Datenschutz (ohne Gewähr!) und Berufsethik der Informatik

1. Datenschutz (ohne Gewähr, teilweise nach BfDI-Info 6 DSGVO)

1.0 Grundlegende Definitionen

DSG regeln
1. Rechte der Betroffenen gegenüber den verantwortlichen Stellen
2. Rechtssituation der Verantwortlichen / Auftragsverarbeiter:
   Pflichten; Einschränkungen, Zulässigkeit der Datenverarbeitung

Art. 1 (1) DSGVO: „Diese Verordnung enthält Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.“

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

1.0 Grundlegende Definitionen

Art. 4 DSGVO „1. als **identifizierbar** wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann“

1.0 Grundlegende Definitionen (Rechtspraxis)

Bestimmbarkeit: Bestimmbar ist eine Person, wenn ihre Identität unmittelbar oder mittels Zusatzwissen festgestellt werden kann. Daten sind personenbezogen, wenn ein Personenbezug hergestellt werden kann.

Gilt auch bei engen finanziellen, persönlichen oder wirtschaftlichen Verflechtungen zwischen einer natürlichen und einer juristischen Person: In diesen Fällen werden gewerbliche und Wirtschaftsdaten zu personen-bezogenen; die beiden Arten sind nicht mehr trennbar.

Berufliche und geschäftliche Sphäre einbezogen!
Einzelfirma, Ein-Mann-GmbH, Einzelkaufmann
Art der Beteiligung an einer Gesellschaft
Art der Zugehörigkeit zu und Funktion in einem Unternehmen
→ EMail-Verschlüsselung!

Quellen: Landesbeauftragter NRW, Bundesbeauftragter

1.0 Grundlegende Definitionen

Besondere Kategorien personenbezogener Daten

Die Verarbeitung von personenbezogenen Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung, Daten über Gesundheit oder Sexualleben und sexuelle Ausrichtung ist grundsätzlich untersagt (Art. 9 (1) DSGVO) – es sei denn es liegen bestimmte ausdrücklich geregelte Ausnahmen vor (Art. 9 (2) DSGVO). Es muss eine Einwilligung ausdrücklich erfolgen.

Ausnahmeregelungen in § 22, 28, 29 BDSG

1.0 Grundlegende Definitionen

Art. 4 DSGVO: „7. „**Verantwortlicher**“ die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet“

§ 2 (4) BDSG: „**Nichtöffentliche Stellen** sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts“

Art. 4 DSGVO: „8. „**Auftragsverarbeiter**“ eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet“

1.0 Grundlegende Definitionen

Art. 4 DSGVO: „2. „**Verarbeitung**“ jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung“

Art. 4 DSGVO: „6. „**Dateisystem**“ jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird“ [d. h. digitale Daten, Karteien und Formulare; nicht: Aktenunterlagen]

1.0 Basic definitions – English

GDPR – General Data Protection Regulation – gdpr-info.eu
Natürliche, juristische Person: natural, legal person
Personenbezogene Daten: personal data
Betroffener: **data subject** – identified or identifiable natural person
Verantwortlicher: **controller**
Auftragsverarbeiter: **processor**
Verarbeitung: processing; automatisiert: by automated means
Dateisystem: filing system
Rechtmäßigkeit: lawfulness
Zweckbindung: purpose limitation
Richtigkeit: **accuracy**
Speicherbegrenzung: storage limitation
Integrität und Vertraulichkeit: integrity and confidentiality
TOM: technical and organisational measures

1.0 Basic definitions – English

Aufsichtsbehörde: supervisory authority
– federführende Aufsichtsbehörde: lead supervisory authority
Auskunftsrecht: right of access
Beschäftigungskontext: context of employment
Datenschutzbeauftragter: **data protection officer**
Datenschutz-Folgenabschätzung: **data protection impact assessment**
Datenschutzverletzung: **personal data breach**
Erheben: collect, obtain
Kohärenzverfahren: consistency mechanism
Meldung: notification
Rechenschaftspflicht: **accountability**
Rechtsbehelf: judicial remedy
Schadenersatz: compensation
Verzeichnis von Verarbeitungstätigkeiten: records of processing activities
Zustimmung: consent

1.1 Rechtsvorschriften

1.1.1 Besondere Geheimhaltungsvorschriften

Sozial(daten)geheimnis: I §35 SGB [Sozialgesetzbuch], X §§67-85 SGB

Heilberufe (ärztliche Schweigepflicht, §27 BayKrG [Bayer. Krankenhaus-gesetz]), Rechtsanwälte (§43a BRAO, §2 BORA),
Steuerberater (Steuergeheimnis: §§57, 62 StBerG, § 30 AO), Sozialberater
Allgemein §203 StGB [Strafgesetzbuch]

Akteneinsicht: §29 BayVwVfG [Bayer. Verwaltungsverfahrensgesetz]

Schulnoten: §62 BayEUG [Bay. G üb. d. Erziehungs- u. Unterrichtswesen]

Ausschluss der Öffentlichkeit in Gerichtsverhandlungen

Geschäfts-, Betriebsgeheimnisse: Unternehmen (StGB, UWG, nicht DS!)

1.1.1 Subsidiarität von Datenschutz-Gesetzen

BDSG ist **subsidiär** („zur Aushilfe dienend“), nachrangig
§1(2) BDSG: „**Andere Rechtsvorschriften** des Bundes über den Datenschutz **gehen den Vorschriften dieses Gesetzes vor** …
Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten … bleibt unberührt.“

1.1.2 Aktuelle Datenschutzgesetze

EU-Richtlinie 95/46/EG und altes BDSG zum 24.05.2018 aufgehoben

EU: Ab 25.05.2018: EU-Verordnung 2016/679 vom 14.04.2016
EU-Datenschutz-Grundverordnung DSGVO
Gesetzescharakter; rechtsverbindlich für alle Mitgliedstaaten
Anwendungsvorrang gegenüber nationalem Recht (D: §1(5) BDSG)
ca. 70 **Öffnungsklauseln** für nationales Recht
(schwierig auffindbar; enthalten das Wort „Mitgliedstaat“)
Daneben: EU-Richtlinie (Directive) 2016/680 vom 14.04.2016
Datenschutz bei justizieller und polizeilicher Zusammenarbeit

D: **Bundesdatenschutzgesetz BDSG-neu** = Art. 1 DSAnpUG-EU
Kommentare: Spiros Simitis; Herbert Auernhammer; Kurt Nagel
Bayerisches Datenschutzgesetz BayDSG

1.1.2 Datenschutz-Grundverordnung EU-DSGVO (2016/679)

Kap. I: Allgemeine Bestimmungen (Art. 1-4)
Kap. II: Grundsätze (Art. 5-11)
Kap. III: Rechte der betroffenen Person
Abschnitt 1: Transparenz und Modalitäten (Art. 12)
Abschnitt 2: Informationspflicht und Recht auf Auskunft (Art. 13-15)
Abschnitt 3: Berichtigung und Löschung (Art. 16-20)
Abschnitt 4: Widerspruchsrecht, automatis. Entscheidungsfindung (21f.)
Abschnitt 5: Beschränkungen (Art. 23)
Kap. IV: Verantwortlicher und Auftragsverarbeiter
Abschnitt 1: Allgemeine Pflichten (Art. 24-31)
Abschnitt 2: Sicherheit personenbezogener Daten (Art. 32-34)
Abschnitt 3: Datenschutz-Folgenabschätzung, vorherige Konsultation (35f)
Abschnitt 4: Datenschutzbeauftragter (Art. 37-39)
Abschnitt 5: Verhaltensregeln und Zertifizierung (Art. 40-43)

1.1.2 Datenschutz-Grundverordnung EU-DSGVO (2016/679) Teil 2

Kap. V: Übermittlungen personenbezogener Daten an Drittländer oder an internationale Organisationen (Art. 44-50)
Kap. VI: Unabhängige Aufsichtsbehörden
Abschnitt 1: Unabhängigkeit (Art. 51-54)
Abschnitt 2: Zuständigkeit, Aufgaben und Befugnisse (Art. 55-59)
Kap. VII: Zusammenarbeit und Kohärenz [Aufsichtsbehörden]
Abschnitt 1: Zusammenarbeit (Art. 60-62)
Abschnitt 2: Kohärenz (Art. 63-67)
Abschnitt 3: Europäischer Datenschutzausschuss (Art. 68-76)
Kap. VIII: Rechtsbehelfe, Haftung und Sanktionen (Art. 77-84)
Kap. IX: Vorschriften für besondere Verarbeitungssituationen (85-91)
Kap. X: Delegierte Rechtsakte und Durchführungsrechtsakte (92-93)
Kap. XI: Schlussbestimmungen (Art. 94-99)

1.1.2 Bundesdatenschutzgesetz (neu) BDSG

Teil 1: Gemeinsame Bestimmungen

Kap. 1: Anwendungsbereich und Begriffsbestimmungen (§§ 1-2)
Kap. 2: Rechtsgrundlagen der Verarbeitung personenbezogener Daten (§§ 3-4)
Kap. 3: Datenschutzbeauftragte öffentlicher Stellen (§§ 5-7)
Kap. 4: Bundesbeauftragter für Datenschutz und Informationsfreiheit (§§ 8-16)
Kap. 5: Europäischer Datenschutzausschuss, Zusammenarbeit von Bund und Ländern (§§ 17-19)
Kap. 6: Rechtsbehelfe (§§ 20-21)

Teil 2: Verarbeitungen gemäß Art. 2 DSGVO

[Sachlicher Anwendungsbereich: automatisierte Verarbeitung personenbezogener Daten sowie für die nichtautomatisierte Verarbeitung in einem Dateisystem gespeicherter pers.bez. Daten]

Kap. 1: Rechtsgrundlagen der Verarbeitung (§§ 22-31)
Kap. 2: Rechte der betroffenen Person (§§ 32-37)
Kap. 3: Pflichten der Verantwortlichen und Auftragsverarbeiter (§§ 38-39)
Kap. 4: Aufsichtsbehörden [der Länder] für nichtöffentliche Stellen (§ 40)
Kap. 5: Sanktionen (§§ 41-43)
Kap. 6: Rechtsbehelfe (§ 44)

Teil 3: Verarbeitungen gemäß Art. 1(1) EU-Richtlinie 2016/680

1.1.2 Bundesdatenschutzgesetz (neu) BDSG

Im BDSG hauptsächlich genutzte nationale Öffnungsmöglichkeiten

Besondere Kategorien (Art. 9 DSGVO; §§ 22, 28, 29 BDSG)
Zweckänderung (Art. 5 (1) b DSGVO; §§ 23, 24 BDSG)
Wissenschaftsprivileg (Art. 5 (1) b und 89 DSGVO; §§ 28, 29 BDSG)
Beschäftigungsverhältnis (Art. 88 DSGVO; § 26 BDSG)
Betroffenenrechte (Art. 13-21 DSGVO; §§ 32-37 BDSG)
Datenschutzbeauftragte (Art. 37-39 DSGVO; § 38 BDSG)
Aufsichtsbehörden (Art. 51-67 DSGVO; §§ 8-14, 17-19, 40 BDSG)

1.2 Datenschutzgesetze (Auszüge)

1.2.1 Sachlicher Anwendungsbereich

Art. 2 (1) DSGVO: „Diese Verordnung gilt für die **ganz oder teilweise automatisierte Verarbeitung** personenbezogener Daten sowie
für die **nichtautomatisierte Verarbeitung** personenbezogener Daten, die in einem **Dateisystem** gespeichert sind oder gespeichert werden sollen.“

Gilt nicht für die Verarbeitung zu persönlichen und familiären Zwecken (Haushaltsausnahme, Art. 2 (2) c DSGVO).
Gilt nicht für die Abwehr von Gefahren für die öffentliche Sicherheit (Art. 2 (2) d DSGVO).

Ähnlich § 1 (1) BDSG

1.2 Datenschutzgesetze (Auszüge)
1.2.1 Räumlicher Anwendungsbereich

§ 1 (1) BDSG: Öffentlich und nicht-öffentlich [wenige Sonderregelungen]

Nicht-öffentlich:
Niederlassungsprinzip: Niederlassung des Verantwortlichen in der EU, unabhängig vom Datenverarbeitungsort (Art. 3(1) DSGVO, §1(4)2 BDSG)
Verarbeitungsortprinzip: umgekehrt (Art. 3(3) DSGVO, §1(4)1 BDSG)
Marktortprinzip [NEU]: nicht nur für
in der EU niedergelassene Verantwortliche / Auftragsverarbeiter
Voraussetzung ist nach Art. 3 (2) DSGVO (§ 1 (4) 3 BDSG) lediglich,
dass sich ein Angebot an einen nationalen Markt in der EU richtet oder
dass die DV der Beobachtung des Verhaltens von Personen in der EU dient

Medienprivileg: Ausgleich zwischen Persönlichkeitsschutz und Kommunikationsfreiheiten bleibt Mitgliedstaaten vorbehalten (Art. 85 DSGVO).

1.2.2 Zulässigkeit der Verarbeitung 1

Grundsätze für die Verarbeitung personenbezogener Daten
Verbot mit Erlaubnisvorbehalt (Art. 5 (1) DSGVO):

a) **Rechtmäßigkeit**
b) **Zweckbindung**: festgelegte, eindeutige und legitime Zwecke
c) **Datenminimierung**: Beschränkung auf das notwendige Maß
(bisher: Datenvermeidung, Datensparsamkeit; jetzt: **Technikgestaltung**)
d) **Richtigkeit**: Unrichtiges unverzüglich löschen oder berichtigen
e) **Speicherbegrenzung** [Dauer]: nur so lange, wie für Verarbeitungszweck erforderlich
f) **Integrität, Vertraulichkeit** [**Datensicherheit**]: **TOM**

(2) **Rechenschaftspflicht**: Der Verantwortliche … muss dessen Einhaltung [des Absatzes 1] nachweisen können (auch Art. 24 (1) DSGVO).

1.2.2 Zulässigkeit der Verarbeitung 2

Rechtmäßigkeit der Verarbeitung

Art. 6 (1) DSGVO

„…, wenn mindestens eine der nachstehenden Bedingungen erfüllt ist:

a) Einwilligung für einen oder mehrere bestimmte Zwecke

- Art. 7 DSGVO: Nachweispflicht des Verantwortlichen
- Einwilligung von anderen Sachverhalten unterscheidbar und unabhängig
- Klare und einfache Sprache
- Einwilligung jederzeit widerrufbar

b) für die Erfüllung eines Vertrags

c) zur Erfüllung einer rechtlichen Verpflichtung

d) lebenswichtige Interessen … einer natürlichen Person zu schützen

e) … im öffentlichen Interesse … oder in Ausübung öffentlicher Gewalt

f) Wahrung der berechtigten Interessen des Verantwortlichen …, sofern nicht die … Grundrechte … der betroffenen Person überwiegen“

1.2.2 Zulässigkeit der Verarbeitung 3

Zweckänderung

Es sind nur solche Änderungen des Verarbeitungszwecks erlaubt, die mit dem ursprünglichen Erhebungszweck vereinbar sind (Art. 5 (1) b sowie Art. 6 (4) DSGVO). Die Datenschutz-Grundverordnung stellt in Art. 6 (4) Kriterien auf, die zu berücksichtigen sind. Hierzu zählen u. a. die Verbindung zwischen den Zwecken, der Gesamtkontext, in dem die Daten erhoben wurden, die Art der personenbezogenen Daten, etc.

Art. 5 (1) b DSGVO: „Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken“

§ 24 BDSG: öffentliche Sicherheit, zivilrechtliche Ansprüche

1.2.2 Zulässigkeit der Verarbeitung 4

Integrität, Vertraulichkeit [**Datensicherheit**]:

Schutz vor … unrechtmäßiger Verarbeitung und vor … Verlust … durch geeignete **technische und organisatorische Maßnahmen [TOM]** (Art. 5 (1) f DSGVO)

Privacy by Design/ Default; **Technikgestaltung**	(Art. 25 DSGVO)
Auftragsverarbeitung	(Art. 28 DSGVO)
Meldungen über Datenschutzverletzungen	(Art. 33, 34 DSGVO)
Datenschutz-Folgenabschätzung	(Art. 35, 36 DSGVO)
Betriebliche / behördliche Datenschutzbeauftragte	(Art. 37-39 DSGVO)
Selbstregulierung durch die Verantwortlichen	(Art. 40-43 DSGVO:

Verhaltensregeln (Code of Conduct), Zertifizierungen;
Register beim Europäischen Datenschutzausschuss)

1.2.3 Rechte der Betroffenen 1 (DSGVO)

12 Transparente Information, Komm., Modalitäten für Rechte-Ausübung
(1) präzise, transparente, verständliche Form, klare, einfachen Sprache
(3) innerhalb eines Monats (plus zwei), (5) unentgeltlich

13 Informationspflicht bei Erhebung bei der betroffenen Person
Verantwortlicher, Zweck, Rechtsgrundlage, Empfänger, Dauer etc.
Rechte auf Berichtigung, Löschung, Widerruf der Einwilligung,
Widerspruch gegen Verarbeitung, Beschwerde bei Aufsichtsbehörde etc.
Einschränkungen: § 32 BDSG (öff. Sicherheit, Strafrecht, Zivilrecht etc.)
14 Informationspflicht bei anderweitigen Erhebungen
Zusätzlich: Quellen; automatisierte Entscheidungsfindung (Art. 22)
Einschränkungen: § 33 BDSG (öff. Sicherheit, Strafrecht, Zivilrecht etc.)

15 Auskunftsrecht: Angaben wie oben; Verweigerung dokumentieren
§ 34 (2) BDSG: Die zu diesem Zweck gespeicherten Daten dürfen nur dafür sowie für Zwecke der Datenschutzkontrolle verarbeitet werden

1.2.3 Rechte der Betroffenen 2 (DSGVO)

Art. 16 DSGVO: Recht auf Berichtigung
17 Recht auf Löschung
Für Zwecke nicht mehr nötig, Widerruf, Widerspruch, Unrechtmäßigkeit
§ 35 BDSG: bei unverhältnismäßig hohem Aufwand nur Einschränkung
17 (2) „Recht auf Vergessenwerden“ (bei Veröffentlichung der Daten)
18 Einschränkung der Verarbeitung (bisher: Sperrung)
Richtigkeit bestritten; Unklarheit über Widerspruch
19 Mitteilung an Empfänger bei Berichtigung, Löschung, Einschränkung

20 Recht auf Datenübertragbarkeit (zwischen Verantwortlichen)

21 Widerspruchsrecht (gegen Verarbeitung nach Art. 6 (1) e,f DSGVO)
uneingeschränkt bei Direktmarketing / Profiling (Ausnahme § 36 BDSG)

Art. 77 (1) DSGVO: Recht auf Beschwerde bei einer Aufsichtsbehörde
Art. 79 DSGVO: Recht auf gerichtlichen Rechtsbehelf (§ 44 BDSG)
Art. 82 (1) DSGVO: Recht auf Schadenersatz bei im(materiellen) Schäden

1.2.3 Rechte der Betroffenen: Werbung (Ges. gg. unlaut. Wettbewerb)

§ 7 UWG Unzumutbare Belästigungen
§ 7 (2) UWG Werbung mit 2. Telefonanruf, 3. elektronische Post (Spam)
ohne vorherige ausdrückliche Einwilligung
§ 7 (3) UWG Ausnahmen von (2):
1. E-Mail-Adresse im Rahmen eines Verkaufs erhalten
3. Kunde hat Verwendung nicht widersprochen
4. Kunde wird jedes Mal auf Möglichkeit des Widerspruchs hingewiesen

Newsletter gilt als E-Mail-Werbung,
aber schärfere Rechtsprechung ohne explizite gesetzliche Regelung:
Daten aus Kaufvertrag nicht einfach zum Newsletter-Versand verwendbar
Doppelte Bestätigung (double opt-in) erforderlich
opt-out genügt definitiv nicht

1.2.4 Automatisierte Einzelentscheidung

Art. 22 (1) DSGVO: „Die betroffene Person hat das Recht,
nicht einer ausschließlich auf einer automatisierten Verarbeitung —
einschl. Profiling — beruhenden Entscheidung unterworfen zu werden,
die ihr gegenüber rechtliche Wirkung entfaltet …“
(2)-(4) Ausnahmen: Vertragsabschluss, -erfüllung, Einwilligung,
Rechtsvorschrift, Überwachung von Betrug und Steuerhinterziehung;
Recht auf Eingreifen einer Person seitens des Verantwortlichen, auf
Anfechtung der Entscheidung; nicht: besondere Kategorien

Erwäg.Grund (71) Online-Kreditantrag, Online-Einstellungsverfahren
„Profiling“: Analyse oder Prognose bezüglich Arbeitsleistung,
wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen,
Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel

Kurz: § 54 BDSG

1.2.4 Verbraucherkredite und Scoring

§ 30 (2) BDSG: „Wer den Abschluss eines Verbraucherdarlehensvertrags infolge einer Auskunft einer [Auskunftei] ablehnt,
hat den Verbraucher unverzüglich hierüber sowie über die erhaltene Auskunft zu unterrichten.“

§ 31 (1) BDSG: Wahrscheinlichkeitswert nur zulässig, wenn
2. Daten … nach wissenschaftlich anerkannten mathematisch-statistischen Verfahren nachweisbar … erheblich sind und
3. nicht ausschließlich Anschriftendaten genutzt wurden und
4. bei Anschriftendaten die betroffene Person … unterrichtet worden ist

(2) Wahrscheinlichkeitswert über Zahlungsfähig- und Zahlungswilligkeit: Nur solche offenen Forderungen berücksichtigungsfähig, für die Gerichtsurteil vorliegt, die der Schuldner ausdrücklich anerkannt hat …

1.2.5 Beschäftigte (Art. 88 DSGVO nationale Öffnungsklausel)

§ 26 (8) BDSG: „Bewerber … sowie Personen,
deren Beschäftigungsverhältnis beendet ist, sind Beschäftigte."
„**Beschäftigte** sind:
1. Arbeitnehmerinnen und Arbeitnehmer
2. zu ihrer Berufsausbildung Beschäftigte 6. in Heimarbeit Beschäftigte
7. Beamte, … Richter …, … Soldaten sowie Zivildienstleistende"

§ 26 (1) BDSG: „Personenbezogene Daten von Beschäftigten dürfen für Zwecke des **Beschäftigungsverhältnisses** verarbeitet werden, wenn dies … für dessen Durchführung … erforderlich ist.…
Zur Aufdeckung von **Straftaten** … nur dann, wenn
zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen,
… die Verarbeitung zur Aufdeckung erforderlich ist und
das schutzwürdige Interesse … des Beschäftigten … nicht überwiegt, …
Art und Ausmaß im Hinbl. auf den Anlass nicht unverhältnismäßig sind."

1.2.6 Anforderungen an verantwortliche Stellen 1 (DSGVO)

Art. 24 DSGVO Verantwortung des Verantwortlichen
(1) … setzt unter Berücksichtigung … der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken … geeignete **technische und organisatorische Maßnahmen** um, um sicherzustellen und nachweisen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt.

Art. 25 DSGVO Technikgestaltung, datenschutzfreundl. Voreinstellungen
Pseudonymisierung, Datenminimierung etc.

Art. 28 DSGVO Auftragsverarbeiter
(1) „Erfolgt eine Verarbeitung im Auftrag eines Verantwortlichen, so arbeitet dieser nur mit Auftragsverarbeitern, die hinreichend Garantien dafür bieten, dass geeignete TOM so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen dieser Verordnung erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.“

1.2.6 Anforderungen an verantwortliche Stellen 2 (DSGVO)

Art. 30 DSGVO **Verzeichnis von Verarbeitungstätigkeiten**
Dokumentationspflicht von Verantwortlichen und Auftragsverarbeitern

Art. 32 DSGVO Sicherheit der Verarbeitung
TOM, Schutzniveau, Prüfverfahren etc. (ähnlich Art. 24)

Art. 33 DSGVO Meldung von Verletzungen an die Aufsichtsbehörde
(1) Im Falle einer Verletzung des Schutzes personenbezogener Daten meldet sie der Verantwortliche unverzüglich und möglichst binnen 72 Stunden nach Bekanntwerden der zuständigen Aufsichtsbehörde

Art. 34 DSGVO Benachrichtigung betroffener Personen über Verletzungen
(1) unverzüglich bei hohem Risiko

1.2.6 Anforderungen an verantwortliche Stellen 3 (DSGVO)

Art. 35 DSGVO **Datenschutz-Folgenabschätzung** (alt: Vorabkontrolle)
(1) Voraussichtlich hohes Risiko für Rechte und Freiheiten nat. Personen
(2) Verantwortlicher holt Rat des Datenschutzbeauftragten ein.
(3) a) systematische und umfassende Bewertung persönlicher Aspekte einschl. Profiling als Grundlage für rechtswirksame Entscheidungen
b) umfangreiche Verarbeitung besonderer Kategorien pers.bez. Daten
c) systematische umfangreiche Überwachung öffentlich zugängl. Bereiche
(4), (5) Aufsichtsbehörden erstellen Positivlisten und Negativlisten
(7) Inhalt der Datenschutz-Folgenabschätzung → Datenschutz-Bewusstsein

Art. 36 DSGVO **Vorherige Konsultation**
(1): „Der Verantwortliche konsultiert vor der Verarbeitung die Aufsichtsbehörde, wenn aus einer Datenschutz-Folgenabschätzung hervorgeht, dass die Verarbeitung ein hohes Risiko zur Folge hätte, sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft.“

1.2.6 Anforderungen an verantwortliche Stellen 4 (DSGVO)

Selbstregulierung: Nachweis des rechtskonformen Verhaltens
von Verantwortlichen und Auftragsverarbeitern gemäß Art. 24-36 DSGVO

Art. 40 DSGVO Verhaltensregeln, Code of Conduct
Art. 41 DSGVO Überwachung durch akkreditierte Stellen

Art. 42 DSGVO Zertifizierung von Verantwortl. / Auftragsverarbeitern
Art. 43 DSGVO Akkreditierte Zertifizierungsstellen (§ 39 BDSG)

Datengeheimnis

§53 BDSG (Teil 3!): „Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten. Sie sind bei der Aufnahme ihrer Tätigkeit auf das Datengeheimnis zu **verpflichten**. Das Datengeheimnis besteht nach der Beendigung ihrer Tätigkeit fort.“

1.2.7 Datenschutzbeauftragter: Benennung (Art. 37 DSGVO)

Art. 37 (1) DSGVO: Der Verantwortliche und der Auftragsverarbeiter benennen auf jeden Fall einen Datenschutzbeauftragten, wenn
a) Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt
b) Kerntätigkeit: Verarbeitungsvorgänge, welche aufgrund Art, Umfang und/oder Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
c) umfangreiche Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10

(5) „Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Qualifikation und insbesondere des **Fachwissens** benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt …“.
(6) … Beschäftigter des Verantwortlichen / Auftragsverarbeiter oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

1.2.7 Datenschutzbeauftragter: nichtöffentliche Stellen (BDSG § 38)

§ 38 (1) BDSG: der Verantwortliche und der Auftragsverarbeiter benennen eine/n Datenschutzbeauftragte/n,
„soweit sie in der Regel **mindestens zehn Personen** ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen“.

„Nehmen der Verantwortliche / Auftragsverarbeiter Verarbeitungen vor, die einer **Datenschutz-Folgenabschätzung** nach Art. 35 DSGVO unterliegen,
oder verarbeiten sie personenbezogene Daten **geschäftsmäßig** zum Zweck der Übermittlung, der anonymisierten Übermittlung oder
für Zwecke der Markt- oder Meinungsforschung,
haben sie
unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen
eine/n Datenschutzbeauftragte/n zu benennen.“

1.2.7 Datenschutzbeauftragter: Stellung (Art. 38 DSGVO)

Art. 38 (2) DSGVO: Der Verantwortliche / Auftragsverarbeiter stellen die für die Erfüllung der Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung.

(3) Der Verantwortliche / Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält.
Er darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Er berichtet unmittelbar der höchsten Managementebene des Verantwortlichen / Auftragsverarbeiters.

(4) Betroffene Personen können den Datenschutzbeauftragten bei allen Fragen zur Verarbeitung ihrer personenbezogenen Daten zu Rate ziehen.

1.2.7 Datenschutzbeauftragter: Aufgaben (Art. 39 DSGVO)

Art. 39 (1) DSGVO
a) Beratung des Verantwortlichen / Auftragsverarbeiters und der Beschäftigten hinsichtlich ihrer Pflichten nach den Datenschutzvorschriften
b) Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen / Auftragsverarbeiters für den Schutz personenbezogener Daten einschließl. der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen;
c) Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäß Art. 35 DSGVO;
d) Zusammenarbeit mit der Aufsichtsbehörde;
e) Tätigkeit als Anlaufstelle für die Aufsichtsbehörde.

(2) Der Datenschutzbeauftragte trägt dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung.

1.3 Öffentliche Kontrolle: Aufsichtsbehörden

Bundesbeauftragter für Datenschutz und Info-Freiheit (§§ 8-16 BDSG)

Art. 51 (1) DSGVO: „Jeder Mitgliedstaat sieht vor, dass eine oder mehrere unabhängige Behörden für die Überwachung der Anwendung dieser Verordnung zuständig sind.“
§ 40 (1) BDSG: „Die nach Landesrecht zuständigen Behörden überwachen im Anwendungsbereich der DSGVO bei den nichtöffentlichen Stellen die Anwendung der Vorschriften über den Datenschutz.“

Bayer. Landesbeauftragter für den Datenschutz; Beirat
Datenschutzregister (Behörden, die personenbezog. Daten verarbeiten)
Verordnung über das Datenschutzregister DSRegV

Bayer. Landesamt für Datenschutz-Aufsicht BayLDA, Ansbach

1.3 Öffentliche Kontrolle: Aufsichtsbehörden; effektive Durchsetzung

Art. 52 (1) DSGVO: Unabhängigkeit der Aufsichtsbehörden
(2) kein Weisungsempfang
(4) Jeder Mitgliedstaat stellt personelle, technische und finanzielle Ressourcen, Räumlichkeiten und Infrastrukturen sicher

Art. 53 DSGVO: Transparentes Ernennungsverfahren der Mitglieder
Art. 58 DSGVO Untersuchungsbefugnisse der Aufsichtsbehörden (damit auch Rechtsaufsicht ggü. anderen Behörden)

Art. 83 (4) DSGVO Sanktionen: „Geldbußen von bis zu 20 000 000 EUR oder im Fall eines Unternehmens von bis zu 4 % seines gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahrs verhängt, je nachdem, welcher der Beträge höher ist“:
Art. 84 DSGVO: Öffnungsklausel für andere länderspezifische Sanktionen
§§ 41-43 Strafvorschriften, Bußgeldvorschriften

1.3 Öffentliche Kontrolle: Aufsichtsbehörden; Koordination

One-Shop-Stop-Mechanismus:
Eine federführende Aufsichtsbehörde am Sitz der Hauptniederlassung des Verantwortlichen auch bei grenzüberschreitender Tätigkeit

Art. 56 DSGVO: Federführende Aufsichtsbehörde (Hauptniederlassung)
Art. 60 DSGVO: Zusammenarbeit der federführenden A. mit anderen
§ 18 BDSG Zusammenarbeit der Aufsichtsbehörden (Bund und Länder)
§ 19 BDSG Zuständigkeiten der Aufsichtsbehörden

Kohärenzverfahren:
Art. 63 DSGVO: Zusammenarbeit der Aufsichtsbehörden „zur einheitlichen Anwendung“ der DSGVO in der EU (One-Stop-Shop-Fälle)
Art. 64-66 Details zum Kohärenzverfahren

2. National Codes of Ethics and Professional Conduct
Berufsethik der Informatik – Nationale Ethikkodizes

2.0 USA
2.1 Canada
2.2 Australia
2.3 New Zealand
2.4 Germany: Ethical Guidelines of the GI
2.5 Informationsethik

2.0 USA

Association of Information Technology Professionals (AITP)
Code of Ethics; Standards of Conduct
http://www.aitp.org

IEEE
Code of Ethics
http://www.ieee.org

Association for Computing Machinery (ACM)
Code of Ethics and Professional Conduct
http://www.acm.org

Neumann, Peter G.: ACM Forum on Risks to the Public
in the Use of Computers and Related Systems. Articles in
ACM Software Engineering Notes; Communications of the ACM

2.1 Canada

Canadian Information Processing Society (CIPS):
Code of Ethics and Professional Conduct. Toronto [1]1985.
http://www.cips.ca/standards/isp/ethics/

1. Protect public interest and maintain integrity
2. Demonstrate competence and quality of service
3. Maintain confidential information and privacy
4. Avoid conflicts of interest
5. Uphold responsibility to the IT profession

2.2 Australia

Australian Computer Society (ACS):
Code of Ethics. Darlinghurst [1]1987.
http://www.acs.org.au/index.cfm?action=show&conID=coe

1. Uphold and advance the honor … of the profession of IT
3. Values, ideals (e.g. enhance quality of life of those affected by my work)
4. Standards of conduct
5. Priorities
6. Competence (e.g. provide products and services which match the operational and financial needs of my clients and employers)
7. Honesty
8. Social implications (e.g. consider and respect people's privacy)
9. Professional development
10. Information technology profession (e.g. seek advice from the Society when faced with an ethical dilemma I am unable to resolve by myself)

2.3 New Zealand

New Zealand Computer Society (NZCS):
Code of Ethics and Professional Conduct. Wellington [1]1987.
http://www.nzcs.org.nz/SITE_Default/about_NZCS/Code_of_Ethics.asp

1. Responsibility for the community comes before other responsibilities
2. Act with integrity, dignity, honor to merit the trust of the community and to contribute positively to the well-being of society
3. Treat people with dignity, good faith and equity, without discrimination, consideration for cultural sensitivities
4. Follow recognized professional practice
5. Develop knowledge, skills and expertise continuously
6. Apply skills and knowledge in the interests of clients or employers
7. Inform of the economic, social, environmental or legal consequences
8. Inform clients or employers of any interest in conflict with their interests

2.4 Germany

Gesellschaft für Informatik (GI):
Ethische Leitlinien / Ethical Guidelines
Informatik-Spektrum 16(1993) 238-240 [Capurro; Coy; Damker et al.];
Informatik-Spektrum 19(1996) 79-86 [Rödiger; Wilhelm]
Aktuelle Version 29.06.2018

https://gi.de/ueber-uns/organisation/unsere-ethischen-leitlinien/

Selbstverpflichtung; Begriffserläuterungen

Preamble

The German Informatics Society (GI) is a registered non-profit organization. With these guidelines, the GI seeks to establish that matters of professional ethics or moral conflicts become the subject of collaborative reflection and action.
The guidelines are designed to offer a point of orientation not only to members of the GI association, but to all persons involved in the design, manufacture, operation or use of IT systems.

The ethical guidelines outlined herein express the intent of GI members to conduct themselves in accordance with the values that form the basis of Basic Law for the Federal Republic of Germany and the Charter of Fundamental Rights of the European Union.

The GI and its members are committed to adhering to these guidelines. They also seek to insure that these guidelines find acknowledgement in public discourse outside the GI.

GI members are especially committed to respecting and protecting human dignity. Whenever norms of the state, society or the private sphere come into conflict with these values, GI members must address the issue.

GI members conduct themselves in such a way as to advocate for the right to self-determination in information and communication technologies, and for the right to guarantee confidentiality and integrity of IT systems.

GI members advocate for discrimination-free organizational structures which take into consideration the divergent needs and diversity of all human beings in the design, manufacture, operation and use of IT systems.

GI members seek to engage and educate the public in discourse concerning the ethical and moral issues pertinent to their individual and institutional conduct.
In a networked world, it is imperative that all potential courses of action be subject to interdisciplinary consideration regarding their foreseeable impact and potential consequences. This is the challenge for each of our members.

The fact that the guidelines established here are as open as they are is testimony to the fact that moral conduct cannot be governed by a definitive code of ethics or stringent regulations.

Section 1: Professional Competence

GI members stay abreast of the current state of science and technology in their respective areas of specialization; they take new developments into account and provide constructive criticism. GI members are constantly working to improve their professional competencies.

Section 2: Expertise and Communicative Competence

GI members are constantly improving their levels of expertise and communicative competencies in order to meet the demands relevant to their duties in the design, manufacture, operation and use of IT systems and to understand the surrounding professional and technical contexts.
In order to assess the consequences of IT-systems in the application environment and to propose suitable solutions, there must be a willingness to understand and take into account the rights, needs and interests of those parties who are impacted by them.

Section 3: Legal Expertise

GI members are familiar with and observant of pertinent legal regulations concerning the design, manufacture, operation and use of IT systems.
GI members, in conjunction with their expertise and professional competencies, participate actively in drafting legislative regulations.

Section 4: Powers of Discernment

GI members sharpen their powers of discernment to render themselves better equipped to contribute to design processes with individual and collective accountability.
This presupposes not only a willingness to call into question and to make judgments about individual and collective actions in public discourse, but also the ability to acknowledge the limits of one's own powers of discernment.

Section 5: Conditions of Employment

GI members are active proponents of socially equitable contractual agreements concerning terms of employment, inclusive of opportunities for professional development and shared governance.

Section 6: Organizational Structures

GI members advocate for organizational structures which foster and facilitate socially equitable contractual agreements concerning terms of employment.

Section 7: Teaching and Learning

GI members who are computer science instructors foster in their students the capacity for critical thinking;
they prepare learners to accept their own individual and collective responsibility, and they act as role models in this regard.

Section 8: Research

GI members who conduct research in the field of computer science adhere to the rules of best practices in scientific research.
Of particular importance in this regard is openness and transparency in dealing with criticism and conflicts of interest, the ability to express and to accept criticism as well as the willingness
to allow the impact of one's own scientific work in the research process to become the subject of discussion.
Scientific research breaches boundaries. These must be clearly articulated.

Section 9: Courage of Convictions

GI members staunchly advocate for the protection and safeguarding of human dignity, even when this is not explicitly mandated by laws, contracts or other norms, or when these stand in direct opposition to the protection and safeguarding of human dignity.
This applies even in situations in which GI members' obligations to clients conflict with their responsibility to third-party stakeholders.

Section 10: Social Accountability

In the design, manufacture, operation and use of IT systems, GI members should contribute to the betterment of local and global living conditions.
GI members are responsible for the social and societal consequences of their work.
Their influence on positioning, marketing and further development of IT systems should contribute to the socially acceptable and sustainable application of these technologies.

Section 11: Facilitating Self-Determination

GI members work toward ensuring that those people impacted by the usage and conditions of use of IT systems are granted adequate opportunity to participate in the design of these systems.
This is especially pertinent with regard to systems whose application involves the exerting influence over, monitoring, or surveillance of said populations.

Section 12: The German Informatics Society

The German Informatics Society encourages its members to adhere to these guidelines at all times.
The GI shall attempt to mediate between parties in situations in which conflicts arise.

2.5 Informationsethik

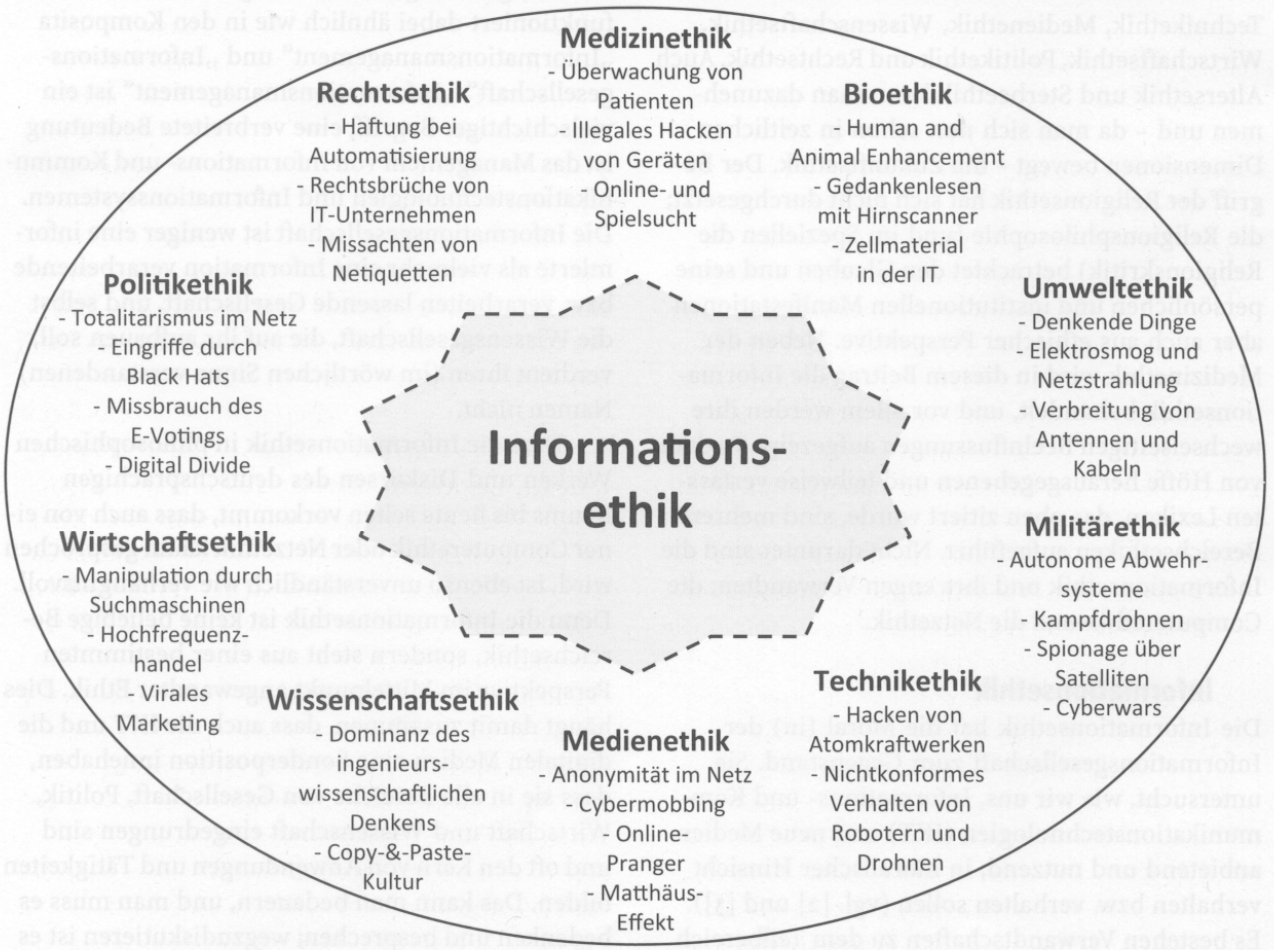

Abb. 1 Das „Ethik-Ei" – Informationsethik im Zentrum der Bereichsethiken (in Anlehnung an [1])