzung der Vorgaben durch die DSGVO.

Stiftung Datenschutz: Die unabhängige Bundesstiftung hat die Aufgabe, Datenschutz in Politik, Wirtschaft, Wissenschaft und Gesellschaft zu fördern. Sie veranstaltet dazu Informations- und Diskussionsveranstaltungen zu Fragen der Datenpolitik und des Datenschutzrechts und stellt praktische Informationen für Zielgruppen wie ehrenamtliche Organisationen oder Kleinunternehmen bereit.

Weiterführende Links

- Ressourcenliste zum Thema DSGVO, Superbloom: https://simplysecure.org/blog/gdpr-resources
- Best Practices für Datenschutz in der Softwareentwicklung, Superbloom: https://simplysecure.org/blog/data-handling
- Guidance on AI and data protection, Information Commissioner‘s Office: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/artificial-intelligence/guidance-on-ai-and-data-protection/about-this-guidance/
- Umgang mit besonderen Datenkategorien – Praxisratgeber, Stiftung Datenschutz: https://stiftungdatenschutz.org/ehrenamt/praxisratgeber/praxisratgeber-detailseite/besondere-datenkategorien-272

Revision #3
Created 19 December 2024 14:03:25 by Sophia
Updated 20 December 2024 08:24:24 by patricia