



Leseprobe aus Heugel und Gudehus, mini-handbuch
Datenschutz für Trainer und Coaches,
ISBN 978-3-407-36787-7 © 2022 Beltz Verlag, Weinheim Basel
[http://www.beltz.de/de/nc/verlagsgruppe-beltz/
gesamtprogramm.html?isbn=978-3-407-36787-7](http://www.beltz.de/de/nc/verlagsgruppe-beltz/gesamtprogramm.html?isbn=978-3-407-36787-7)

Inhaltsverzeichnis

TEIL I

Es geht los 8

Wie Sie dieses Buch verwenden können 10

Dank 11

DSGVO: Einfacher als gedacht 12

Rechte 13

Die DSGVO aus Sicht der Verantwortlichen 20

Definitionen: Was bedeutet »Daten verarbeiten?« 20

Wann darf ich personenbezogene Daten verarbeiten? 24

Compliance 28

Was bedeutet »Daten schützen?« 29

Warum müssen die Daten überhaupt geschützt werden? 31

Gegenmaßnahmen 32

Die Aufsicht 34

Meldepflichten 35

Sanktionen 36

Datenschutzbeauftragter 38

Auftragsverarbeitung 43

Positive Kriterien für eine Auftragsverarbeitung 43

Negative Kriterien für eine Auftragsverarbeitung 44

Auftragsverarbeitungs-Vertrag (AVV) 46

Datenübermittlung in Staaten

außerhalb der Europäischen Union 48

Die Sache mit den Bildern 51

Das Recht am eigenen Bild 51

Bildrechte 54

Webseiten sicher betreiben 57

Impressum 59

Datenschutzhinweise	62
Einbettung von Videos in die Webseite	64
Plug-ins für Soziale Medien und andere Zwecke	65
Cookies und wie wir damit umgehen (sollten)	66

Soziale Medien – Facebook, LinkedIn und Co. 73

Facebook	73
Andere soziale Medien	75

Videokonferenzen 78

Sind Sie verantwortlich?	79
Auch online Regeln gelten lassen	81
Den passenden Dienstleister wählen	84
Dokumentieren	85

TEIL II

Praxisteil oder Herr Meyer schützt die Daten 88

Herr Meyer, guten Tag!	89
Der Start: Herr Meyer hat ein mulmiges Gefühl	90
Herr Meyer fasst einen Entschluss oder:	
Auch die längste Reise beginnt mit dem ersten Schritt	92
Verbündete auf dem Weg: Das Rad nicht neu erfinden	92
In sechs Schritten zum Ziel	93
Schritt 1: Ziel der Datenverarbeitung definieren	94
Schritt 2: Anforderungen an das zukünftige System festlegen	96
Schritt 3: Standort bestimmen: Was ist der aktuelle Stand?	104
Schritt 4: Maßnahmen ableiten	109
Schritt 5: Maßnahmen umsetzen	116
Schritt 6: Erfolgskontrolle	117

Schlusswort 119

DSGVO: Einfacher als gedacht

Dieser Abschnitt gibt einen Überblick über die Datenschutzgrundverordnung, kurz DSGVO. Er ist überhaupt nur deswegen vorhanden, weil wir davon überzeugt sind, dass im Verstehen eine besondere Magie liegt: Das Verstehen macht den Unterschied zwischen »Warum nur macht es jemand auf diese Weise?« und »Aha, darum wird es so gemacht«. Er legt außerdem die Grundlage dafür, dass Sie sinnvolle Fragen stellen können: »Muss ich das tatsächlich machen?« oder »Kann ich etwas auch lassen?«.

Wir stellten nämlich in zahlreichen Gesprächen, Schulungen und Workshops fest, dass die meisten Menschen ein recht unscharfes Konzept im Kopf hatten, wenn es um die DSGVO geht. Dabei ist es nicht so kompliziert. Also, worum geht es im Kern?

Ganz kurz: Die DSGVO gibt allen Menschen bestimmte *Rechte* gegenüber allen, die ihre Daten verarbeiten. Damit das auch tatsächlich funktioniert, *definiert* die DSGVO, was »Verarbeiten von Daten« ist, stellt Regeln auf, an die sich alle Verarbeiter halten müssen (*Compliance*), installiert eine *Aufsicht* und rüstet diese mit scharfen Waffen (*Sanktionen*) aus, damit ein Fehlverhalten so teuer wird, dass es sich nicht lohnt, sich nicht an die Regeln zu halten.

Es geht also um...

- Rechte
- Definitionen
- Compliance
- Aufsicht
- Sanktionen

RECHTE

Die DSGVO definiert Rechte für Menschen. Genauer: Rechte, die Sie haben, wenn jemand anderes Daten über Sie verarbeitet (was »Ihre Daten« sind und was »verarbeiten« bedeutet, wird dabei ganz nebenbei ebenfalls festgelegt). Die DSGVO erlegt Ihnen in Ihrer Rolle als Beraterin also nicht nur Pflichten auf, sondern gewährt Ihnen als Privatperson bestimmte Rechte gegenüber jedem, der Ihre Daten verarbeitet. Rechte und Pflichten bilden quasi einen Spiegel.

Wenn Sie also als Privatperson bestimmte Rechte haben, muss es jemanden geben, der Ihnen gegenüber diese Rechte erfüllen muss. Sie haben es vielleicht schon erraten: das ist der Verarbeiter der Daten. Also Sie, wenn Sie die Daten anderer Menschen verarbeiten.

Grundsätzlich gilt: Der Verarbeiter der Daten ist dafür verantwortlich, dass alle Regeln erfüllt werden. Diese (natürliche oder juristische) Person bleibt auch immer verantwortlich. Wir sagen es nochmals: Immer. Auch wenn Sie Dienstleister dazu beauftragen. Mehr dazu später, zurück zu den Rechten. Dies sind Ihre Rechte aus der DSGVO:

1. Recht auf Transparenz
2. Recht auf Auskunft
3. Recht auf Berichtigung
4. Recht auf Löschung
5. Recht auf Einschränkung der Verarbeitung
6. Recht auf Übertragung der Daten
7. Recht, keiner automatischen Entscheidung unterworfen zu werden

RECHT AUF TRANSPARENZ

Das Recht auf Transparenz bedeutet, dass Sie informiert werden, wenn jemand Ihre Daten verarbeitet. Praktisch umgesetzt wird dies durch einen Text, der beschreibt, was mit Ihren Daten geschieht. Einen Mustertext für Datenschutzhinweise finden Sie in den Online-materialien.

Sie kennen das vielleicht von Banken, Versicherung oder auch Ärzten. Freundliche Menschen fordern, gerne noch mit dem Hinweis »Hier müssen Sie noch schnell für den Datenschutz unterschreiben...«, eine Unterschrift von Ihnen ein. Womit wir schon gleich beim ersten weitverbreiteten Missverständnis sind, denn Ihre Unterschrift (oder Ihre Einwilligung) ist dazu gar nicht nötig. Bestenfalls möchte Ihr Gegenüber dokumentieren, dass Sie die Transparenzhinweise erhalten haben. Schlimmstenfalls sollen Sie in Dinge einwilligen, die Ihr Gegenüber lieber verschleiern möchte.

Der Inhalt eines Transparenzhinweises ist nicht normiert (Sie können also frei formulieren), es müssen jedoch auf jeden Fall einige Elemente enthalten sein:

- Wer genau verarbeitet Ihre Daten (wer ist also verantwortlich)?
- Wozu (was ist der Zweck der Verarbeitung)?
- Gibt es weitere Empfänger Ihrer Daten (werden sie also weitergereicht)?
- Und gibt es einen Datenschutzbeauftragten, an den Sie sich wenden können?

TIPP

► Populärer Irrtum: »Wenn ich Daten verarbeite, brauche ich dazu eine Unterschrift.« Nein, brauchen Sie nicht. Ein Vertrag (auch mündlich) reicht dazu völlig aus. Das machen Sie übrigens genau so beim Einkaufen, wenn Sie mit Karte bezahlen: Dann unterschreiben Sie auch nicht, obwohl der Supermarkt für den Bezahlvorgang eine ganze Menge Ihrer Daten verarbeitet. Mehr dazu weiter unten (»Wann darf ich personenbezogene Daten verarbeiten?«).

► Für Sie als Privatperson: Wann immer von Ihnen jemand verlangt, »für den Datenschutz zu unterschreiben«: Prüfen Sie, was Sie da unterschreiben. Oftmals wird Ihnen dabei die Zustimmung zu etwas vorgelegt (man könnte auch sagen »untergeschoben«). Für einen

Transparenzhinweis genügt eine Formulierung wie »Ich habe die Datenschutzhinweise zur Kenntnis genommen.« Wann immer es ein längerer Text ist: Vorsicht!

► Widerstehen Sie der Versuchung, Ihren Kunden etwas »unterzuschieben«, denn ein solcher Versuch weist darauf hin, dass Sie nicht seriös sind.

RECHT AUF AUSKUNFT

Sie haben als Verbraucher das Recht zu erfahren, welche Daten jemand über Sie verarbeitet. Als Verantwortlicher sind Sie dazu verpflichtet, eben diese Auskunft auf Nachfrage zu erteilen. Das ist nicht abstrakt gemeint (wir verarbeiten Ihren Namen und Ihre Adresse), sondern im Falle einer konkreten Nachfrage ganz konkret: »Max Mustermann, Teststraße 1, 12345 Irgendwo«. Die DSGVO sagt dazu »vollständig und konkret«.

Dieses Recht steht Ihnen immer zu. Wenn jemand keine Daten über Sie verarbeitet, dann besagt die Auskunft genau das (auch »Fehlanzeige« genannt). Sie haben das Recht auf Auskunft also gegenüber jeder Einrichtung, jedem Unternehmen. Sie haben es jedoch nur, wenn die Verarbeitung durch die DSGVO geregelt ist, also im gewerblichem Bereich (Unternehmen) in Behörden oder auch gegenüber Vereinen.

Alle Daten, die privat verarbeitet werden, sind davon nicht erfasst. Die DSGVO liefert Ihnen also nicht die Grundlage dafür, eine Auskunft von Ihrem Nachbarn oder Ihrem Ex-Freund einfordern zu können.

Die Auskunft selbst ist kostenlos. Im Wiederholungsfall können Ihnen allerdings die Kopierkosten berechnet werden.

TIPP

► Nutzen Sie privat einen Dienstleister wie Facebook, WhatsApp, Netflix, Amazon, ...? Oder wollen Sie wissen, was die Schufa über Sie weiß? Wenn Sie wirklich wissen wollen, was über Sie gespeichert wird, fragen Sie nach: »Sehr geehrte Damen und Herren, bitte teilen Sie mir gemäß Artikel 15 der DSGVO mit, welche meiner Daten Sie verarbeiten. Schicken Sie die Auskunft bitte innerhalb der nächsten vier Wochen an die Ihnen bekannte Adresse.«

RECHT AUF BERICHTIGUNG

Sie haben als Verbraucher das Recht, fehlerhafte Daten über Sie korrigieren zu lassen. Das kann ein falsch geschriebener Name oder eine fehlerhafte Adresse sein. Wenn Sie also feststellen, dass jemand Sie nicht in »12345 Irgendwo« sondern in »12345 Nirgendwo« verortet, haben Sie einen Anspruch auf Korrektur.

Es kann aber auch um andere Sachverhalte gehen: Ein Kredit mit falschem Betrag oder eine Bestellung, die Sie nicht tätigten.

Das Recht auf Auskunft ist die Grundlage dafür, dass Sie das Recht auf Berichtigung überhaupt sinnvoll nutzen können, denn nur wenn Sie wissen, dass ein Fehler vorliegt, können Sie eine Berichtigung verlangen. Sie ahnen es schon: Sie als Verantwortliche sind nach einem solchen Verlangen zur Korrektur verpflichtet.

RECHT AUF LÖSCHUNG

Sie dürfen als Verbraucher verlangen, dass über Sie gespeicherte Daten gelöscht werden. Hier steht bewusst »verlangen«, denn dieses Recht ist beschränkt: nämlich auf Daten, die ein Verarbeiter über Sie aus *eigenem Interesse* speichert. Wenn er die Daten speichert, weil er dazu verpflichtet ist (etwa für die Aufbewahrung einer Rechnung, 10 Jahre) oder die Daten benötigt, um einen Vertrag mit Ihnen zu erfüllen, dann haben Sie auch keinen Anspruch auf Löschung.

Auch dieses Recht gilt nur, wenn die DSGVO angewendet wird, also nicht im privaten Bereich.

Für Sie als Verantwortliche gilt: Alle gesetzlichen Bestimmungen, die eine Aufbewahrung von Ihnen verlangen, haben Vorrang vor dem Recht auf Löschung.

RECHT AUF EINSCHRÄNKUNG DER VERARBEITUNG

Vielleicht möchten Sie gar nicht alles löschen lassen, sondern nur bestimmte Informationen. Genau das räumt Ihnen dieses Recht ein. Auch hier gilt wieder die Einschränkung, dass der Verarbeiter der Daten möglicherweise verpflichtet ist, die Daten weiterhin zu nutzen. Sie können aber davon ausgehen, dass die Information, wann Sie »Pause« in einem Film gedrückt haben, der Ihnen durch einen Streaming-Anbieter auf Ihr Tablet geliefert wurde, nicht in diese Kategorie fällt. Sie können etwa verlangen, dass die Daten zwar weiter gespeichert, jedoch nicht mehr verwendet werden dürfen.

TIPP

▸ Das Recht auf Einschränkung der Verarbeitung wird zwar selten genutzt, kann aber unglaublich viel Arbeit machen. Sollten Sie jemals mit einem solchem Begehren konfrontiert werden: Machen Sie aus der Not eine Tugend und löschen Sie alles, was Sie nicht zwingend aufbewahren müssen.

RECHT AUF ÜBERTRAGUNG DER DATEN

Dieses Recht wird in der Praxis bisher noch wenig genutzt (und kann auch nicht gut verwendet werden). Im Kern bedeutet es, dass Ihre Daten von einem Verarbeiter zum nächsten übertragen werden können. Das wäre etwa sinnvoll, wenn Sie einen neuen Arzt aufsuchen, der dann die Daten seines Kollegen über Sie gleich weiter ver-

wenden könnte, etwa die letzten Röntgenbilder und Diagnosen aus der Vergangenheit.

Dazu müsste es zwischen den genutzten Programmen ein (universelles) Verfahren geben, mit der die Übertragung geregelt wird. Und genau diese Schnittstelle gibt es leider nur selten. Für Software, die schon länger im Einsatz ist, gibt es vielfach noch nicht einmal die Möglichkeit, Daten pro Kunde aus dem alten System heraus und in das neue System hinein zu bringen.

TIPP

- Für Sie als Trainer ist dieses Recht Ihrer Kunden derzeit (Stand 2021) praktisch ohne Bedeutung.

RECHT, KEINER AUTOMATISCHEN ENTSCHEIDUNG
UNTERWORFEN ZU WERDEN

Mit diesem Recht können Sie verlangen, dass letztlich ein Mensch und keine Maschine über Sie entscheidet. Wenn also Ihr Kreditantrag nicht bewilligt wird, kann sich Ihr Kreditinstitut nicht damit rechtfertigen, dass »das System es so entschieden« habe. Das gibt Ihnen die Möglichkeit, dem entscheidenden Menschen weitere Informationen zu liefern. Dieser hört Ihnen hoffentlich zu und kann dann seine Entscheidung überdenken.

TIPP

- Dieses Recht ist kein Hebel, um eine unerwünschte Entscheidung rückgängig zu machen: Natürlich verwendet Ihre Bank einen automatischen Mechanismus, um zu berechnen, ob Sie kreditwürdig sind oder nicht. Aus einem »Nein« dieses Systems können Sie keinen Anspruch auf den Kredit ableiten, nur weil es eine automatische Entscheidung ist: Am Ende entscheidet es dann ein Mensch in der

Bank – und in seine Entscheidung fließt die Antwort des Systems natürlich ein.

- Für Sie als Trainer ist auch dieses Recht Ihrer Kunden derzeit (Stand 2021) praktisch ohne Bedeutung.

Damit endet der Überblick über Ihre Rechte. Fazit daraus: Wenn Sie Rechte haben muss jemand anders Pflichten haben. Wer sollte Ihnen sonst Ihre Rechte gewähren? Damit sind Sie im Spiel: Wann immer Sie jenseits des privaten Bereichs Daten über andere Menschen verarbeiten, sind Sie verantwortlich für diese Daten. Die DSGVO spricht auch tatsächlich von »Verantwortlicher«. Und Sie als Verantwortlicher sind es, der dann die Rechte der Menschen erfüllen muss. Daher wechseln wir jetzt die Seite und betrachten die DSGVO aus der Sicht der Verantwortlichen.

Die DSGVO aus Sicht der Verantwortlichen

DEFINITIONEN: WAS BEDEUTET »DATEN VERARBEITEN?«

An dieser Stelle ist es für das Verständnis sinnvoll, einige Begriffe zu klären. Es geht der DSGVO um Daten und deren Verarbeitung. Doch was sind eigentlich »Daten« und was bedeutet »verarbeiten«?

DATEN

»Daten« bezeichnet alles, was Sie in einem Computer speichern können oder speichern *könnten*. Auf die Art des Computers kommt es nicht an (es kann auch ein Smartphone oder ein Tablet sein). »Speichern könnten« bezieht sich besonders auf Informationen auf Papier, also herkömmliche Akten oder handschriftliche Notizen.

TIPP

▸ Eine handgeschriebene Liste über Ihre Mitarbeitenden, deren Krankheiten und Fehlzeiten gehört also auch zu den »Daten«. An dieser Stelle gleich der Hinweis: Sollten Sie eine solche Liste haben: Vernichten Sie sie schleunigst. Überlegen Sie für sich, warum Sie eine solche Liste angefertigt haben. Organisieren Sie für sich Unterstützung, um solches Handeln in Zukunft zu vermeiden.

PERSONENBEZOGENE DATEN

Die DSGVO bezieht sich immer auf *personenbezogene* Daten. Hier geht es also um Daten, die einem Menschen zugeordnet werden können.

Ein Name, eine Adresse oder auch ein Geburtsdatum sind Beispiele für personenbezogene Daten. Auch das Nutzungsverhalten gehört dazu (»hat den Film ›Arrival‹ am 23. September 2021 ab 19:34 Uhr gesehen«, »war auf der Webseite www.mfcd.de« usw.), eine Rechnung, eine Aktennotiz, dass jemand Interesse am Bau eines Hauses äußerte. Überraschenderweise ist auch die IP-Adresse, die beim Besuch einer Webseite genutzt wurde, gehört zu den personenbezogenen Daten. Ebenso eine Videoaufzeichnung, auf der ein Mensch zu sehen ist. Kurz: Alles, was einen Menschen oder seinem Verhalten zuzuordnen ist, sind personenbezogene Daten.

Keine personenbezogenen Daten sind solche, die keinen Bezug zu einem Menschen haben: Die Lottozahlen der letzten Woche, die Temperaturen in Erfurt im Jahr 2020, die Anzahl der Flipchart-Blöcke im Lager. Auch die *reinen* Verkaufszahlen dieses Buches beim Verlag im Jahr 2022 sind ebenfalls noch keine personenbezogenen Daten. Sobald jedoch die Namen der Autoren mit dabei sind, sind es wieder personenbezogene Daten. Hier ist schon zu sehen: Es gibt scheinbar eine Grauzone. Jedoch nur scheinbar: Im Zweifel können und sollten Sie davon ausgehen, dass es sich um personenbezogene Daten handelt.

TIPP

- Auch wenn Sie statt des Namens eine Nummer verwenden, bleiben es immer noch personenbezogene Daten.
- Die DSGVO gilt nicht für den privaten Bereich. Privat meint aber tatsächlich privat und nur privat. Ein Verein ist kein privater Bereich mehr. Und ab dem Moment, in dem Sie freiberuflich oder gewerblich (also für eine Gegenleistung) oder regelmäßig für andere tätig sind und dafür die Daten anderer Menschen verarbeiten, gilt auch für Sie die DSGVO.