

Datenbank-Programmierung

Kapitel 6: Datenschutz: Einführung

Prof. Dr. Stefan Brass

Martin-Luther-Universität Halle-Wittenberg

Sommersemester 2024

<http://www.informatik.uni-halle.de/~brass/dbp24/>

Lernziele

Nach diesem Kapitel sollten Sie Folgendes können:

- Einige Vorgehensweisen von Hackern erklären.
- Sicherheitsrelevante DBMS Funktionen erklären.
- Einige Grundzüge des deutschen Datenschutzrechtes beim Aufbau von Datenbanken berücksichtigen.

Oder zumindest erkennen, wann Sie weitere Informationen einholen müssen.

Datenschutz-Recht (2)

- Der Text der DSGVO ist z.B. hier verfügbar:
 - [<https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:32016R0679>]
Das dort auch erhältliche PDF hat 88 Seiten, von denen die ersten 31 Seiten „Erwägungsgründe“ sind, also eine Art Kommentar.
 - [<https://.../?uri=CELEX:02016R0679-20160504>]
Diese Version enthält Berichtigungen/Aktualisierungen bis 2021.
 - [<https://dsgvo-gesetz.de/>]
 - [<https://dejure.org/gesetze/DSGVO>]
- Das Bundesdatenschutzgesetz (BDSG) ergänzt die DSGVO:
 - [https://www.gesetze-im-internet.de/bdsg_2018/]
 - [<https://dsgvo-gesetz.de/bdsg/>]

Datenschutz-Recht (3)

- **Datenschutzgesetze** sollen davor schützen, dass man durch Umgang mit seinen personenbezogenen Daten in seinem verfassungsmäßig garantierten Persönlichkeitsrecht beeinträchtigt wird (freie Selbstbestimmung bei der Entfaltung der Persönlichkeit).
- Das **Volkszählungsurteil** des Bundesverfassungsgerichts von 1983 war wegweisend und enthält u.a. folgende Begründung:

„Wer damit rechnet, dass etwa die Teilnahme an einer Versammlung oder einer Bürgerinitiative behördlich registriert wird und dass ihm dadurch Risiken entstehen können, wird möglicherweise auf eine Ausübung seiner entsprechenden Grundrechte (Art. 8, 9 GG) verzichten.“

Rechtmäßigkeit der Datenverarbeitung (1)

- Verarbeitung personenbezogener Daten ist verboten, wenn nicht einer der folgenden Gründe vorliegt (**Art. 6 DSGVO**):
 - Einwilligung der betroffenen Person
 - Notwendig zur Erfüllung eines Vertrages mit der betroffenen Person (auch vorvertragliche Maßnahmen, z.B. Angebot).
 - Es gibt rechtliche Verpflichtung (z.B. Rechnung 10 Jahre).
 - Um lebenswichtige Interessen zu schützen (Notaufnahme).
 - Aufgabe im öffentlichen Interesse (z.B. „Knöllchen“).
 - Wahrung berechtigter Interessen des Verantwortlichen (d.h. der Firma) oder eines Dritten, sofern nicht Interessen bzw. Grundrechte der betroffenen Person überwiegen.

Rechtmäßigkeit der Datenverarbeitung (2)

Einwilligung:

- Die Einwilligung muss freiwillig erfolgen.

Die Erfüllung eines Vertrags/Erbringung einer Dienstleistung darf nicht von der Einwilligung zur Verarbeitung personenbezogener Daten abhängig gemacht werden, die für diesen Zweck nicht erforderlich sind ([Art. 7 \(4\) DSGVO](#)) („Kopplungsverbot“). Es muss Alternativen geben, ggf. kostenpflichtige. Daten-gegen-Leistung muss transparent sein und dann ist ein Vertrag Rechtsgrundlage, nicht die freiwillige Einwilligung ([LDI NRW 26. Bericht 2021](#)).

- Einwilligungen können jederzeit widerrufen werden.

Vorher erfolgte Verarbeitungen bleiben natürlich rechtmäßig. Der Widerruf der Einwilligung muss so einfach wie die Erteilung der Einwilligung sein.

- Einwilligungen können nicht versteckt sein in Erklärungen, die noch andere Sachverhalte betreffen (klar unterscheidbar).

Rechtmäßigkeit der Datenverarbeitung (3)

Berechtigtes Interesse/Werbung:

- Das Versenden von Werbung per Post ist von den „berechtigten Interessen“ gedeckt, Werbung per EMail bedarf dagegen nach dem **§ 7 UWG** (Gesetz gegen unlauteren Wettbewerb) einer Einwilligung.

Siehe: Michael Rohrlisch: Datenschutz einfach umsetzen, S. 38, 40.

Es gibt allerdings das „Bestandskundenprivileg“: Falls der Unternehmer die Email-Adresse vom Kunden erhalten hat, und es um eigene ähnliche Waren geht, der Kunde nicht widersprochen hat, und der Kunde bei Erhebung sowie jeder Verwendung auf die Widerspruchsmöglichkeit hingewiesen wird, stellt die EMail keine unzumutbare Belästigung dar (ist also legal).

- Gegen Verarbeitung aufgrund von „berechtigtem Interesse“ besteht in bestimmten Situationen ein Widerspruchsrecht (**Art. 21 DSGVO**), insbesondere auch bei Direktwerbung.

Rechtmäßigkeit der Datenverarbeitung (4)

Besonders schützenswerte, sensitive Daten:

- „Besondere Kategorien personenbezogener Daten“ sind (Art. 9 DSGVO):
 - rassische und ethnische Herkunft
 - politische Meinungen
 - religiöse oder weltanschauliche Überzeugungen
 - Gewerkschaftszugehörigkeit
 - Genetische und biometrische Daten
 - Gesundheit
 - Sexualeben, sexuelle Orientierung
- Für diese Daten gelten verschärfte Vorschriften.

Insbesondere entfällt die Rechtfertigung „berechtigtes Interesse“.

Rechtmäßigkeit der Datenverarbeitung (5)

Zweckbindung:

- Daten müssen „für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden“ (**Art. 5 DSGVO**).

Im öffentlichen Interesse liegende Archivzwecke, sowie wissenschaftliche, historische und statistische Zwecke sind ausgenommen.

- Es gibt allerdings eine etwas verschwommene Klausel in **Art. 6 (4) DSGVO**. Demnach kann die Verarbeitung zu einem anderen Zweck mit dem ursprünglichen Zweck vereinbar sein. Siehe auch Informationspflicht nach **Art. 13 (3) DSGVO**.

[<https://www.dr-datenschutz.de/dsgvo-zweckaenderung-der-datenverarbeitung-am-beispiel-werbung/>]

Rechtmäßigkeit der Datenverarbeitung (6)

Speicherfrist:

- Personbezogene Daten müssen „in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist“ ([Art. 5 DSGVO](#)).

- In anonymisierter Form dürfen sie natürlich beliebig lange gespeichert werden.

Dann sind es ja auch keine personenbezogenen Daten mehr.

- Es müssen natürlich weitere Rechtsvorschriften beachtet werden, z.B. sind Rechnungen 10 Jahre aufzubewahren.

Siehe [§ 257 HGB](#) und [§ 14b UStG](#).

- Siehe auch [Art. 17 DSGVO](#) für die Pflicht zur Löschung.

Rechtmäßigkeit der Datenverarbeitung (7)

Weiteres:

- Im **BDSG** ergänzen § 22–31 die Rechtsgrundlagen für die Verarbeitung personenbezogener Daten, insbesondere bezieht sich **§ 26 BDSG** auf Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses.
- Falls eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der Betroffenen hat, ist vorab eine Datenschutz-Folgenabschätzung erforderlich.
 - Siehe **Art. 35 DSGVO**. Es kann außerdem eine vorherige Konsultation der Aufsichtsbehörde nötig sein (**Art. 36 DSGVO**).
- Die **DSGVO** gilt nicht für ausschließlich persönliche oder familiäre Tätigkeiten (**Art. 2 (2) DSGVO**).

Wenn man Fotos ins Internet stellt, ist es nicht mehr ausschließlich persönlich.

Datenschutzbeauftragte (1)

- Öffentliche Stellen, die personenbezogene Daten verarbeiten, müssen einen Datenschutzbeauftragten bestellen.
- Ebenso Firmen, deren Kerntätigkeit darin besteht, systematische Überwachung von Personen durchzuführen oder sensible Daten (Folie 29) in großem Umfang zu verarbeiten (**Art. 37 DSGVO**).
- Firmen, bei denen mindestens 20 Mitarbeiter mit der Verarbeitung personenbezogener Daten beschäftigt sind, brauchen auch einen Datenschutzbeauftragten (**§ 38 BDSG**).
- Der Datenschutzbeauftragte muss Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis haben.
- Er/Sie ist in Ausübung dieser Tätigkeit weisungsfrei.

Datenschutzbeauftragte (2)

- Es darf keinen Interessenskonflikt geben (**Art. 38 DSGVO**).
Z.B. Geschäftsführer und IT-Abteilungsleiter kommen nicht in Frage.
- Der/Die Datenschutzbeauftragte muss der Aufsichtsbehörde gemeldet werden und Kontaktdaten müssen (z.B. auf der Webseite) veröffentlicht werden.
- Aufgaben des Datenschutzbeauftragten (**Art. 39 DSGVO**):
 - Beratung des Managements (des Verantwortlichen),
 - Schulung der Benutzer in den Datenschutz-Vorschriften,
 - Überwachung der Einhaltung der Rechtsvorschriften,
 - Zusammenarbeit mit der Aufsichtsbehörde,
 - Ansprechpartner für betroffene Personen (**§ 6 (5) BDSG**).

Informationspflicht (1)

- Wenn Daten bei der betroffenen Person erhoben werden, sind folgende Informationen mitzuteilen (**Art. 13 DSGVO**):
 - Name und Kontaktdaten des Verantwortlichen, sowie ggf. des Datenschutzbeauftragten,
 - die Zwecke, für die die personenbezogenen Daten verarbeitet werden, sowie die Rechtsgrundlage für die Verarbeitung, Im Falle von „berechtigten Interessen“ sind diese aufzulisten. Könnte die Person die Daten auch nicht bereitstellen, mit welchen Konsequenzen?
 - Informationen zur Weitergabe der Daten,
 - die Dauer der Speicherung (bzw. Kriterien dafür),
 - Aufklärung über Rechte des Betroffenen
Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Widerspruchsrecht, Datenübertragbarkeit, Widerruf einer Einwilligung, Beschwerderecht bei Aufsichtsbehörde.

Informationspflicht (2)

- Für automatisierte Entscheidungsfindung gibt es zusätzliche Regeln (**Art. 22 DSGVO**), wozu auch die Offenlegung der Logik gehören kann (**Art. 13 DSGVO**).
- Wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben werden, ergibt **Art. 14 DSGVO** im Prinzip die gleichen Informationspflichten, jetzt aber mit mehr Ausnahme-Möglichkeiten.
- Man braucht sowohl für Online- wie für Offline-Verarbeitung personenbezogener Daten eine Datenschutzerklärung.

Beispiel: [<https://www.ldi.nrw.de/datenschutz/medien-und-technik/websites-muster-fuer-datenschutzhinweise>]

Verzeichnis von Verarbeitungstätigkeiten (1)

- Jeder Verantwortliche muss ein „Verzeichnis von Verarbeitungstätigkeiten“ führen und dieses auf Anfrage der Aufsichtsbehörde zur Verfügung stellen (**Art. 30 DSGVO**).
- Dies enthält Namen und Kontaktdaten des Verantwortlichen und ggf. des Datenschutzbeauftragten und pro Tätigkeit:
 - Zweck der Verarbeitung,
 - Kategorien betroffener Personen,
 - Kategorien personenbezogener Daten,
 - Kategorien von Empfängern,
 - Das können auch die eigenen Mitarbeiter sein, die zugriffsberechtigt sind.
Besonders kritisch: Datenübermittlungen in ein Drittland.
 - Fristen für Löschung (soweit möglich).

Verzeichnis von Verarbeitungstätigkeiten (2)

- Außerdem müssen technische und organisatorische Maßnahmen (TOMs) für die Sicherheit der Daten dokumentiert werden (**Art. 32 DSGVO**).

Man darf es Hackern nicht allzu leicht machen, sondern muss sich um Sicherheit auf dem aktuellen Stand der Technik kümmern.

Negativ-Beispiel: Account eines Dienstleisters war 5 Jahre nach Vertragsende nicht gesperrt, Bankdaten inkl. Postident/Personalausweis-Kopie entwendet: **Urteil LG München I, 09.12.2021** (2500 € Schmerzensgeld). Weiteres Urteil für anderen Kunden: **LG Köln 28 O 328/21** (1200 €). 33.200 Kunden betroffen.

- Einfaches Beispiel eines Verzeichnisses von Verarbeitungstätigkeiten (Einzelhändler):

[https://www.lda.bayern.de/media/muster/muster_12_einzelhaendler_verzeichnis.pdf]

[https://www.lda.bayern.de/media/dsk_muster_vov_verantwortlicher.pdf]

Rechte der betroffenen Personen (1)

Recht auf Auskunft:

- Nach **Art. 15 DSGVO** hat die betroffene Person das Recht, eine Bestätigung zu bekommen, ob sie betreffende personenbezogene Daten verarbeitet werden, und falls ja, folgende Informationen zu bekommen:
 - Verarbeitungszwecke,
 - Kategorien personenbezogener Daten,
 - Empfänger gegenüber denen die Daten offengelegt wurden oder noch werden,
 - Speicherdauer,
 - falls die Daten nicht bei der betroffenen Person erhoben wurden, alle verfügbaren Informationen zur Herkunft der Daten,

Rechte der betroffenen Personen (2)

Recht auf Auskunft, Forts.:

- Zu liefernde Informationen, Forts.:
 - Hinweis auf Rechte,
 - im Falle einer automatisierten Entscheidungsfindung Informationen zur Logik, Tragweite, angestrebten Auswirkungen,

Dies bezieht sich nur auf automatisierte Entscheidungsfindung gemäß [Art. 22 DSGVO](#) (1) und (4), was ohnehin rechtlich kritisch ist. Der Begriff „Profiling“ ist definiert in [Art. 4 Nr. 4 DSGVO](#), und enthält z.B. die Bewertung/Analyse/Vorhersage der wirtschaftlichen Lage, von Vorlieben/Interessen oder des Aufenthaltsorts.
 - Im Falle der Übermittlung in ein Drittland die geeigneten Garantien für den Datenschutz und durchsetzbare Rechte ([Art. 46 DSGVO](#)).

Rechte der betroffenen Personen (3)

Recht auf Auskunft, Forts.:

- Dem Recht auf Auskunft muss normalerweise kostenlos entsprochen werden.

Es kann nur abgelehnt werden, wenn es offensichtlich unbegründet ist oder rechtsmissbräuchlich erfolgt, also exzessiv häufig neu angefragt wird.

In diesem Fall kann auch ein Entgelt verlangt werden ([Art. 12 \(5\) DSGVO](#)).

- Es ist wichtig, dass Auskünfte nur an die betroffene Person gegeben werden (erfordert Identitätsfeststellung).

Z.B. schickt die Schufa die [Datenkopie nach Art. 15 DS-GVO](#) per Post an die Meldeadresse. Andere Unternehmen verlangen eine Personalausweis-Kopie (Teile dürfen darauf geschwärzt sein). Wenn die Person z.B. als Kunde ein Login in einem Webshop hat, sind die Daten des Benutzerkontos dort ohnehin einsehbar, und es könnte nach dem Login auch eine Zusammenstellung der Daten nach DSGVO angeboten werden.

Rechte der betroffenen Personen (4)

Recht auf Auskunft, Forts.:

- Der Bundesbeauftragte für Datenschutz und die Informationsfreiheit (BfDI) sagt, dass die Auskunft auch Kopien von Korrespondenz enthalten muss (also nicht nur Zeilen der DB).

[https://www.bfdi.bund.de/DE/Buerger/Inhalte/Allgemein/Betroffenenrechte/Betroffenenrechte_Auskunftsrecht.html]

- Das Bundesdatenschutzgesetz (§ 34 BDSG) enthält einige Einschränkungen.

Das Auskunftsrecht besteht nicht, wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder nur Zwecken der Datensicherung und der Datenschutzkontrolle dienen, und die Auskunftserteilung unverhältnismäßigen Aufwand erfordern würde. Backup-Medien müssen also nicht durchsucht werden. Weitere Ausnahmen, wenn zivilrechtliche Ansprüche oder die öffentliche Sicherheit und Ordnung gefährdet sind.

Rechte der betroffenen Personen (5)

Musterschreiben Auskunftsrecht:

- (Quelle: Landesbeauftragter für Datenschutz und Informationsfreiheit Baden-Württemberg)

In den Erläuterungen zum Schreiben wird auf die Identifizierbarkeit hingewiesen. Dazu sollen Sie neben der vollständigen Adresse z.B. Kunden- und/oder Rechnungsnummer angeben (eventuell auch das Geburtsdatum). Besonders bei einem Antwortwunsch per EMail ist die Identifizierung wichtig.

- Hiermit erbitte ich von Ihnen gemäß Art. 15 Abs. 1 DS-GVO unentgeltliche und schriftliche Auskunft, ob Sie mich betreffende personenbezogene Daten verarbeiten (Definition des Begriffs „Verarbeitung“ siehe Art. 4 Nr. 2 DS-GVO).
- Falls ja, schließe ich folgende Fragen an:
 - ... (siehe folgende Folien)

Rechte der betroffenen Personen (9)

Recht auf Berichtigung:

- Nach **Art. 16 DSGVO** hat die betroffene Person das Recht, die Berichtigung sie betreffender falscher Daten zu verlangen.

Dieses muss „unverzüglich“ geschehen. Auch die Vervollständigung unvollständiger Daten kann verlangt werden (machmal entsteht ein unrichtiger Eindruck gerade durch das Fehlen von Einträgen).

- Falls die Richtigkeit von personenbezogenen Daten bestritten wird, und die Überprüfung etwas länger dauert, kann in der Zwischenzeit auch die „Einschränkung der Verarbeitung“ nach **Art. 18 DSGVO** verlangt werden.

Das bedeutet effektiv, dass die Daten als „gelöscht markiert“ werden, also nicht mehr in die normalen Verarbeitungsprozesse einbezogen werden. Zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen und bei einem wichtigen öffentlichen Interesse dürfen sie allerdings verwendet werden.

Rechte der betroffenen Personen (10)

Recht auf Löschung / Recht auf „Vergessenwerden“:

- In den folgenden Fällen können die betroffenen Personen verlangen, dass Daten über sie gelöscht werden, und dies muss dann auch unverzüglich geschehen (**Art. 17 DSGVO**):

- Die Daten sind für den ursprünglichen Zweck nicht mehr nötig.

- Die betroffene Person widerruft ihre Einwilligung.

Und es gibt keine andere Rechtsgrundlage für die Verarbeitung der Daten.

- Wenn die Daten „aus berechtigtem Interesse“ gespeichert wurden, kann die betroffene Person ihr Widerspruchsrecht nach **Art. 21 DSGVO** ausüben.

Dies geht immer für den Zweck der Direktwerbung, ansonsten muss die betroffene Person es mit ihrer besonderen Situation begründen, und es ist ggf. mit zwingenden schutzwürdigen Gründen abzuwägen.

Datenpannen (1)

- Eine Verletzung des Schutzes personenbezogener Daten („Datenpanne“, **Art. 4 Nr. 12 DSGVO**) liegt vor, wenn z.B.
 - eine Email mit personenbezogenen Daten an den falschen Empfänger geschickt wurde,
 - Es ist auch nicht ok, eine Rundmail an eine große Zahl von Empfängern so zu verschicken, dass sie alle anderen Adressen sehen können (→ bcc).
 - ein Hacker Zugriff auf den Rechner bekommt,
 - Und Dateien mit personenbezogenen Daten kopiert.
 - ein USB-Stick mit personenbezogenen Daten verloren geht,
 - Und die Daten nicht verschlüsselt waren.
 - ein Notebook/Smartphone mit solchen Daten gestohlen wird,
 - Z.B. auch, wenn gebrauchte Notebooks verkauft werden, und eigentlich gelöschte Dateien darauf noch wiederhergestellt werden können.
 - Daten gelöscht wurden, die noch wichtig sein könnten.

Datenpannen (2)

- Nach **Art. 33 DSGVO** muss eine Datenpanne unverzüglich und möglichst binnen 72 Stunden an die zuständige Aufsichtsbehörde (**Art. 55 DSGVO**) gemeldet werden,
Die 72 Stunden beginnen vom Zeitpunkt der Kenntnis (durch irgendeinen Mitarbeiter) und werden auch durch Wochenende/Feiertage nicht unterbrochen.
- es sei denn, die Verletzung des Schutzes personenbezogener Daten führt voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen.
Beispiel für geringes Risiko (**Landesbeauftragter für Datenschutz Niedersachsen**):
Falsche Anlage zu Hotelrechnung: Nur Namen und gebuchte Daten, aber keine Adressen oder gar Bankverbindungen.
- Für Inhalte der Meldepflicht siehe **Art. 33 (3) DSGVO**.
Sie enthält auch eine Beschreibung der wahrscheinlichen Folgen und Maßnahmen zur Behebung der Schutzverletzung und zur Abmilderung ihrer negativen Folgen.

Datenpannen (3)

- Bei „voraussichtlich hohem Risiko für die persönlichen Rechte und Freiheiten“ müssen nach **Art. 34 DSGVO** die betroffenen Personen unverzüglich informiert werden.

Der Europäische Datenschutzausschuss (**EDSA/ EDPB**) hat in den **Leitlinien 01/2021** Beispiele für die Meldung von Verletzungen des Schutzes personenbezogener Daten zusammengestellt.

- Wenn z.B. Kreditkartendaten bekannt geworden sind, kann der Betroffene seine Kreditkarte sperren lassen.
- Natürlich kann der Betroffene die Firma dann auf Schadensersatz und Schmerzensgeld verklagen.

Selbst wenn das Schmerzensgeld (ohne objektiv zu beziffernden Schaden) in Deutschland im einzelnen Fall nicht besonders hoch ist, kann es sich bei vielen Betroffenen natürlich aufsummieren.

Literatur/Quellen

- Michael Rohlich: Datenschutz einfach umsetzen. Akademische Arbeitsgemeinschaft, 2023, ISBN 978-3-96533-286-7, 264 Seiten.
- Bayerisches Landesamt für Datenschutzaufsicht (Hrsg.): Erste Hilfe zur Datenschutz-Grundverordnung für Unternehmen und Vereine. C.H.Beck, 2017, ISBN 978-3-406-71662-1, 64 Seiten.
- Ralph Wagner: Vorlesung Datenschutzrecht. TU Dresden, Sommersemester 2018. [https://tu-dresden.de/ing/informatik/sya/ps/ressourcen/dateien/studium/materialien/mat_datenschutzrecht/1-Teil-Vorlesung-DS-Recht.pdf]
- Dresdner Institut für Datenschutz: Arbeitshilfen. [<https://www.dids.de/arbeitshilfen/>]
- Ruth Janal: Vorlesung Technikrecht — Datenschutz: Einführung. [<https://www.zivilrecht8.uni-bayreuth.de/pool/dokumente/PDFs/6-Datenschutz.pdf>]
- Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: Tätigkeitsbericht 2023. [<https://www.datenschutzzentrum.de/tb/tb41/>]
- Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI): Datenschutz-Grundverordnung - Bundesdatenschutzgesetz - Texte und Erläuterungen. [<https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Broschueren/INFO1.html>]
- Datenschutzkonferenz. [<https://www.datenschutzkonferenz-online.de/>]
- EDSA: Datenschutzleitfaden für kleine Unternehmen. [https://www.edpb.europa.eu/sme-data-protection-guide/home_de]