Ralf Kneuper

Datenschutz für Softwareentwicklung und IT

Eine praxisorientierte Einführung

EBOOK INSIDE

Springer Vieweg

Datenschutz für Softwareentwicklung und IT

Ralf Kneuper

Datenschutz für Softwareentwicklung und IT

Eine praxisorientierte Einführung

Springer Vieweg

Ralf Kneuper
Darmstadt, Hessen, Deutschland

ISBN 978-3-662-63086-0 ISBN 978-3-662-63087-7 (eBook)
https://doi.org/10.1007/978-3-662-63087-7

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Planung/Lektorat: David Imgrund
Springer Vieweg ist ein Imprint der eingetragenen Gesellschaft Springer-Verlag GmbH, DE und ist ein Teil von Springer Nature.
Die Anschrift der Gesellschaft ist: Heidelberger Platz 3, 14197 Berlin, Germany

Vorwort

Spätestens seit der Einführung der europäischen Datenschutz-Grundverordnung (DSGVO), die seit dem 25. Mai 2018 anzuwenden ist, hat der Datenschutz in der Öffentlichkeit eine große Aufmerksamkeit erhalten. Diese Aufmerksamkeit war allerdings bei weitem nicht immer positiv, verursacht u.a. durch teilweise überschweifende Interpretationen und Angstmache, die seither veröffentlicht wurden.

Ein wesentliches Ziel dieses Buches ist es daher, eine realistische Einführung in das Thema Datenschutz zu geben. Anders als die Bezeichnung nahelegt, befasst der Datenschutz sich nicht mit dem Schutz von Daten, sondern mit dem Schutz von Personen vor *Missbrauch* ihrer persönlichen Daten. Darüber hinaus geht es um das Recht, selbst darüber zu bestimmen, welche persönlichen Daten anderen mitgeteilt werden und von diesen genutzt werden dürfen. Im täglichen Leben überlässt man ständig persönliche Daten an Dritte, sei es der Arbeitgeber, ein Arzt, ein Online Shop, oder ein soziales Netzwerk. Dies geschieht üblicherweise im Vertrauen darauf, dass diese Daten angemessen (z. B. nur für den vereinbarten Zweck) genutzt und nicht missbraucht werden, wobei es sehr unterschiedliche Meinungen gibt, was das genau bedeutet. Regelungen zum Datenschutz wie die DSGVO formalisieren und konkretisieren diese Erwartungen und definieren, was als „angemessene Nutzung“ und was als „Missbrauch“ von personenbezogenen Daten zu verstehen ist.

Da die Verarbeitung dieser personenbezogenen Daten naturgemäß zu einem erheblichen Anteil durch Software und IT gestaltet und umgesetzt wird, tragen Softwareentwicklung und IT auch einen erheblichen Teil der Verantwortung dafür, wie dies geschieht. Das vorliegende Buch soll dabei helfen, diese Verantwortung angemessen und kompetent umzusetzen.

Zielgruppen des Buches sind daher in erster Linie Softwareentwickler, IT-Berater, Anforderungsanalytiker und Projektleiter in IT-Projekten, aber auch Datenschutz-Verantwortliche und Datenschutzbeauftragte im Umfeld von Softwareentwicklung und IT. Eine eindeutige Abgrenzung zwischen Datenschutzthemen, die diese Zielgruppen betreffen und anderen Themen ist allerdings nicht möglich, da Softwareentwicklung fast alle Geschäftsprozesse einer Organisation betreffen kann. Der Schwerpunkt dieses Buches wird aber auf die typischerweise für die genannte Zielgruppe besonders

relevanten Themen gelegt, einschließlich der direkten Auswirkungen des Datenschutzes auf die Softwareentwicklung, beispielsweise in Form funktionaler Anforderungen an Softwaresysteme, die sich aus dem Datenschutz ergeben. Der spätere Betrieb der Software wird ebenfalls betrachtet, hat aber eine geringere Bedeutung, da die wesentlichen Datenschutzaspekte im Rahmen der Entwicklung festgelegt werden. Der wichtigste Beitrag des IT-Betriebs besteht in der Gewährleistung der IT-Sicherheit für die betrachtete Software und die gesamte Infrastruktur.

Wichtig ist in diesem Kontext die Unterscheidung zwischen der Entwicklung von Individual-Software, meist im Auftrag eines Kunden, und der Entwicklung von Standard-Software. Bei Standard-Software trägt die Entwicklungsorganisation einen deutlich größeren Anteil der Verantwortung, dass die Software die relevanten gesetzlichen Regelungen, in diesem Kontext also die des Datenschutzes, erfüllt, während bei Individual-Software mehr Verantwortung beim Kunden/Auftraggeber liegt.

Rechtliche Hinweise Da dieses Buch an vielen Stellen auf der DSGVO aufbaut, ist es empfehlenswert, beim Lesen ein Exemplar dieser Verordnung greifbar zu haben.[1] Einzelne, in diesem Kontext besonders wichtige Ausschnitte der DSGVO sind auch in Anhang A dieses Buches enthalten. Ergänzend dazu geht das Buch an relevanten Stellen auch auf wesentliche Aspekte nationaler Gesetzgebungen im deutschsprachigen Raum ein, insbesondere das Bundesdatenschutzgesetz in Deutschland, das Datenschutzgesetz in Österreich, sowie – außerhalb der EU und damit nicht auf der DSGVO aufbauend – dem Schweizer Bundesgesetz über den Datenschutz. Referenz ist in allen diesen Fällen der zum Zeitpunkt des Schreibens Ende 2020 gültige Stand der Gesetze.

Ausgerichtet an der Zielgruppe orientiert sich die Beschreibung an der DSGVO, aber der Schwerpunkt liegt auf den grundsätzlichen Konzepten des Datenschutzes und ist daher unabhängig von den Details der aktuellen Gesetzeslage. Im Gegenteil haben viele Aussagen sogar über Europa hinaus Gültigkeit, aber das kann natürlich nicht für alle Aussagen gelten.

Dazu kommt, dass es bei rechtlichen Regelungen nicht immer eindeutig ist, wie diese zu interpretieren sind, und die Entscheidung darüber letzten Endes bei den zuständigen Gerichten liegt. Bei einem relativ neuen Gesetz wie der DSGVO, zu der es noch wenig Rechtsprechung gibt, gibt es daher derzeit noch besonders viele offene Fragen. Daher kann der Autor natürlich keine Haftung für die rechtlichen Aussagen übernehmen, sondern nur dafür, dass sie nach bestem Wissen und Gewissen auf Basis des aktuellen

[1] Die DSGVO ist kostenlos verfügbar, beispielsweise elektronisch direkt bei der EU in den verschiedenen EU-Sprachen unter https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504 oder als Informationsbroschüre der deutschen Bundesbeauftragten für Datenschutz und Informationsfreiheit unter https://www.bfdi.bund.de/SharedDocs/Publikationen/Infobroschueren/INFO1.html?nn=5217204.

Informationsstandes zusammengetragen wurden, und offene Fragen nach Möglichkeit als solche benannt werden.

Im Zweifel sollte daher im konkreten Fall ein IT-Jurist oder anderer Datenschutz-Spezialist herangezogen werden. In diesem Fall hilft dieses Buch aber, zumindest die richtigen Fragen zu stellen und die juristisch formulierten Antworten zu verstehen und umzusetzen.

Fallstudien und Beispiele Zum besseren Verständnis der behandelten Inhalte werden die folgenden Fallstudien über das gesamte Buch hinweg verwendet, die jeweils ein bestimmtes Unternehmen und seine Umsetzung des Datenschutzes beschreiben. Auch wenn diese Unternehmen in exakt dieser Form nicht existieren, so orientiert sich ihre Beschreibung doch stark an tatsächlich existierenden Unternehmen.

Fallstudie 0.1. (Online-Shop) Bei dem hier betrachteten Unternehmen handelt es sich um einen Online-Shop mit Web-Präsenz, Kundenverwaltung im Back-Office und einem externen Dienstleister für Lagerhaltung und Versand.

Dabei ist allerdings zu beachten, dass das Online-Marketing in seinen vielen Varianten nur mit Einschränkungen zur Softwareentwicklung gehört und daher hier nur oberflächlich betrachtet wird. Gerade ist die Interpretation der gesetzlichen Vorgaben auch noch stärker im Fluss als bei anderen Themen. Um hier tiefer einzusteigen, sollte daher aktuelle Spezialliteratur oder der Rat spezialisierter Datenschutzfachleute oder IT-Anwälte eingeholt werden.

Fallstudie 0.2. (Softwarehaus) Als zweites Unternehmen wird ein Softwarehaus betrachtet, das Anwendungen und Werkzeuge zur Datenanalyse für Kundenunternehmen entwickelt. Teilweise werden die entsprechenden Anwendungen und Werkzeuge dem jeweiligen Kunden bereitgestellt, teilweise werden auch die Auswertungen selbst beim Softwarehaus durchgeführt. Das betrachtete Softwarehaus hat seinen Hauptsitz in Deutschland und ein rechtlich selbständiges kleines Tochterunternehmen in Österreich.

Zusätzlich zu den Fallstudien gibt es eine Reihe von Beispielen zu den jeweils behandelten Themen, die ebenfalls in einer grauen Box dargestellt werden und die sich ebenfalls an tatsächlich existierenden Unternehmen orientieren, auch wenn diese zur Anonymisierung etwas verändert beschrieben sind.

Beispiel 0.1. (Beispiel zum Thema) Dies ist ein Beispiel zum aktuellen Thema.

Aufbau des Buches Kap. 1 führt in das Thema ein und gibt dazu einen ersten Überblick über die Grundbegriffe des Datenschutzes sowie über die relevanten gesetzlichen Grundlagen.

Das folgende Kap. 2 geht dann tiefer auf die DSGVO ein, insbesondere die wesentlichen Grundkonzepte, Begrifflichkeiten, und Anforderungen, allerdings noch weitgehend allgemein und ohne deren spezielle Interpretation im Kontext von Software und IT zu betrachten.

Diese spezielle Umsetzung und Interpretation der DSGVO-Forderungen bei Software und IT wird dann ab Kap. 3 behandelt, beginnend mit den in der DSGVO definierten Grundsätzen des Datenschutzes (Kap. 3) und den Rechten der Betroffenen (Kap. 4).

An der Verarbeitung von Daten sind häufig mehrere Organisationen beteiligt, die jeweils unterschiedliche Rollen übernehmen und die Daten nach Bedarf untereinander austauschen, beispielsweise im Fall der Auftragsverarbeitung durch einen Dienstleister. Kap. 5 behandelt die dafür relevanten Konstellationen, die rechtlichen Rahmenbedingungen und deren praktische Umsetzung.

Während die bisherige Diskussion sich auf die Betrachtung einzelner Anforderungen und deren Umsetzung konzentrierte, betrachtet Kap. 6 allgemeiner die technische und organisatorische Gestaltung des Datenschutzes, insbesondere seine Einbettung in den Softwarelebenszyklus, sowie das in der DSGVO geforderte Konzept des Datenschutzes durch Technikgestaltung *(Privacy/Data Protection by Design).*

Eine wesentliche Grundlage für die Umsetzung des Datenschutzes ist die IT-Sicherheit. Kap. 7 gibt daher einen Überblick über dieses Thema, natürlich mit Schwerpunkt auf die für den Datenschutz relevanten Aspekte.

Softwareentwicklung und IT sind allerdings nicht nur Gestalter des Datenschutzes für andere Organisationen, sondern auch selbst Betroffene, deren Daten beispielsweise in Entwicklungswerkzeugen erfasst und verarbeitet werden, und die Datenschutz für die eigene Organisation umsetzen müssen. Dieses Thema wird in Kap. 8 behandelt.

In den Anhängen sind die in diesem Zusammenhang wichtigsten Ausschnitte aus der Charta der Grundrechte der EU und der DSGVO enthalten, außerdem ein Glossar der wichtigsten verwendeten Begriffe.

Darmstadt Ralf Kneuper
Januar 2021

Danksagung

Zum Abschluss möchte ich all jenen danken, die zu diesem Buch beigetragen haben. Benedikt Buchner, Alexander Feder, Michaela Moser, Ilona Paukert-Kneuper, Mark Perlitz und Jörg Sawatzki haben Vorabversionen ganz oder teilweise Korrektur gelesen und damit geholfen, das Buch klarer zu formulieren und Fehler zu beheben.

Inhaltsübersicht

Inhaltsverzeichnis

Über den Autor

Ralf Kneuper ist Professor für Wirtschaftsinformatik und Informatik an der IU Internationale Hochschule im Bereich Fernstudium. Daneben berät er Unternehmen zu Softwarequalitätsmanagement, Prozessverbesserung und Datenschutz und ist TÜV-zertifizierter externer Datenschutzbeauftragter.

Abkürzungsverzeichnis

AVV	Auftragsverarbeitungsvereinbarung
BDSG	Bundesdatenschutzgesetz (Deutschland)
BDSG a. F.	Bundesdatenschutzgesetz alte Fassung, gültig bis 24.05.2018 (Deutschland)
BDSG n. F.	Bundesdatenschutzgesetz neue Fassung, gültig ab 25.05.2018 (Deutschland)
CPO	Chief Privacy Officer
DPO	Data Protection Officer
DSAnpUG	Datenschutz-Anpassungs- und Umsetzungsgesetz (Deutschland)
DSB	Datenschutzbeauftragter
DSB	Österreichische Datenschutzbehörde
DSFA	Datenschutz-Folgenabschätzung
DSG	Datenschutzgesetz (Österreich)
DSG a. F.	Datenschutzgesetz alte Fassung, gültig bis 24.05.2018 (Österreich)
DSG n. F.	Datenschutzgesetz neue Fassung, gültig ab 25.05.2018 (Österreich)
DSG	Bundesgesetz über den Datenschutz (Schweiz)
DSGVO	Datenschutz-Grundverordnung
DSK	Datenschutzkonferenz (Gremium der deutschen DS-Aufsichtsbehörden)
EDÖB	Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter (Schweiz)
EG	Erwägungsgrund (in der DSGVO)
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWR	Europäischer Wirtschaftsraum (EU plus Island, Liechtenstein und Norwegen)
GDPR	General Data Protection Regulation (englischsprachige Version der DSGVO)
ITK-System	IT- und Kommunikationssystem
pbD	personenbezogene Daten
SDM	Standard-Datenschutzmodell
TOM	technische und organisatorische Maßnahme(n)
VDSG	Verordnung zum Bundesgesetz über den Datenschutz (Schweiz)

Einführung

1

Zusammenfassung

Datenschutz dient – anders als die Bezeichnung nahelegt – nicht dem Schutz von Daten, sondern dem Schutz von Individuen vor Missbrauch ihrer Daten. Trotzdem wird der Datenschutz oft als bürokratisches Hindernis betrachtet, das es zu umgehen gilt, wenn man es schon nicht ignorieren kann. Angestoßen durch die europäische Datenschutz-Grundverordnung hat der Datenschutz in der EU und darüber hinaus aber 2018 einen wesentlich höheren Stellenwert bekommen. Das hat auch Auswirkungen auf Softwareentwicklung und IT, einerseits in ihrer Rolle als Gestalter des Datenschutzes, andererseits als selbst vom Datenschutz Betroffene. Das vorliegende Kapitel gibt daher eine Einführung in die Grundideen des Datenschutzes, und die Rolle sowie die Verantwortung von Softwareentwicklung und IT in diesem Kontext. Ergänzt wird diese Einführung durch einen ersten Überblick über die relevanten rechtlichen Grundlagen, insbesondere die Datenschutz-Grundverordnung und andere Referenzmodelle für den Datenschutz.

1.1 Grundbegriffe des Datenschutzes

Datenschutz ist ein Thema, das vor allem mit der europäischen Datenschutzgrundverordnung (DSGVO) sehr an Bedeutung und an Aufmerksamkeit gewonnen hat, in erster Linie natürlich in Europa, aber auch weit darüber hinaus. Bevor im Weiteren die Anforderungen des Datenschutzes und ihre Umsetzung im Rahmen von Softwareentwicklung und IT weiter diskutiert werden, ist zuerst einmal wichtig zu verstehen, worum es beim Datenschutz geht und welche Ziele damit verfolgt werden. Leider ist die Bezeichnung „Datenschutz“ irreführend, und wird dementsprechend auch häufig falsch interpretiert: Beim Datenschutz geht

R. Kneuper, *Datenschutz für Softwareentwicklung und IT,*
https://doi.org/10.1007/978-3-662-63087-7_1

es um den Schutz von *Personen*[1] vor unangemessener Verarbeitung oder Missbrauch ihrer Daten, und damit nur indirekt um den Schutz der Daten selbst. Kern des Datenschutzes ist das Recht des Einzelnen, selbst darüber zu entscheiden, was mit seinen persönlichen Daten geschieht und wer diese in welchem Umfang verwenden darf. Dementsprechend befasst sich der Datenschutz auch nur mit *personenbezogenen Daten* (pbD) und nicht mit anderen möglicherweise ebenfalls vertraulichen Daten (z. B. Konstruktionsdaten oder Finanzdaten), auch wenn die verwendeten Schutzmechanismen oft identisch sind und die Umsetzung des Datenschutzes daher meist gleichzeitig dem Schutz anderer vertraulicher Daten dient. Wenn daher in diesem Buch von „Daten" die Rede ist, dann sind damit *personenbezogene* Daten gemeint, auch wenn das nicht immer explizit formuliert wird.

Als Grundlage für die weitere Diskussion und insbesondere ihre Umsetzung in Softwareentwicklung und IT sollen zuerst einige grundlegende Ideen und Begriffe des Datenschutzes eingeführt werden.

Datenschutz ist entstanden als eine Ausprägung des *allgemeinen Persönlichkeitsrechtes* und daraus abgeleitet dem *Recht auf informationelle Selbstbestimmung.* Auch wenn man „nichts zu verbergen" hat, ist es ein wichtiger Aspekt der persönlichen Freiheit, nicht ständig unter Beobachtung zu stehen, wie dies bereits im sogenannten *Volkszählungsurteil* des deutschen Bundesverfassungsgerichtes von 1983 formuliert wurde:

> Mit dem Recht auf informationelle Selbstbestimmung wären eine Gesellschaftsordnung und eine diese ermöglichende Rechtsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß. Wer unsicher ist, ob abweichende Verhaltensweisen jederzeit notiert und als Information dauerhaft gespeichert, verwendet oder weitergegeben werden, wird versuchen, nicht durch solche Verhaltensweisen aufzufallen. […] Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist. (BVerfG, Urteil des Ersten Senats vom 15. Dezember 1983–1 BvR 209/83 –, Rn. 146) [2]

Aus den gleichen Gründen wurde der Datenschutz auch u. a. in die *Charta der Grundrechte der Europäischen Union* aufgenommen, siehe Anhang A.

Dabei ist Datenschutz aber kein völlig neues Konzept, sondern in diversen Varianten wie beispielsweise als Beichtgeheimnis oder Bankgeheimnis schon lange verbreitet. Mit den neuen Möglichkeiten der elektronischen Datenverarbeitung und dem massiv steigenden Umfang der Datennutzung wuchs gegen Ende des 20. Jahrhunderts auch der Bedarf an einer Begrenzung und an Schutz vor einer unangemessenen Nutzung dieser Möglichkeiten stark an. Die Verarbeitung der Daten führt in den meisten Fällen zu einem deutlichen Machtungleichgewicht zwischen den für die Verarbeitung Verantwortlichen und den von

---

[1] In diesem Buch wird der Begriff der „Person" immer im Sinne einer *natürlichen Person* verwendet. Rechtlich gesehen gibt es auch *juristische Personen,* beispielsweise Unternehmen oder Vereine, aber diese sind im Kontext des Datenschutzes nach DSGVO nicht relevant.

[2] Verfügbar unter http://www.bverfg.de/e/rs19831215_1bvr020983.html.

der Verarbeitung Betroffenen, deren Daten also verarbeitet werden, weil sie beispielsweise ein bestimmtes Produkt gekauft haben, eine bestimmte Webseite besuchen oder bei einem bestimmten Unternehmen arbeiten.

Leider führt der Datenschutz auch zu einigen bürokratischen Hürden, die gerade kleinen und mittleren Unternehmen das Leben stellenweise erschweren. Wie die Erfahrung der letzten Jahre gezeigt hat, nützt eine Lockerung dieser Regelungen aber nicht wirklich diesen kleinen und mittleren Unternehmen, sondern erleichtert vor allem den großen Monopolisten die Sammlung und Nutzung personenbezogener Daten, da es diesen leichter fällt, die Datenerhebung und sonstige Verarbeitung juristisch korrekt umzusetzen und dabei rechtliche Grenzen auszuloten. Das Internet neigt zur Monopolisierung, und ohne Regulierung wird dieser Mechanismus unterstützt [Wei19].

Grundsätze des Datenschutzes Die wesentlichen Ideen des Datenschutzes werden durch einige Grundsätze oder Prinzipien beschrieben, die in leichten Variationen in allen relevanten Regelwerken verwendet werden, im englischen Sprachraum teilweise bekannt als „Fair Information Practice Principles“ (FIPP). Die in der DSGVO verwendete Variante wird in Abschn. 2.5 ausführlicher behandelt. Die folgende Aufstellung fasst als Alternativbeispiel die in ISO/IEC 29100 (vgl. Abschn. 1.3) definierten Grundsätze zusammen (Übersetzung durch den Autor):

1. *Einwilligung und Wahlfreiheit* (consent and choice): Die Betroffenen haben grundsätzlich die Wahl, ob ihre Daten verarbeitet werden oder nicht.
2. *Legitimer, festgelegter Zweck* (purpose legitimacy and specification): Personenbezogene Daten werden nur für einen rechtlich erlaubten und festgelegten Zweck verarbeitet.
3. *Beschränkte Erfassung* (collection limitation): Daten werden nur gesammelt, soweit das rechtlich erlaubt und jeweiligen Zweck notwendig ist.
4. *Datenminimierung* (data minimization): Dieses Prinzip erweitert die beschränkte Erfassung und fordert, dass auch die weitere Verarbeitung der Daten auf das notwendige Maß beschränkt wird.
5. *Beschränkte Nutzung, Aufbewahrung und Weitergabe* (use, retention and disclosure limitation): Die Nutzung, Aufbewahrung und Weitergabe der Daten wird auf das notwendige Maß beschränkt.
6. *Genauigkeit und Qualität* (accuracy and quality): Es wird sichergestellt, dass die verarbeiteten Daten genau, vollständig und aktuell sind.
7. *Offenheit, Transparenz und Auskunft* (openness, transparency and notice): Die Betroffenen erhalten offene und transparente Information über die Art und Weise sowie den Zweck der Verarbeitung ihrer Daten.
8. *Beteiligung und Zugang der Betroffenen* (individual participation and access): Die Betroffenen erhalten Zugang zu ihren Daten und können diese prüfen und ggf. Korrekturen, Ergänzungen oder die Löschung dieser Daten fordern.

9. *Rechenschaftspflicht* (accountability): Es werden geeignete Arbeitsabläufe dokumentiert und kommuniziert, um die Vorgaben des Datenschutzes einzuhalten und bei Vorfällen entsprechend zu handeln und die Betroffenen zu informieren.
10. *Informationssicherheit* (information security): Die Vertraulichkeit, Integrität und Verfügbarkeit der Daten werden gegen externe Einflüsse oder Angriffe geschützt.
11. *Datenschutz-Compliance* (privacy compliance): Die Einhaltung der Vorgaben zum Datenschutz wird nachgewiesen und durch geeignete Prüfmechanismen überprüft.

Konkretisiert wurden diese bisher eher abstrakt formulierten Erwartungen an den Datenschutz dann in Gesetzen, wobei die Datenschutzgrundverordnung (DSGVO) der EU derzeit sicher die größte Bedeutung hat und daher in diesem Buch im Vordergrund steht. Darüber hinaus gibt es viele weitere relevante Gesetze wie beispielsweise das in jedem EU-Staat vorhandene nationale Datenschutzgesetz, das die DSGVO in ausgewählten Punkten ergänzt und konkretisiert. Abschn. 1.2 gibt einen ersten Überblick über diese gesetzlichen Grundlagen innerhalb der EU und darüber hinaus.

„Data Protection“ und „Privacy“ Die unterschiedlichen Bedeutungen des Begriffes „Datenschutz“ werden noch etwas deutlicher, wenn man sich die in englischen Texten in diesem Kontext verwendeten Begriffe betrachtet, nämlich „Data Protection“ und „Privacy“. Diese sind nicht identisch, auch wenn nicht immer streng zwischen beiden unterschieden wird. Im englischen Kulturraum ist meist der Begriff „Data Protection“ verbreitet, während im amerikanischen Kulturraum meist von „Privacy“ die Rede ist. Darüber hinaus fokussiert sich „Privacy“ meist auf die technische Sicherstellung der Vertraulichkeit, während „Data Protection“ etwas weiter gesehen wird und auch die Rechte der Betroffenen, beispielsweise auf Auskunft, einschließt. Dabei handelt es sich aber um keine strenge Abgrenzung, beispielsweise nutzt auch die ISO/IEC 29100, aus der die oben gelisteten Datenschutzprinzipien stammen, die Bezeichnung „Privacy“.

Gefährdungen Beim Thema Datenschutz denken viele zunächst nur daran, dass die persönlichen Daten Unbefugten bekannt werden, dass also die Vertraulichkeit der Daten gefährdet ist. Darüber hinaus gibt es aber viele weitere Gefährdungen des Datenschutzes, wie Solove in der in Abb. 1.1 dargestellten Taxonomie beschrieben hat. Datenschutz hat damit die Aufgabe, gegen all diese Gefährdungen zu schützen.

Datenanalyse Datenanalysen können einzelne Personen auch betreffen, ohne deren personenbezogene Daten zu berücksichtigen oder auch nur zu kennen: Wenn die Datenanalyse beispielsweise zeigt, dass Bewohner einer bestimmten Region durchschnittlich ein geringes Einkommen haben und eine hohe Wahrscheinlichkeit, Kredite nicht zurückzuzahlen, dann kann das auch Auswirkungen auf Personen in dieser Region haben, die nicht in der Datenanalyse berücksichtigt wurden und für die diese Feststellungen nicht zutreffen.

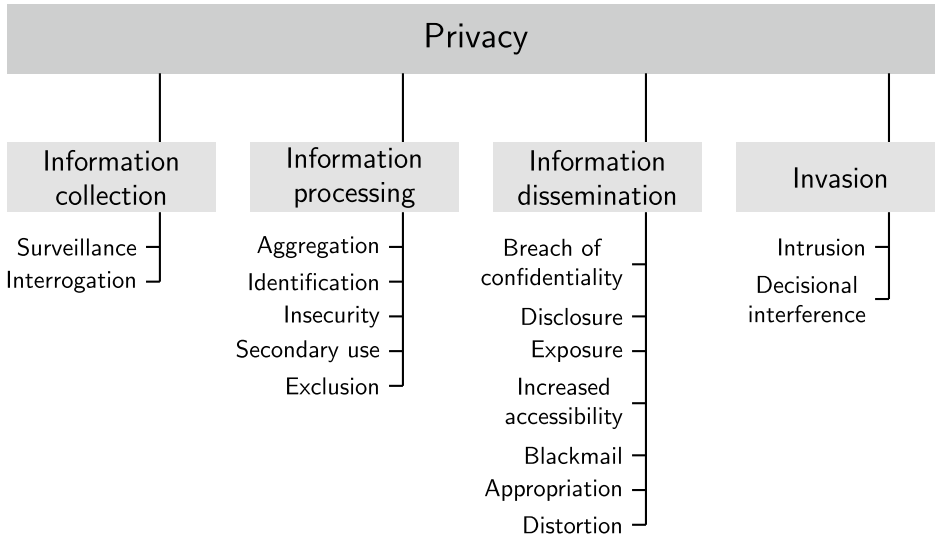

Abb. 1.1 Taxonomie der Datenschutz-Gefährdungen nach Solove [Sol06]

Die Rechtmäßigkeit derartiger Analysen, die also zu verschiedenen Formen von Diskriminierung einschließlich Rassismus führen können, ist sicher eine wichtige ethische und rechtliche Frage. Sie wird aber in diesem Buch entsprechend der üblichen, auch in gesetzlichen Regelungen wie der DSGVO verwendeten Sichtweise als vom Datenschutz separates Thema betrachtet und daher auch in diesem Buch nicht weiter betrachtet.

1.2 Gesetzliche Grundlagen

Um die Erwartungen der betroffenen Personen bei der Verarbeitung ihrer persönlichen Daten zu konkretisieren und um das dabei meist bestehende Machtungleichgewicht zwischen den Betroffenen und den datenverarbeitenden Organisationen wenigstens teilweise auszugleichen, gibt es in den meisten Staaten Gesetze zum Datenschutz, die festlegen, welche dieser Erwartungen in dem jeweiligen Geltungsbereich als legitim angesehen werden und einzuhalten sind. Innerhalb der EU gilt hier seit 2018 die DSGVO, die in den einzelnen EU-Staaten durch nationale Datenschutzgesetze ergänzt wird, siehe Abb. 1.2.

Im Folgenden soll ein kurzer Überblick über die gesetzlichen Grundlagen des Datenschutzes, mit Schwerpunkt auf der DSGVO im deutschsprachigen Raum, gegeben werden, der dann in den folgenden Kapiteln vertieft wird.

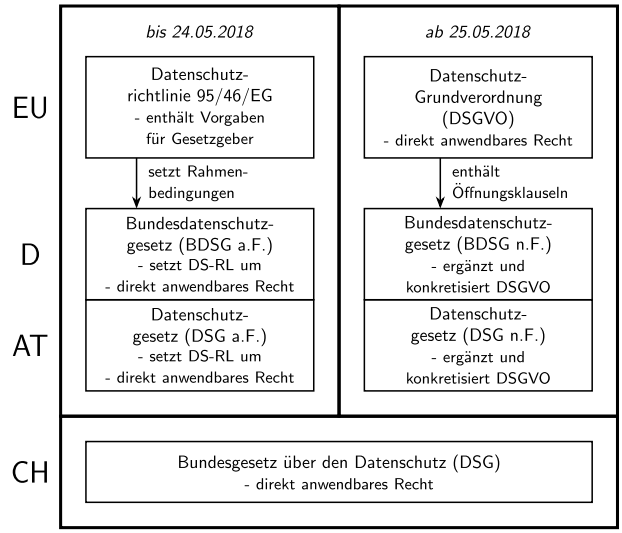

Abb. 1.2 Wesentliche gesetzliche Grundlagen für Datenschutz in Deutschland, Österreich und der Schweiz

1.2.1 Die Datenschutz-Grundverordnung (DSGVO)

Die DSGVO wurde 2016 nach langen Diskussionen als Nachfolger der europäischen Datenschutzrichtlinie 95/46/EG verabschiedet.[3] Zwischen beiden Gesetzen gibt es einen grundsätzlichen Unterschied: EU-Richtlinien wie die genannte Datenschutzrichtlinie enthalten Vorgaben für die jeweiligen Gesetzgeber aller EU-Staaten und müssen von diesen in nationale Gesetze überführt werden. EU-Verordnungen dagegen, beispielsweise die DSGVO, enthalten direkt in allen EU-Staaten anwendbares Recht, wie in Abb. 1.2 dargestellt. Dieses EU-Recht hat damit im Zweifelsfall auch Vorrang vor dem nationalen Recht der Einzelstaaten. Das wirft derzeit viele offene Fragen auf, da nicht immer eindeutig ist, inwieweit bestimmte nationale Regelungen als weiterhin geltende Konkretisierung oder als im Widerspruch zur DSGVO stehende und damit abgelöste Regelungen gelten. Beispiele für solche derzeit offene Diskussionen sind das deutsche Kunsturhebergesetz (KUG), das u. a. in §§ 22–24 Regelungen zum „Recht am eigenen Bild“ enthält, oder das noch nicht angepasste ebenfalls deutsche Telemediengesetz (TMG)[4].

Da die DSGVO in den verschiedenen EU-Sprachen verabschiedet wurde, gibt es natürlich auch unterschiedliche Namen und Abkürzungen dieser Verordnung. Im englischsprachigen Ausland ist die DSGVO bekannt unter dem Namen „General Data Protection Regulation“ (GDPR).

---

[3] Der Film „Democracy – Im Rausch der Daten“ (siehe http://www.democracy-film.de/) gibt einen guten Einblick in diese Diskussionen und die Hintergründe der Entstehung der DSGVO.

[4] Zum Stand des Telemediengesetzes gibt es eine Stellungnahme der deutschen Datenschutzbehörden, siehe https://www.datenschutz.rlp.de/fileadmin/lfdi/Dokumente/Orientierungshilfen/DSK_Positionsbestimmung_TMG.pdf.

Ein grundlegendes Prinzip der DSGVO, das bereits in der Richtlinie 95/46/EG enthalten war, ist das „Verbot mit Erlaubnisvorbehalt", d. h. die Verarbeitung von personenbezogenen Daten ist grundsätzlich verboten, wenn sie nicht ausdrücklich erlaubt ist.

„Öffnungsklauseln" Neben den für alle EU-Staaten einheitlichen Regelungen enthält die DSGVO auch eine Reihe von meist als „Öffnungsklauseln"[5] bezeichneten Stellen, an denen den einzelnen EU-Staaten ausdrücklich die Möglichkeit gegeben wird, die allgemeinen Regelungen auszugestalten, so beispielsweise bei der Altergrenze, ab der Jugendliche selbst in die Verarbeitung ihrer Daten einwilligen können (Art. 8 Nr. 1 DSGVO). Dies hat naturgemäß zur Folge, dass die gesetzlichen Regelungen zum Datenschutz gegenüber der Situation vor der DSGVO EU-weit einheitlicher geworden sind, aber weiterhin nicht völlig einheitlich – fmit allen damit verbundenen Vor- und Nachteilen.

1.2.2 Das deutsche Bundesdatenschutzgesetz (BDSG)

Die bis 24.05.2018 gültige Fassung des Bundesdatenschutzgesetzes war ein eigenständiges Gesetz, das die in Deutschland für privatwirtschaftliche Organisationen sowie für Bundesbehörden geltenden Regelungen zum Datenschutz beschrieb. Mit der Einführung der DSGVO wurden die meisten dieser Regelungen abgelöst bzw. in die DSGVO übernommen, so dass parallel zur DSGVO eine völlig überarbeitete Fassung des BDSG (meist als neue Fassung BDSG n. F. bezeichnet, im Gegensatz zur alten Fassung BDSG a. F.) eingeführt wurde. Das BDSG n. F. hat in erster Linie die Aufgabe, die in den Öffnungsklauseln der DSGVO definierten Entscheidungsspielräume auszufüllen, und stellt damit nur noch eine kleine Ergänzung zur DSGVO dar, kein eigenständiges Regelwerk.[6]

Neben dem BDSG n. F. gibt es noch eine Reihe weiterer deutscher Gesetze mit Bezug zum Datenschutz, die aber deutlich geringere praktische Bedeutung haben und hier daher i. A. nicht weiter betrachtet werden sollen. Dazu gehören beispielsweise die Landesdatenschutzgesetze der einzelnen Bundesländer, die einerseits den rechtlichen Rahmen für die Arbeit der Landesdatenschutzbeauftragten als Aufsichtsbehörde festlegen, andererseits Vorgaben zum Datenschutz analog dem BDSG n. F. definieren, allerdings mit Landesbehörden und kommunalen Behörden als Regelungsadressaten. Für ausgewählte Anwendungsbereiche gibt es auch spezielle Datenschutzregelungen, so beispielsweise für Sozialdaten im zehnten Sozialgesetzbuch (SGB X), oder für den Datenschutz innerhalb der Kirchen.

---

[5] Juristisch gesehen handelt es sich hierbei in den meisten Fällen allerdings nicht wirklich um Öffnungsklauseln, da diese Klauseln Ergänzungen und Verfeinerungen, aber keine Abweichungen von der DSGVO zulassen.

[6] Formal gesehen wurden die neue Fassung des BDSG sowie die Anpassungen der anderen betroffenen Gesetze durch das sogenannte *Datenschutz-Anpassungs- und Umsetzungsgesetz (DSAnpUG)* eingeführt, ein sogenanntes *Artikelgesetz,* dessen Inhalt also darin besteht, andere Gesetze zu einem bestimmten Aufgabenbereich zu ändern. In diesem Fall wurde durch das 1. DSAnpUG eine Vielzahl von Regelungen zum Datenschutz in verschiedenen Gesetzen an die DSGVO angepasst, ergänzt und teilweise geändert durch das 2. DSAnpUG von 2019.