



Software-Engineering-Praxis

Prof. Dr. Gerd Beneken

Kapitel 9.3

Datenschutzgrundverordnung DSGVO

Personenbezogene Daten

personenbezogene Daten sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (...) beziehen“ (Art. 4 Nr. 1 DSGVO)

- Normale Daten: Name, Anschrift, Geschlecht, ..
- Sensible Daten: Gesundheit, Sexuelle Orientierung, Politische Orientierung, Gene ... (Art. 9 DSGVO)
- Auch: IP-Adresse, Standort, MAC-Adresse, E-Mail
- Anonymisierung -> Kein Datenschutz
- Möglichkeit der Identifizierung entscheidend

DSGVO regelt den Umgang mit personenbezogenen Daten

- Seit 25.05.2018 wirksam (ab jetzt zahlt man Strafen)
- Regelung auf europäischer Ebene, damit in ganz Europa ein einheitliches Datenschutzniveau

Verstöße

- Jeder Verstoß kann unabhängig vom Sitz des Anbieters bei der Datenschutzbehörde gemeldet werden
- Gravierende Verstöße: bis zu 20 Millionen Euro / 4% des gesamten weltweit erzielten Jahresumsatzes
- Normale Verstöße: 10 Mio / 2%
- Datenweitergabe kann Strafbar sein (§42 BDSG)

Wann dürfen sie personenbezogene Daten verarbeiten?

Ein Verbot mit Erlaubnisvorbehalt

- Verarbeitung personenbezogener Daten ist **verboten**, soweit keine (ausnahmsweise) Erlaubnis besteht.
- Erlaubnisse:
 - Einwilligung
 - Freiwilligkeit setzt voraus, dass der Benutzer gut informiert ist
 - Beispiel: Double-Opt-In Verfahren = Bestätigung der Einwilligung
 - Vertragserfüllung (z.B. Bestellung im Online Shop)
 - Achtung: Koppelungsverbot
 - Berechtigtes Interesse (Achtung: Widerspruchsrecht)
 - Z.B. Kamera in der U-Bahn

DSGVO Grundsätze

Sie müssen aufpassen, wie lange sie welche Daten speichern!

Grundsätze bei der Verarbeitung von Daten

- ***Zweckbindung***
- ***Datenminimierung***
- Privacy By Design / Privacy by Default
- ***(zeitliche) Speicherbegrenzung***
- Integrität und Vertraulichkeit
- Rechenschaftspflicht

Rechte eines Bürgers

Artikel 12 – 23 DSGVO

- Recht auf Auskunft (Art. 15 DSGVO)
 - Z.B. Prüfen, ist Grundsatz der Datensparsamkeit erfüllt?
 - Z.B. Prüfen, Zweck der Datenverarbeitung erfüllt?
- Recht auf Löschung (Art. 17. DSGVO)
 - Entfällt Zweck der Verarbeitung -> Löschung Pflicht
- Erlaubt: Umzug von Daten (Art. 20 DSGVO)
„Recht auf Datenübertragbarkeit“
- Privacy by Default (Art. 25 DSGVO)
„Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen“
- Weiterleitung an Dritte (Transparenz), nur erlaubt wenn Datenschutz gewährleistet

Was hat das jetzt mit dem Datenmodell zu tun?

Verarbeitungsverzeichnis (Art. 30 DSVO)

Für alle erhobenen Daten:

- die Zwecke der Verarbeitung
- Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- wenn möglich, eine allgemeine Beschreibung der technischen und organisatorischen Maßnahmen zur Sicherheit der Verarbeitung

Betrachten Sie alle Datensätze mit Personenbezogenen Daten

Quelle: Studierenden-Team für TechDivision

Datenarten (Entscheider)

DSK 1 = intern
DSK 2 = Vertraulich
DSK 3 = streng Vertraulich

Technical University of Applied Sciences 

Nr	Datenfeld	Gruppe	Verw.Zw.	Nutzungsdauer	DSK
14	MitarbeiterID	Entscheider	Ident.	Dauerhaft (bis Ausscheiden)	1
15	Name	Entscheider	Ident.	Dauerhaft (bis Ausscheiden)	1
16	Vorname	Entscheider	Ident.	Dauerhaft (bis Ausscheiden)	1

Zu jedem Attribut

- Gruppe (Welche Rolle greift zu?)
- Verwendungszweck
- Nutzungsdauer
- Datenschutzklasse (DSK)

Betrachten Sie alle Datensätze mit Personenbezogenen Daten

Quelle: Studierenden-Team für TechDivision

Datenlöschung

Nr	Datensatz	Kriterien für Löschung	Gesetzl. Löschfrist	Gesetzl. Aufbewahrungsfrist
1-10	Bewerberdaten	Keine Einwilligung	Sobald Stelle besetzt	??
11-13	HR Mitarbeiter	Ausscheiden	??	10 Jahre (?)

Zu jeder Entität

- Kriterium: Wann soll gelöscht werden?
- Gesetzliche Pflicht zum Löschen (Frist)
- Gesetzliche Pflicht zum Aufbewahren (Frist)

Literatur und Quellen, Vorlesung IT-Security bei Prof.Dr.Hüttl sowie: <https://dsgvo-gesetz.de> (kommerziell)

WORKSHOP / 17. Mai

PRIVACY BY DESIGN

— IM —
Software Engineering

Gemeinsam mit dem Zentrum Digitalisierung.Bayern und TechDivision bietet das Innovationslabor der Hochschule Rosenheim am 17. Mai 2019 einen Workshop zu Privacy by Design im Software Engineering an.

Bei dem Workshop lernst Du:

- /// was es mit dem Begriff Privacy by Design auf sich hat und wie das bei der Softwareentwicklung berücksichtigt wird
- /// welche datenschutzrechtlichen Grundlagen Du bei der Entwicklung von Anwendungen schon mal gehört haben solltest
- /// und wie eine großer Webdienstleister das in die Produkte seiner Kunden einbaut

Klingt spannend?
Dann melde Dich bis zum 13. Mai per Email an: martin.kuch@fh-rosenheim.de (Betreff: PbD-Workshop)
Die Teilnehmerzahl ist auf 25 begrenzt – first come, first serve!

Der Workshop findet am 17. Mai von 10 bis 15:45 in Raum B0.11 (Hochschulstraße 1) statt.

ct wissen DSGVO Was 2019 wirklich wichtig ist mit Webinar

- + Aus der Praxis: 100 Seiten Ratgeber von Fachjuristen
- + Hilfen für Unternehmen, Vereine und Fotografen
- + Mit FAQs, Kurzanleitungen und Checklisten

90 Minuten Webinar

150 Tage DSGVO:
Was wirklich wichtig ist – Löschen, Melden, Bußgelder!

50 Unternehmen und Medienredaktionen

- Kurzanleitungen
- Wirtschaftliche Anbieterdatenschutzrichtlinien
- Geschäftsletter und Datenschutzerklärungen
- Internetauftritte und Webseiten
- Bußgelder und Abmahnungen

Bestellen Sie Ihre
Heute und
Lieferung
gemäß 10. Buchstabe

€ 19,90 15031

JANUARI 2019