WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Seminararbeit

am Institut für Business Information Systems

LV.-Nr.: 4152
im SS 2021

EU-DSGVO:

Ein wirksamer Schutz der Persönlichkeitsrechte der Bürger?

Vanessa Schadl (h11779184)

LV-Leitung: ao.Univ.Prof. Mag. Dr. Rony G. Flatscher

Wien, 28.03.2021

Welthandelsplatz 1, A-1020, Wien
Telefon: +43/1/313 36/4622 ● Telefax: +43/1/313 36/717
Web: www.wu.ac.at/retail

EFMD EQUIS ACCREDITED

WIRTSCHAFTS UNIVERSITÄT WIEN VIENNA UNIVERSITY OF ECONOMICS AND BUSINESS

Eidesstaatliche Erklärung

Ich versichere hiermit:

1. dass ich die Seminararbeit selbstständig verfasst habe, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt und mich auch sonst keiner unerlaubten Hilfe bedient habe.
2. dass ich dieses Thema weder im In- noch im Ausland (einer Beurteilerin/einem Beurteiler zur Begutachtung) in irgendeiner Form als Prüfungsarbeit vorgelegt habe.

Mit der Unterschrift nehme ich zur Kenntnis, dass falsche Angaben studien- und strafrechtliche Konsequenzen haben können.

28.03.2021	
Datum	Unterschrift

Welthandelsplatz 1, A-1020, Wien
Telefon: +43/1/313 36/4622 ● Telefax: +43/1/313 36/717
Web: www.wu.ac.at/retail

Inhaltsverzeichnis

Abbildungsverzeichnis

Abkürzungs- und Begriffsverzeichnis

Abs	Absatz, Auflistung unterhalb des Artikels in Gesetzbüchern
Art	Artikel (auch Paragraf oder §), Überschrift in Gesetzbüchern
Aufsichtsbehörde	vom Mitgliedsstaat eingerichtete Überwachungsbehörde
Auftragsverarbeiter	Person, die im Auftrag des Verantwortlichen handelt
Betroffene Person	Datenverarbeitung einer natürlichen Person
Big Data	große Massenansammlung von willkürlichen Daten
bzw.	Beziehungsweise
Corona	Covid-19 Pandemie (Ausbruch 31.12.2019 in China)
Data Breach	Vergehen der EU-DSGVO Bestimmungen (Datenpanne)
Datenschutz-beauftragte	unternehmerisches Überwachungsorgan zur Einhaltung der DSGVO-Bestimmungen
DSG	Datenschutzgesetz
EU	Europäische Union (Staatenbund mit 27 Mitgliedern)
EU-DSGVO	Europäische Datenschutzgrundverordnung
etc.	Et cetera (und so weiter)
Industrie 4.0	Digitalisierung von Mensch u. Maschine zum Informationsaustausch
Mitgliedsstaat	Staat einer Gemeinschaft, wie z.B. der europäischen Union
Natürliche Person	Person mit einer zuordenbaren Kennung wie den Namen
Personenbezogene Daten	Informationen zur Identifizierung einer Person (Name, Adresse, Wohnort, usw.)
Juristische Person	Unternehmen mit einer Gesellschaftsform
Ratifizieren	völkerrechtlichen Vertrag genehmigen (vom Staatsoberhaupt)
Sensible Daten	personenbezogene Daten besonderer Kategorie, z.B. Meinungen
Union	Europäische Union
usw.	Und so weiter
Verantwortlicher	Person, die über die Datenverarbeitung entscheidet
WKO	Wirtschaftskammer Österreich
z.B.	zum Beispiel

Zusammenfassung

Durch das digitale Zeitalter erlebten viele Unternehmen einen Umbruch in ihrer Marketing- und Verkaufsstrategie. Das Internet wurde zum wesentlichen Treiber und dient zur Verfügbarkeit von weltweiten Kunden für die verschiedenen Unternehmensbranchen. Ein Missbrauch zur Erlangung der personenbezogenen Daten der Kunden sowie deren willkürliche Datenspeicherung stellte sich ein („Big Data“). Viele Unternehmen sind abhängig von diesen Daten und nutzen sie, um personenangepasste Angebote senden zu können, um vom höheren Gewinn zu profitieren und einen Wettbewerbsvorteil gegenüber der Konkurrenz zu erlangen.

Die EU-DSGVO trat am 25. Mai 2016 in Kraft, um dem Datenmissbrauch einen Riegel vorzuschieben. Die Unternehmen hatten bis zum 25.Mai 2018 Zeit, die Bestimmungen der Verordnung umzusetzen. Das Ziel der neuen Verordnung ist dabei eine Vereinheitlichung, wie Unternehmen die Daten von natürlichen Personen verarbeiten dürfen. Alle Informationen einer natürlichen Person dürfen nur mit dem Einverständnis der betreffenden Person gespeichert/verarbeitet werden. Die Verordnung regelt somit die Erhebung, Verarbeitung und Nutzung aller personenbezogenen Daten, für alle in der EU tätigen Unternehmen. Um die Einhaltung der Bestimmungen zu gewährleisten, werden Zuwiderhandlungen mit hohen Sanktionen geahndet.

Das Ziel dieses Aufsatzes ist es, einen Überblick über die einzelnen Bestimmungen der EU-DSGVO in den verschiedenen Teilbereichen zu gewinnen und die Notwendigkeit deren Einführung. Anhand der Fokussierung auf die angewandten Mechanismen zur Erreichung des Datenschutzes soll die Forschungsfrage, ob die EU-DSGVO ein wirksamer Schutz der Persönlichkeitsrechte der Bürger ist, beantwortet werden. Als kritischer Gesichtspunkt soll dabei der Umgang mit sensiblen Daten im medizinischen Bereich dienen. Es soll erforscht werden, ob die Bestimmungen der EU-DSGVO auch in Zeiten von Corona eingehalten werden.

Um die wissenschaftliche Integrität der Arbeit zu gewährleisten, werden ausschließlich einschlägige wissenschaftliche Abhandlungen im Internet, seriöse Fachzeitschriften und Gesetzestexte verwendet. Die notwendigen Gesetzesänderungen werden hauptsächlich aus der Sicht von Österreich betrachtet, durch den geologischen Bezug der Wirtschaftsuniversität Wien und der Tatsache, dass Österreich ein betroffenes Mitgliedsstaat der EU ist (Stand: April 2021). Aus Gründen der leichteren Lesbarkeit wird bevorzugt die männliche Sprachform gewählt und soll aber als geschlechtsneutral gelten.

1 Einleitung

1.1 Theoretischer Rahmen

Die europäische Datenschutzgrundverordnung ist eine Gesetzesverordnung, die vom europäischen Parlament und des Rates am 14. April 2016 beschlossen und am 25. Mai 2016 verabschiedet wurde. Anwendbar wurde die Verordnung ab dem 25. Mai 2018 und musste von allen Unternehmen, die in der EU tätig sind, eingehalten werden. Damit ist sie den nationalen Gesetzgebungen übergeordnet und Richtlinien in Bezug auf Datenschutz wurden abgelöst, um eine einheitliche europäische Standardisierung mit dem Umgang von Daten zu erreichen.

Die EU-DSGVO umfasst dabei mehrere Gesetze mit dem Umgang von personenbezogenen Daten von natürlichen Personen. Es werden dabei Mechanismen mitunter zur Datenerhebung, Datenverarbeitung, Datenspeicherung, Datenlöschung und Datennutzung von personenbezogenen Daten vorgeschrieben. Um die Einhaltung der Vorschriften zu gewährleisten, werden Zuwiderhandlungen mit hohen Sanktionen geahndet. Die Verordnung soll somit den Schutz der Persönlichkeitsrechte der Bürger sicherstellen.

1.2 Inhaltlicher Kontext

Der Schutz natürlicher Personen bei der direkten oder indirekten Verarbeitung personenbezogener oder sensibler Daten durch Unternehmen wurde ein Grundrecht gemäß Art.1 Abs.2 DSGVO.[1] Als Unternehmen sind gemäß Art.4 Abs.18 DSGVO natürliche und juristische Personen eingeschlossen, die eine wirtschaftliche Tätigkeit ausüben, unabhängig von deren Rechtsform (einschließlich Personengesellschaften und Vereinigungen).[2] Als natürliche Person gilt dabei jeder Mensch, der zugleich Träger von Rechten und Pflichten ist und eine juristische Person entsteht automatisch durch die Bekanntgabe eines Rechtsakts (z.B. Gesellschaften oder Vereine).[3] Jedes Unternehmen, welches innerhalb der EU tätig ist (also auch ausländische Betriebe, die Tätigkeiten in der EU durchführen), ist von den Regeln der europäischen Datenschutzgrundverordnung

[1] (Datenschutzgrundverordnung 2016)
[2] (Datenschutzgrundverordnung 2016)
[3] (Oesterreich.gv.at 2021)

betroffen. Unter den Begriff „personenbezogene Daten“, werden alle Daten zusammengefasst, die in irgendeiner Art und Weise den Bezug zu einer natürlichen Person herstellen können (also sprich wie Name, Adresse, Bilder etc.).[4] Sensible Daten (laut DSGVO jetzt besondere Kategorien personenbezogener Daten) beinhalten sowohl genetische und biometrische Informationen, zur eindeutigen Identifizierung einer natürlichen Person, aber auch Gesundheitsdaten und Meinungsbekenntnisse in den verschiedenen Bereichen, wie Religion oder Politik. Biometrische Daten sind dabei Informationen einer natürlichen Person, welche sich aus physischen, physiologischen oder verhaltensbedingten Merkmale ergeben (wie z.B. Gesichtserkennung, Fingerabdruck oder Irisscan) und in sicherheitstechnischen Bereichen Anwendung finden. Genetische Daten sind jene Daten, welche vererbte Eigenschaften einer natürlichen Person aufweisen, die aus einer DNS oder RNS entstanden sind. Der Schutz von Daten oder Informationen, die nicht mehr explizit einer natürlichen Person zugeordnet werden können, sind ebenfalls abgedeckt und werden unter dem Oberbegriff „pseudonymisierte Daten“ zusammengefasst. Nur mit der ausdrücklich frei erteilten Zustimmung der betroffenen natürlichen Person in Bezug auf Datenerhebung, Datenbereitstellung, Datenspeicherung oder Datenvernichtung können Unternehmen die Daten in vordefinierter Art und Weise dieser betroffenen Person verarbeiten. Die Verordnung umfasst dabei einen großen Abdeckungsbereich zur eindeutigen Bestimmung und zur Vermeidung von Sicherheitslücken zum Schutz des Bürgers, allerdings bietet sich auch hier viel Spielraum für die Mitgliedsstaaten und auch Abschwächungen bei speziellen Fällen.

1.3 Historische Entwicklung

Die Vorreiterrolle in Sachen Datenschutz, nimmt 1970 das Bundesland Hessen (Deutschland) ein, mit dem sogenannten „Hessische Datenschutzgesetz 1970“.[5] Das erste österreichische Datenschutzgesetz wurde erst 1978 erlassen.[6] Diese Gesetzesverfassungen beinhalteten mehr oder weniger den Schutz vor Datenmissbrauch, speziell den Schutz von personenbezogenen Daten. Die Gesetzesentwürfe unterlagen dabei aber keinerlei Bestimmungen oder Vorlagen, sodass

[4] (Wko 2021a)
[5] (Lindeverlag o. D.)
[6] (Bundesgesetzblatt für die Republik Österreich 1978)

jeder Staat seine individuell angepassten nationalen Datenschutzregelungen entwerfen konnten. Diese regulatorischen Ansätze boten dem Bürger aber nur einen sehr geringen Schutz seiner personenbezogenen Daten, da viele Einzelheiten (bewusst) ausgelassen wurden, um die Wirtschaft zu schützen. Die erste internationale Datenschutzregelung entstand 1980 mit den OECD-Leitsätzen für multinationale Unternehmen. Die Leitsätze waren ein Meilenstein für den Datenschutz, da dadurch internationale Standards und Prinzipien vorgeschrieben wurden, die den Datenschutz auf eine höhere Ebene beförderte. Die Teilnahme an dem OECD-Projekt war freiwillig und die Nichtteilnahme war nicht an Sanktionen gebunden. Dennoch verfolgten 37 Mitgliedsstaaten die Ansätze und der Begriff „Datenschutz“ wurde dadurch auf der ganzen Welt bekannter und ernster genommen. Die Mitgliedsstaaten verpflichteten sich, nationale Kontaktpunkte einzurichten, um die Verbreitung der Leitsätze voranzutreiben und in ihrem Hoheitsgebiet zu überwachen.[7] Österreich war ebenfalls ein Teilnehmerstaat der OECD und errichtete den österreichischen nationalen Kontaktpunkt (öNKP), um den Datenschutz zu fördern. Inspiriert von der OECD-Initiative trat die Europäische Datenschutzkonvention 1985 durch den Europarat in Kraft. Damit war sie die erste international verbindliche Datenschutzregelung, die eine Übereinkunft der Mitgliedsstaaten beinhaltete. Wichtiges Kernelement war der Schutz vor internationalem Austausch bei der automatischen Verarbeitung der personenbezogenen Daten. Die Datenerhebung erfolgte laut der Konvention nun nach Treu und Glauben und auf rechtmäßige Weise.[8] Österreich gehörte zu den ersten 7 Mitgliedsstaaten, die die Europäische Datenschutzkonvention (Vertrag 108) unterzeichnet hatten und 1988 wurde der Vertag schließlich in Österreich auch ratifiziert.[9] Nach jahrelangen Diskussionen und Entscheidungen, kam es im Oktober 1995 zum nächsten Meilenstein des Datenschutzes. Das europäische Parlament und der Rat haben in Anlehnung an die europäische Datenschutzkonvention die Datenschutzrichtlinie RL 95/46/EG verabschiedet. Zweck der Richtlinie ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten im Binnenmarkt der Mitgliedsstaaten. Die Richtlinie bietet ein gewisses Mindestmaß an Sicherheitsanforderungen und erlaubt es den Mitgliedsstaaten,

[7] (Bundesministerium o. D.)
[8] (Bundeszentrale für politische Bildung 2021)
[9] (Europarat 2021)

zusätzliche Regelungen einzubinden. Die Mitgliedsstaaten verpflichteten sich dabei, die zusätzlich getroffenen Vorgaben in nationale Gesetze zu übertragen und bekamen dafür eine 3-Jahres-Frist. Viele Mitgliedsstaaten waren bei der Übertragung in ein nationales Gesetz säumig und es wurden viele Vertragsverletzungsverfahren eingeleitet.[10] Österreich verabschiedete das DSG 2000 erst 1999 und Deutschland setzte die BDSG erst 2001 in Kraft. Am 25.05.2016 trat schließlich die EU-DSGVO in Kraft und ersetzte somit die Datenschutzrichtlinie. Die Mitgliedstaaten hatten danach 2 Jahre Zeit, ihre zusätzlich getroffenen, nationalen Gesetze der Datenschutzrichtlinie an die Bestimmungen der EU-DSGVO anzupassen. Die Regelungen der Verordnung sind für alle Mitgliedsstaaten sofort bindend und muss nicht in nationale Gesetze umgewandelt werden. Die EU-DSGVO ist aktuell und bildet somit momentan die letzte Station des Datenschutzes, das österreichische Bundesgesetz für Datenschutz (DSG) ergänzt die Verordnung lediglich. Die Datenschutzentwicklung durchlebte schon viele Jahre und es hat sich auch viel entwickelt, um den Bürger vor Datenmissbrauch zu schützen. Dabei ist der Aufwand allein für einen Mitgliedsstaat wie Österreich enorm.[11]

1.4 Motivation der Einführung

Das Ziel des Hessischen Datenschutzgesetzes von 1970 war der Schutz von personenbezogenen Daten und Hessen reagierte damit auf die zunehmende Automatisierung der Datenverarbeitung.[12] Weitere Länder folgten unter dem Aspekt der Gleichstellung und weniger um Sorge der Persönlichkeitsrechte der Bürger, da der Missbrauch von personenbezogenen Daten zwar beachtet wurde, aber keine einheitliche Regelung mit dem Umgang von Daten bzw. Sanktionsmechanismen bei Nichteinhaltung festgelegt wurde.[13] Aufgrund der Tatsache, dass keine Strafen drohten, ignorierten viele Unternehmen die Datenschutzbestimmungen und sammelten weiter die Daten von potenziellen Kunden für den Wettbewerbsvorteil ohne Kenntnisnahme der betroffenen Personen. Die Nichtbeachtung der Datenschutzbestimmungen von den Unternehmen und das Voranschreiten des technologischen Fortschritts mit der Digitalisierung, dienten als Grundlage für die Einführung der Datenschutzrichtlinie 95/46/EG. Das Ziel der Richtlinie war eine einheitliche Harmonisierung der Datenschutzrechte innerhalb der

[10] (Datenschutz.org 2021)
[11] (Arge Daten 2019)
[12] (Datenschutz Hessen o. D.)
[13] (Bundesgesetzblatt für die Republik Österreich 1978)

Mitgliedsstaaten inklusive Sanktionsmaßnahmen. Allerdings war es nur eine grobe Richtlinie und Vorlage für die Mitgliedsstaaten und sie hatten großen Spielraum bei den individuellen Rechtslegungen und Anpassungen, insbesondere bei den Sanktionsmechanismen in Art.24.[14] 1995 war der Wissensstand über das Internet und deren Einsatzmöglichkeiten allerdings nicht vergleichbar mit der heutigen Sicht. Zusätzlich wurden neue technologische Meilensteine erreicht, wie z.B. Big Data, Industrie 4.0, Robotik oder künstliche Intelligenz, was eine Neuerung der Datenschutzbestimmungen dringend erforderlich machte.[15] Die EU-DSGVO folgte dem Ruf und die Verordnung ließ keine inhaltlichen Anpassungen wie bei einer Richtlinie zu. Die Bestimmungen sind für alle, in der EU tätigen, Unternehmen bindend und Zuwiderhandlungen werden zudem mit abschreckenden Bußgeldern geahndet. Die DSGVO soll dabei die Transparenz erhöhen, wie Websites und Unternehmen mit den personenbezogenen Daten umgehen, um endgültig einen Riegel vor den Datenmissbrauch zu schieben und die natürliche Person zu schützen.[16]

2 Anwendungsbereich

2.1 Sachlicher Anwendungsbereich

Dieser Absatz fasst den sachlichen Anwendungsbereich gemäß Art.2 DSGVO zusammen.[17] Die Verordnung gilt für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Ausgeschlossen sind dabei Tätigkeiten, die nicht in den Anwendungsbereich des Unionsrechts fallen (z.B. Tätigkeiten für die nationale Sicherheit), Tätigkeiten für den privaten oder familiären Gebrauch oder auch Tätigkeiten zur Strafverfolgung und Strafvollstreckung. Dabei gilt die Verordnung ausschließlich zum Schutz von natürlichen Personen. Der Datenschutz für juristische Personen und Grauzonen wie manuelle Dateien, die keiner Ordnung unterliegen, werden nicht erfasst (z.B. ungeordnete Akten in Papierform).[18]

[14] (Amtsblatt Nr. L 281 1995)
[15] (Ionos 2021)
[16] (Debitoor o. D.)
[17] (Datenschutzgrundverordnung 2016)
[18] (Wko 2021b)

2.2 Räumlicher Anwendungsbereich

Dieser Absatz fasst den räumlichen Anwendungsbereich gemäß Art.3 DSGVO zusammen.[19] Die Verordnung gilt für alle Unternehmen, sofern eine Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union existiert und die Tätigkeit der Verarbeitung von personenbezogenen Daten innerhalb oder außerhalb der EU ausgeführt wird. Beim Sitz des Verantwortlichen oder des Auftragsverarbeiters außerhalb der EU, greift die Verordnung bei Tätigkeiten wie Verhaltensbeobachtungen und Waren-/ Dienstleistungsangebote, sofern die betroffene Person innerhalb der EU ist und unabhängig davon, ob die betroffene Person eine Zahlung zu leisten hat. Bei einem nicht in der EU niedergelassenen Verantwortlichen an einem Ort, der aufgrund Völkerrechts dem Recht eines Mitgliedsstaates unterliegt, greifen ebenfalls die Bestimmungen der DSGVO.

2.3 Zeitlicher Anwendungsbereich

Die Bestimmungen der EU-DSGVO sind ab dem 25. Mai 2018 für alle Mitgliedsstaaten der EU einzuhalten und gelten danach zeitlich uneingeschränkt. Eine EU-Verordnung ist nationalem Recht übergeordnet und eine Aufhebung oder Abänderung der Bestimmungen, kann nur direkt von dem europäischen Parlament und des Rates mit plausibler Begründung oder bei einer Änderung der gesetzlichen Grundlage erfolgen.[20] Bei einer Vertragsverletzung kann eine Klage beim Gerichtshof erfolgen und eine Verordnung als nichtig erklärt werden, wie bei der Rechtssache Isoglukose (Urteil vom 29. Oktober 1980, Rechtssachen 138 und 139/79).[21] Ein weiterer Fall, der zur Aufhebung einer EU-Verordnung führte, war die Veröffentlichung von Subventionen in der Agrarwirtschaft und damit ein Verstoß gegen Grundrechte.[22]

3 Rechte & Pflichten

3.1 Unternehmen

[19] (Datenschutzgrundverordnung 2016)
[20] (Rechtsinformationssystem des Bundes 2008)
[21] (Europäisches Parlament 2021)
[22] (Ennöckl 2010)

Alle Unternehmen, die die Tätigkeit der Verarbeitung von personenbezogenen Daten einer natürlichen Person innerhalb der EU ausüben, sind von den Pflichten der EU-DSGVO betroffen, unabhängig von deren Niederlassung oder Rechtsform. In der Datenschutzgrundverordnung werden juristische Personen nicht erfasst und haben demnach auch kein Recht in Bezug auf Datenschutz. In der früheren österreichischen Gesetzesverfassung „DSG 2000“ waren unter dem Begriff „Betroffener“ neben den natürlichen Personen auch juristische Personen und Personengemeinschaften angeführt, deren Schutz bei der Verarbeitung ihrer personenbezogenen Daten nun mit der DSGVO verfällt.[23]

3.1.1 Datenverarbeitung

Der Begriff „Verarbeitung“ vereint gemäß Art.4 Abs.2 DSGVO 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.[24] Damit sind alle Tätigkeiten in Bezug auf personenbezogene Daten abgedeckt, um den Schutz des Bürgers zu gewährleisten. Bei einer Datenverarbeitung ist der Verantwortliche jene natürliche oder juristische Person, die über die Rahmenbedingungen der personenbezogenen Daten entscheidet und in allen Belangen bei Missbrauch oder Nichteinhaltung der Bestimmungen haftet. Vollzogen werden kann die Datenverarbeitung direkt von den Verantwortlichen oder von einem Auftragsverarbeiter, der im Interesse des Verantwortlichen handelt. Bei der Datenverarbeitung müssen die Bestimmungen über die Grundsätze (Art.5 DSGVO) und die Rechtmäßigkeit der Verarbeitung (Art.6 DSGVO) beachtet und eingehalten werden. Der folgende Absatz fasst die wesentlichen Kerninhalte der beiden Artikel zusammen:[25]

[23] (Preslmayr Rechtsanwälte 2019)
[24] (Datenschutzgrundverordnung 2016)
[25] (Vgl. Feiler und Horn 2018, 10-11)

Es dürfen nur jene personenbezogenen Daten verarbeitet werden, die wirklich benötigt werden und man damit einen begründbaren legitimen Zweck verfolgt. Die Verarbeitung von personenbezogenen Daten muss auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren und transparenten Art und Weise erfolgen. Es dürfen auch nur Daten weiterverarbeitet werden, für die man eine ausdrückliche Einwilligung der betroffenen Person erhält. Der Grundsatz der Datenminimierung muss eingehalten werden, da man nur so viele Daten speichern darf, wie für die Durchführung der Verarbeitungszwecke benötigt werden. Die Integrität und Darstellung der Daten müssen korrekt sein, wenn diese für die Verarbeitungszwecke benötigt werden. Die Daten müssen aktuell gehalten werden und auf Anfrage des Betroffenen auch abgeändert oder gelöscht werden. Die gespeicherten personenbezogenen Daten dürfen nur so lange aufbewahrt werden, wie der Verarbeitungszweck es vorsieht und der betroffenen Person auch vermittelt worden ist. Nach Ablauf der vereinbarten Frist müssen die Daten unwiderruflich gelöscht werden und dürfen nicht weiterhin gespeichert werden, mit Ausnahme der ausdrücklichen Einverständniserklärung der betroffenen Person. Für die Datenverarbeitung müssen auch geeignete Mechanismen innerhalb der Organisation durchgeführt werden, um die Sicherheit der gewonnenen personenbezogenen Daten zu gewährleisten und zu schützen. Eine Rechenschaftspflicht ist für Unternehmen bindend, da sie nachweisen müssen, dass die Bestimmungen der DSGVO auch eingehalten werden. Eine Datenverarbeitung außerhalb der Einverständniserklärung der betroffenen Person ist nur in speziellen Ausnahmefällen rechtens, unter anderem wenn die Verarbeitung im Interesse der betroffenen Person wäre, um ihr Leben retten zu können oder, wenn die Verarbeitung im öffentlichen Interesse geschieht, zwecks Strafverfolgung.

Sobald die Kerntätigkeit des Unternehmens der Verarbeitung von personenbezogenen oder sensiblen Daten entspricht oder wenn mehr als 9 Personen im Unternehmen sich mit der Verarbeitung von personenbezogenen Daten befassen, ist das Unternehmen verpflichtet, einen internen oder externen Datenschutzbeauftragten zu bestellen.[26] Kerntätigkeiten umfassen dabei eine umfangreiche Verarbeitung von sensiblen oder strafrechtlich relevanten Daten sowie eine systematische Überwachung von Personen.

[26] (Siebert, Brünen und Lexow 2021)

Ein Datenschutzbeauftragter überwacht und koordiniert die Datenverarbeitung und ist verpflichtet, bei Verstößen den Verantwortlichen zu informieren, dass er seiner Meldepflicht an die Aufsichtsbehörde unverzüglich nachkommen muss. Weiters ist es jedem Unternehmen gestattet, freiwillig einen Datenschutzbeauftragten zu bestellen, auch wenn das Unternehmen dazu nicht verpflichtet wäre. Die Option des externen Datenschutzbeauftragten dient für Unternehmen, welche aufgrund der internen Unternehmensstruktur nicht in der Lage sind, einen zu wählen, ohne einen Interessenkonflikt auszulösen. Behörden und öffentliche Stellen sind jedenfalls immer dazu verpflichtet, einen Datenschutzbeauftragten zu bestellen.

3.1.2 Verantwortlicher

Der Verantwortliche ist jene Person, die über die Verarbeitung von personenbezogenen Daten entscheidet und die Einhaltung der DSGVO-Bestimmungen, insbesondere der Grundsätze gemäß Art.5 DSGVO, für seine Organisation übernimmt. Dabei kann es sich um eine natürliche Person handeln, wie den Geschäftsführer eines kleinen Unternehmens, aber auch direkt die juristische Person als Ganzes, wie z. B. bei Großkonzernen. Der Verantwortliche ist die haftende Person bei Verstößen und der erste Ansprechpartner bei Problemen. Bei der Ausführung ist er dazu verpflichtet, technische und organisatorische Maßnahmen zu treffen, um die Einhaltung der Bestimmungen zu gewährleisten. Die DSGVO schreibt ihm dabei viele Pflichten, aber auch Rechte für die Zielerreichung vor.

3.1.2.1 Informationspflicht

Der Verantwortliche hat gegenüber den betroffenen Personen, von denen die Daten verarbeitet werden sollen, vorher eine Informationspflicht zu erfüllen, gemäß Art.13 DSGVO. Dabei ist die betroffene Person direkt zum Zeitpunkt der Datenerhebung, umfassend über die Verarbeitungsvorgänge zu informieren.[27] Die Informationspflicht obliegt dabei keiner vordefinierten Form und kann individuell verfasst werden, sie muss aber in einer einfachen verständlichen Sprache, transparent und auf leicht zugänglichem Wege für die betroffene Person, übermitteln werden (siehe Abbildung 1). Der

[27] (Dataprotect 2018)

Verantwortliche hat darauf zu achten, dass bestimmte Fragestellungen geklärt und entsprechend kommuniziert werden, z. B.: Wer ist der Verantwortliche und wie wird er erreicht? Welchen Zweck hat es die Daten zu verarbeiten? Welche Daten sind betroffen? Auf welcher Rechtsgrundlage basiert die Datenverarbeitung? Erfolgt eine Übermittlung der Daten an Dritte? Welche Rechte hat die betroffenen Personen laut DSGVO? Wie lange soll die Verarbeitung der personenbezogenen Daten erfolgen? Welche organisatorischen und technischen Maßnahmen werden gesetzt, um den Schutz der personenbezogenen Daten zu gewährleisten?[28] Die Datenverarbeitung ist erst bei einer Einverständniserklärung der betroffenen Person und bei strikter Einhaltung, der in der Informationspflicht kommunizierten Fakten, regelkonform.

3.1.2.2 Auskunftspflicht

Binnen 1 Monat nach Erhalt der Anfrage der betroffenen Person hat der Verantwortliche Zeit, Auskunft über die Verarbeitung der sie betreffenden personenbezogenen Daten zu geben, gemäß Art.15 DSGVO.[29] Die Identität der betroffenen Person kann dabei vom Verantwortlichen verlangt werden, um die Daten nicht an Falsche zu senden und damit ein Data Breach auszulösen. Die Auskunft umfasst dabei Kopien aller, konkret oder in irgendeiner Art und Weise in Verbindung stehenden gespeicherten Daten der betroffenen Person, inklusive Erhebungsgrundlage und Herkunft der Daten, Verarbeitungszweck, Zugriff für Dritte, Sicherheitsmaßnahmen und Dauer der Speicherung (siehe Abbildung 2). Der Verantwortliche muss die gewünschte Auskunft unentgeltlich und in elektronischer Form übermitteln. Dem Wunsch nach Anpassung oder Löschung der Daten, als Reaktion auf die Auskunft der betroffenen Person, muss nachgegangen und dies muss auch bewiesen werden.

3.1.2.3 Mitteilungspflicht

Gemäß Art.19 DSGVO, muss der Verantwortliche nach jeder Anpassung oder Löschung der personenbezogenen Daten, alle Empfänger der Daten davon in Kenntnis setzen. Eine Mitteilung an die betroffene Person über die Empfänger ist nur nach Wunsch der betroffenen Person erforderlich. Wenn der Verantwortliche beweisen kann, dass die

[28] (Datenschutz Praxis 2019)
[29] (PVE o. D.)

Mitteilung unmöglich oder mit zu viel Aufwand verbunden wäre, kann die Mitteilungspflicht erlassen werden und der Zuständigkeitsbereich wird von der entsprechenden Rechtsprechung des Mitgliedsstaates oder von der Aufsichtsbehörde geregelt und entschieden.

3.1.2.4 Rechenschaftspflicht

Mit der Rechenschaftspflicht muss der Verantwortliche sicherstellen, dass er die Grundsätze der Datenverarbeitung in Bezug auf den Umgang mit personenbezogenen Daten, gemäß Art.5 DSGVO nicht nur strikt einhält, sondern muss die Einhaltung auch beweisen können. Die Grundsätze umfassen dabei die Rechtmäßigkeit, die Richtigkeit nach Treu und Glauben, die Zweckbindung, die Minimierung, die Integrität und die Vertraulichkeit der personenbezogenen Daten.[30] Ein Verstoß gegen die Grundsätze der DSGVO wird mit sehr hohen Geldbußen geahndet, weswegen der Verantwortliche sicherstellen sollte, dass die erhobenen Daten auch vor dem unbefugten Zugriff durch Dritte geschützt sind. Verantwortliche führen daher oft IT-gestützte Software mit Zugriffsberechtigungen in ihrem Unternehmen ein, um den Datenmissbrauch zu verhindern und die Rechenschaftspflicht als Ganzes professioneller zu erfüllen. Der Umfang von organisatorischen und technischen Maßnahmen muss der Verantwortliche selbst anhand einer Risikoanalyse und den Gegebenheiten bestimmen, z. B. sollten mehr Maßnahmen ergriffen werden, wenn mit sensiblen Daten gearbeitet wird und der Zugriff durch mehrere Personen erfolgt. Rechenschaft muss der Verantwortliche direkt bei der Datenaufsichtsbehörde ablegen. Bei einer Anfrage der Aufsichtsbehörde über die Datenverarbeitung des Unternehmens, muss der Verantwortliche in der Lage sein zu beweisen, dass er die Datenverarbeitung regelkonform durchführt und die Grundsätze einhält. In welcher Art und Weise die Rechenschaft erfolgt, ist dabei nicht vorgeschrieben und kann vom Verantwortlichen selbst festgelegt werden. Die Datenaufsichtsbehörde muss davon überzeugt werden, dass im Unternehmen der Umgang mit personenbezogenen Daten sensibilisiert behandelt wird, wodurch individuell angepasste IT-Programme durch ihr professionelles Auftreten einen Vorteil haben.

3.1.2.5 Meldepflicht

[30] (Cat o. D.)

Bei einem Data Breach hat der Verantwortliche gegenüber der Datenaufsichtsbehörde gemäß Art. 33 DSGVO eine Meldepflicht innerhalb von 72 Stunden zu tätigen, mit Ausnahme, wenn es bei der Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen kommt.[31] Sollte der Verantwortliche der Frist von 72 Stunden nicht nachkommen, muss er diese Verzögerung glaubhaft begründen und auch wenn er der Meinung ist, dass die Verletzung zu keinem Risiko für die natürliche Person führt, muss er es nachweisbar begründen können. Eine Datenpanne kann dabei durch vorsätzliches/bewusstes oder auch durch fahrlässiges Handeln, beispielsweise durch den Verlust eines Speichermediums, passieren. Bei einer Data Breach Meldung, soll genauestens beschrieben werden, um welche Art der Verletzung es sich handelt und wie viele Personen (vermutlich) betroffen sind. Es müssen die Kontaktdaten des Verantwortlichen und gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten gemeldet werden und zusätzlich eine Risikobewertung, welche Folgen entstehen können und wie diese Verletzung behoben werden kann bzw. die Auswirkungen des Schadens verringert werden können.[32] Eine Meldung an die betroffene(n) Person(en) von dem Vorfall ist nur bei einer groben Verletzung der Rechte und Freiheiten der Person(en) erforderlich, z. B. bei einem Data Breach von sensiblen Daten.

3.1.2.6 Dokumentationspflicht

Der Verantwortliche ist verpflichtet gemäß Art. 30 DSGVO, ein Verzeichnis aller Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, zu führen. Dokumentiert werden müssen dabei die Kontaktdaten des Verantwortlichen, eines eventuellen Vertreters und eines eventuellen Datenschutzbeauftragten, für welchen Zweck diese Daten verarbeitet werden, Beschreibung der Kategorien betroffener Personen, der personenbezogener Daten und der Empfänger, festgelegte Fristen für die Löschung der Daten und Verwendung von organisatorischen und technischen Maßnahmen (siehe Abbildung 3). Die Dokumentationspflicht entfällt für Unternehmen mit weniger als 250 Mitarbeitern, wenn die Datenverarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt, die Verarbeitung nur gelegentlich erfolgt oder die Verarbeitung keine sensiblen Daten bzw. keine Daten über strafrechtliche Verurteilungen

[31] (Datenschutzgrundverordnung 2016)
[32] (Dsb 2021)

beinhaltet.[33] Sollte die Aufsichtsbehörde eine Anfrage auf diese Verzeichnisse tätigen, so muss der Verantwortliche mit der Aufsichtsbehörde zusammenarbeiten und diese Verzeichnisse vorlegen. Mit diesem Vorgehen ist sichergestellt, dass die Verarbeitungsvorgänge von den verschiedenen Unternehmen jederzeit kontrolliert werden können.

3.1.2.7 Recht auf Auftragsverarbeitungsverträge

Der Verantwortliche hat das Recht Verträge zu verfassen, um seine Tätigkeiten oder Pflichten auf einen Auftragsverarbeiter zu verlagern, unter den Bedingungen von Art.28 DSGVO. Der Inhalt des Vertrages muss unmissverständlich strukturiert sein, welchen Bereich der Verarbeitung von personenbezogenen Daten der Auftragsverarbeiter übernimmt, um im Falle eines Verstoßes sich darauf berufen zu können. Eine Person darf ohne einen Auftragsverarbeitungsvertrag, keine Daten im Auftrag des Verantwortlichen verarbeiten. Die ausgewählten Auftragsverarbeiter müssen Garantien erbringen, dass geeignete technische und organisatorische Maßnahmen vorhanden sind, um im Einklang mit den DSGVO-Bestimmungen Daten verarbeiten zu können. Sollte es zu einem Data Breach kommen, weil der Auftragsverarbeiter gegen die Bestimmungen des Vertrages gehandelt hat, haftet der Auftragsverarbeiter und muss mit Sanktionen rechnen.

3.1.2.8 Schweigepflicht

Der Verantwortliche darf die Informationen der personenbezogenen Daten nur an jene Dritte weiterleiten, welche ausschließlich mit der betroffenen Person vereinbart wurden. Allen anderen Personen gegenüber hat er eine Schweigepflicht zu erfüllen und muss das Einverständnis der betroffenen Person einholen, bevor er diese Informationen weiterleiten darf. Die Schweigepflicht findet häufig im medizinischen Bereich Anwendung, wenn es um Patientendaten geht.

3.1.3 Auftragsverarbeiter

Ein Auftragsverarbeiter ist eine natürliche oder juristische Person/Organisation/Verein und arbeitet im Auftrag und Interesse des Verantwortlichen. Dabei verarbeitet er nur Daten, die

[33] (Wko 2021d)

ihm vom Verantwortlichen zugeteilt wurden und muss auch geeignete technische und organisatorische Maßnahmen vorweisen können, um die Daten regelkonform mit der DSGVO verarbeiten und für deren Sicherheit garantieren zu können. Der Auftragsverarbeiter haftet gleich wie der Verantwortliche und hat demnach auch die gleichen Pflichten zu erfüllen, allerdings fällt der Umfang der Dokumentationspflicht deutlich geringer aus. Er unterliegt einer Warnpflicht, wenn Anweisungen vom Verantwortlichen gegen die DSGVO verstoßen und darf diese nicht annehmen.[34] Wenn dem Auftragsverarbeiter eine Verletzung des Schutzes personenbezogener Daten bekannt wird, meldet er diese dem Verantwortlichen unverzüglich, um weitere Schritte einleiten zu können.

3.1.4 Datenschutzkoordinator

Ein Datenschutzkoordinator ist nicht Inhalt der DSGVO und daher auch nicht verpflichtend. Gerade bei größeren Unternehmen ist es aber vom Vorteil, wenn Datenschutzkoordinatoren eingestellt werden, um eine bessere Kontrolle über den Datenschutz zu erlangen und die Aufgaben auf mehrere Leute verteilen zu können. Die Datenschutzkoordinatoren unterstützen sowohl den Verantwortlichen als auch den Datenschutzbeauftragten, bei der Erfüllung der DSGVO-Regeln. Sie besitzen Fachwissen im Bereich des Datenschutzes und kennen die Prozesse und Abläufe innerhalb der Organisation und werden daher als Schnittstelle zwischen der Organisation und dem Datenschutzbeauftragten angesehen.[35] Bei einem Verstoß bekommt er als erstes alle relevanten Informationen zu dem Vorfall und leitet diese an die entsprechenden Abteilungen weiter, wie der IT-Abteilung, Geschäftsführung und dem Datenschutzbeauftragten.[36] Durch einen Datenschutzkoordinator kann also wertvolle Zeit bei einem Data Breach gewonnen werden und jede Abteilung kann sofort mit der Bearbeitung beginnen. Weiters ist es möglich, einen Datenschutzmanager einzustellen, der Anweisungen an die einzelnen Datenschutzkoordinatoren vergibt und somit als deren Vorstand anzusehen ist.

[34] (Wko 2021e)
[35] (Dr. Datenschutz 2017)
[36] (Isico 2019)

3.1.5 Datenschutzbeauftragter

Ein Datenschutzbeauftragter wird gemäß Art.37 DSGVO von dem Verantwortlichen und dem Auftragsverarbeiter auf freiwilliger Basis ernannt oder ist verpflichtend, wenn die Kerntätigkeit des Unternehmens die Verarbeitung von personenbezogenen Daten beinhaltet oder wenn es sich bei dem Unternehmen um eine Behörde oder öffentliche Stelle handelt.[37] Ein Datenschutzbeauftragter kann intern eingestellt oder extern als freier Dienstnehmer berufen werden und dient als Überwachungsorgan der korrekten Einhaltung der DSGVO-Bestimmungen und als Bezugsperson bei unternehmensinternen Fragen bezüglich der DSGVO. Der Vorteil des externen Datenschutzbeauftragten ist das bereits vorhandene hohe Wissen über die Bestimmungen der Verordnung, durch die Erfahrung in anderen Organisationen. Er verfügt bereits über alle erforderlichen Kenntnisse und muss nicht erst eingearbeitet oder eingeschult werden. Er ist allerdings nicht in der internen Firmenpolitik integriert und weiß anfangs nur wenig über die verwendeten IT-Systeme und Programme. Weiters kennen die Mitarbeiter den externen Datenschutzbeauftragten nicht und werden daher weniger Fragen bei Problemen stellen. Als Aufsichtsorgan betreffen Sanktionen, bei Verstößen und Nichteinhaltung der Bestimmungen, daher ausschließlich die Organisation und nicht den Datenschutzbeauftragten. Daher ist es wichtig, dass er niemals im Interesse des Unternehmens handeln darf, sondern ausschließlich im Interesse der Datenschutzbestimmungen. Der folgende Absatz ist eine eigenständige Zusammenfassung der Rechte und Pflichten des Datenschutzbeauftragten gemäß den Bestimmungen der DSGVO und der Literatur „*Umsetzung der DSGVO in der Praxis*“.[38]

Datenschutzbeauftragte unterliegen der Weisungsfreiheit bei allen Tätigkeiten, die ihm nach der DSGVO zugewiesen wurden, bei zusätzlichen Tätigkeiten, die nicht den Datenschutz betreffen, trifft die Weisungsfreiheit nicht zu. Der Datenschutzbeauftrage darf während einer vereinbarten Frist für seine korrekte Ausführung der Arbeit nicht benachteiligt oder abberufen werden. Das Recht auf Kündigungsschutz eines internen Datenschutzbeauftragten wurde eingeführt, um die uneingeschränkte Ausübung der Tätigkeiten eines Datenschutzbeauftragten zu gewährleisten, da er im Unternehmen

[37] (Datenschutzgrundverordnung 2016)
[38] (Vgl. Feiler und Horn 2018)

einen eher unpopulären Ruf bei den Mitarbeitern und der Geschäftsleitung genießen dürfte. Abberufen werden darf der Datenschutzbeauftragte demnach nur dann, wenn er die Aufgaben gemäß DSGVO nicht ordnungsgemäß einhält oder ausübt und nicht aufgrund seiner womöglich strengen Vorgehensweise bei der Überwachung des Datenschutzes aus Sicht des Verantwortlichen. Eine weitere Pflicht ist die Berichterstattung an das obere Management oder Geschäftsleitung. Der Datenschutzbeauftrage muss demnach den Geschäftsführer einer Firma über die laufende datenschutzrechtliche Situation innerhalb der Organisation informieren. Dabei muss in festgelegten, regelmäßigen, zeitlichen Abständen (mindestens 1x pro Jahr) ein Datenschutzbericht erstellt werden, über die aktuellen Geschehnisse, Kontrolltätigkeiten, Risiken und auch über die Verstöße. Der Datenschutzbericht wird ausschließlich vom Datenschutzbeauftragten verfasst und an das oberste Management übergeben. Durch die direkte Verfassung, ausschließlich vom Datenschutzbeauftragten, wird die Integrität des Datenschutzberichts gewährleistet und ist daher manipulationssicher. Bei Verstößen überwacht der Datenschutzbeauftragte die korrekte Vorgehensweise der Meldung des Verantwortlichen an die zuständige Aufsichtsbehörde. Bei Ausübung einer zusätzlichen anderen Tätigkeit, muss darauf geachtet werden, dass es zu keinem Interessenkonflikt kommt. Ein Datenschutzbeauftragter kann z. B. nicht zusätzlich in der IT-Abteilung arbeiten, da er sich dann selbst kontrollieren müsste und das 4-Augen Prinzip nicht eingehalten werden würde. Generell ist darauf zu achten, dass der Datenschutzbeauftragte ausreichend Zeit zur Durchführung seiner Tätigkeiten erhält, um eine ordnungsgemäße und sorgfältige Arbeitsweise zu gewährleisten. Er hat also das Recht, zusätzliche zeitliche Ressourcen zu verlangen, wenn es benötigt wird. Eine seiner Hauptaufgaben besteht darin, die Mitarbeiter in der Organisation über die datenschutzrechtlichen Pflichten aufzuklären. Dabei sollten nicht nur rechtliche Informationen weitergegeben werden, sondern auch Anweisungen über die datenschutzrechtlich konforme Umsetzung innerhalb der Organisation. Der Datenschutzbeauftragte kann die Mitarbeiter der Organisation über die richtige Vorgehensweise schulen und zwecks Übersicht eine Liste der Mitarbeiter anfertigen, die an den Schulungen bereits teilgenommen haben. Als Bezugsperson rund um das Thema Datenschutz beantwortet er Fragen innerhalb der Organisation, um das Verständnis der Mitarbeiter bezüglich des Datenschutzes zu stärken und Fehler zu vermeiden. Weiters ist es seine Aufgabe, die Einhaltung der datenschutzrechtlichen Bestimmungen innerhalb der Organisation zu überprüfen und auch Verbesserungspotenziale aufzuzeigen.

Erwähnenswert ist dabei, dass er als Aufsichtsorgan lediglich darauf hinweisen muss, jedoch nicht für deren Einhaltung verantwortlich ist. Diese Verantwortung übernimmt nach wie vor weiterhin der Verantwortliche bzw. der Auftragsverarbeiter. Der Datenschutzbeauftragte unterliegt einer Verschwiegenheitspflicht gegenüber Dritten, allerdings ist die Aufsichtsbehörde dabei ausgenommen, um wichtige Informationen auch weiterleiten zu können. Die Zusammenarbeit zwischen dem Datenschutzbeauftragten und der Aufsichtsbehörde ist verpflichtend und die Aufsichtsbehörde unterstützt ihn bei den alltäglichen Aufgaben. Weiters ist der Datenschutzbeauftragte die erste Anlaufstelle für Informationen oder Fragen der Datenschutzbehörden. Als Ausweisungspflicht genügt allerdings eine E-Mail-Adresse vom Datenschutzbeauftragten, damit die Datenschutzbehörde eine direkte Kontaktperson für ihr Anliegen in Bezug zu den DSGVO-Bestimmungen hat. Ein Name ist nicht zwingend erforderlich, sofern die E-Mail-Adresse zum richtigen Datenschutzbeauftragten führt.

Die wichtigsten Funktionen eines Datenschutzbeauftragten sind also die Überwachung der Einhaltung der Bestimmungen der Datenschutzgrundverordnung innerhalb einer Organisation. Er steht in Zusammenarbeit mit der Aufsichtsbehörde und ist als Fachkundiger die erste Anlaufstelle bei Fragen oder Problemen für die Mitarbeiter oder die Geschäftsleitung des Unternehmens. Er handelt nicht im Interesse des Unternehmens und muss bei Verstößen gegen die DSGVO sicherstellen, dass diese auch wirklich der Aufsichtsbehörde gemeldet werden, auch wenn das zu folgeschweren Problemen für das Unternehmen führt. Um seine Tätigkeiten zu schützen, genießt er während seiner festgelegten befristeten Einsatzzeit einen Kündigungsschutz und kann nur in begründbaren Ausnahmesituationen abbestellt werden (z. B. bei nicht korrekter Einhaltung der Tätigkeiten laut DSGVO).

3.2 Betroffene Personen

Die betroffene Person ist jene natürliche Person, von welcher die Daten direkt oder indirekt verarbeitet werden. Sie profitiert von den Pflichten der Unternehmen, um die Verarbeitung ihrer personenbezogenen Daten nach den DSGVO-Regeln durchzuführen. Die folgenden Rechte sind Zusammenfassungen aus der Datenschutzgrundverordnung.

3.2.1 Auskunftsrecht

Eine betroffene Person kann ihr Recht auf Auskunft gemäß Art.15 DSGVO ausüben und bei dem Verantwortlichen eines Unternehmens nachfragen, ob personenbezogene Daten verarbeitet werden und falls zutreffend, die Zweckbindung, Kategorien, Empfänger und Dauer der Datenverarbeitung erfragen. Der Verantwortliche muss die entsprechenden Daten zur Einsicht schriftlich oder elektronisch zusenden. Widerrufen kann der Verantwortliche die Anfrage nur, wenn er bei einem Hoheitsakt tätig ist und durch die Auskunft seine gesetzlich übertragenden Aufgaben nicht mehr erfüllen kann oder damit ein Geschäfts-/ Betriebsgeheimnis bzw. Dritte gefährdet wären.[39]

3.2.2 Berichtigungs- und Löschungsrecht

Die betroffene Person kann jederzeit, die von ihm nicht (mehr) korrekten personenbezogenen Daten, gemäß Art.16 DSGVO, berichtigen lassen. Weiters kann er verlangen, dass, solange die Daten nicht berichtigt wurden, eine Einschränkung der Datenverarbeitung nach Art.18 DSGVO vorliegt. Danach darf der Verantwortliche jegliche Verarbeitung der Daten (außer Speicherung) nur mit Einwilligung der betroffenen Person durchführen, mit Ausnahme, wenn es sich um die Ausübung und Geltendmachung von Rechtsansprüchen oder um öffentliches Interesse handelt. Eine Löschung der Daten gemäß Art.17 DSGVO kann veranlasst werden, wenn die betroffene Person die Einwilligung widerruft und es keine anderweitige Rechtsgrundlage für die Verarbeitung gibt, wenn die Zweckmäßigkeit nicht mehr erfüllt ist oder wenn die Datenverarbeitung unrechtmäßig durchgeführt wurde. Die Daten müssen dabei zur Gänze gelöscht werden, sodass sie vergessen werden und keine Rückschlüsse auf deren Existenz zurückverfolgt werden können (inklusive der Daten, die bei Dritten gelagert sind).

3.2.3 Beschwerderecht

Bei Vermutung einer Vorschriftsverletzung der DSGVO, kann jederzeit eine Beschwerde an die zuständige Datenschutzaufsichtsbehörde formlos eingereicht werden. Nach Überprüfung des Falls und Gültigkeit der Beschwerde können Schadensersatzzahlungen vom Verantwortlichen/Auftragsverarbeiter an die betroffene Person geltend gemacht werden.

[39] (Dsb o. D.)

3.2.4 Datenübertragungsrecht

Eine betroffene Person hat das Recht, die aus dem Auskunftsrecht erhaltenen Daten an einen anderen Verantwortlichen weiterzuleiten. Dabei darf es zu keiner Behinderung oder Widerruf des ersten Verantwortlichen kommen. Weiters hat die betroffene Person auch das Recht, dass die personenbezogenen Daten direkt von einem Verantwortlichen zum anderen Verantwortlichen übermittelt werden, sofern dies technisch machbar ist.

3.2.5 Widerspruchsrecht

Die betroffene Person kann gemäß Art.21 DSGVO jederzeit aus situationsabhängigen Gründen die Verarbeitung der sie betreffenden personenbezogenen Daten widerrufen, mit Ausnahme, wenn die Datenverarbeitung zur Ausübung und Geltendmachung von Rechtsansprüchen dient. Der Antrag auf Widerspruch kann dabei in mündlicher Form per Telefon oder in schriftlicher Form per Brief oder E-Mail erfolgen. Der Verantwortliche muss dem Widerspruch binnen 1 Monat Folge leisten, sofern er keine Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder er die Identität der anfragenden Person bezweifelt. Beim Widerspruch gegen personenbezogene Daten, die zum Betreiben von Direktwerbung genutzt werden, dürfen die Daten für diesen Zweck ausnahmslos nicht mehr verwendet werden. Gegen personenbezogene Daten, die zu wissenschaftlichen, historischen oder zu statistischen Forschungszwecken genutzt werden sollen, kann ebenfalls Widerspruch eingelegt werden, allerdings kann der Verantwortliche sich auf die Ausnahmeregelung des öffentlichen Interesses berufen. Ein erfolgreicher Widerspruch führt automatisch zur Löschung der personenbezogenen Daten.

4 Sanktionsmaßnahmen

4.1 Allgemein

Bei Nichteinhaltung der Bestimmungen laut EU-DSGVO, kann die Aufsichtsbehörde Sanktionen über die Verantwortlichen oder den Auftragsverarbeiter verhängen. Die Entscheidung, ob es überhaupt zu einer Strafe kommt und die Höhe der Geldbuße bei Verhängung, entscheidet allein die Aufsichtsbehörde und hängt von vielen Faktoren ab. Gegen das rechtmäßige Urteil der Aufsichtsbehörde kann allerdings Berufung

eingefordert werden und Beschwerden können, laut dem österreichischen Datenschutzgesetz, an das Bundesverwaltungsgericht Österreich eingereicht werden und danach wird über weitere Schritte entschieden.[40]

4.2 Rechtmäßige Durchführung

Jede natürliche Person hat das Recht, eine Beschwerde an die Datenaufsichtsbehörde zu melden, wenn er/sie glaubt, dass gegen die Bestimmungen der Datenschutzgrundverordnung gehandelt wurde. Dabei spielt es keine Rolle, wenn die Person nicht weiß, gegen welche Bestimmung im Speziellen verstoßen wurde. Die Aufsichtsbehörde muss den Fall überprüfen und entscheidet durch ihr vorhandenes Fachwissen, ob es sich um einen Verstoß handelt oder nicht. Während des gesamten Entscheidungsprozesses muss die Datenaufsichtsbehörde die Person, die die Beschwerde eingereicht hat, über den Stand und die Ergebnisse der Beschwerde einschließlich der Möglichkeit eines gerichtlichen Rechtsbehelfs informieren.[41] Gegen den Beschluss der Aufsichtsbehörde kann die Person, die die Beschwerde eingereicht hat, Klage beim obersten Gerichtshof einreichen, die den Fall nochmals überprüft. Solche Fälle sind keine Seltenheit und trotz des Fachwissens der Aufsichtsbehörde kann der Gerichtshof gegen den Beschluss der Aufsichtsbehörde entscheiden, wie im Beispiel der Beschwerde gegen die irische Aufsichtsbehörde.[42] Wenn die beschwerdeeinreichende Person Recht bekommt, werden Sanktionen an die/den Verantwortlichen oder Auftragsverarbeiter verhängt und geltend gemacht, da sie für solche Vergehen haften. Das Ausmaß der Sanktion hängt von der Schwere der Datenschutzverletzung ab und bei einer Geldbuße erhält jede betroffene Person, die einen materiellen oder immaterielleren Schaden erlitten hat, einen Schadensersatz als Ausgleich. Generell sind die verhängten Geldbußen aber direkt beim Bund zu entrichten.

4.3 Strafumfang

Ob eine Sanktion mit einer Geldbuße geahndet oder nur eine Verwarnung ausgesprochen wird, entscheidet die Aufsichtsbehörde des jeweiligen Mitgliedsstaates oder der

[40] (Bundesverwaltungsgericht Rebublik Österreich o. D.)
[41] (Wko 2021c)
[42] (Gerichtshof der europäischen Union 2020)

Gerichtshof und hängt von der Schwere des Vergehens ab. Die Bestimmungen über die Sanktionen und die Höhe der Geldbuße, werden dabei in Art.83 und Art.84 DSGVO beschrieben und im folgenden Absatz zusammengefasst:[43]

Die Mitgliedstaaten legen nationale Gesetzvorschriften über Sanktionen für Verstöße gegen die Bestimmungen der DSGVO fest, die keiner Geldbuße unterliegen. Sie treffen alle, zu deren Anwendung erforderlichen, Maßnahmen und diese Sanktionen müssen wirksam, verhältnismäßig und abschreckend sein. Bei Verhängung einer Geldstrafe hängt die Höhe vorwiegend von der Art, Schwere und Umfang des Verstoßes der betreffenden Verarbeitung sowie der Zahl der, von der Verarbeitung betroffenen, Personen und das Ausmaß des von ihnen erlittenen Schadens. Fragen, unter anderem, ob der Verantwortliche oder Auftragsverarbeiter vorsätzlich oder fahrlässig gehandelt hat, ob gegen eine oder gegen mehrere Bestimmungen verstoßen wurde, ob geeignete technische und organisatorische Maßnahmen zur Einhaltung der Bestimmungen vorhanden sind, ob bereits frühere Verstöße des Verantwortlichen/Auftragsverarbeiters bekannt sind, ob ein ausreichend großer Umfang der Zusammenarbeit mit der Aufsichtsbehörde existiert oder ob der Datenschutzbeauftragte bereits auf den Verstoß hingewiesen hat etc., sind alles Anhaltspunkte, um die Höhe der Geldbuße festzulegen. Eine maximale Höhe von 10 Mio. € oder von bis zu 2% des, vom Unternehmen gesamten weltweit erzielten, Jahresumsatzes des vorangegangenen Geschäftsjahrs werden vorgeschrieben, wenn gegen die Pflichten des Verantwortlichen/Auftragsverarbeiter, gegen die Pflichten der Zertifizierungsstelle oder gegen die Pflichten der Überwachungsstelle verstoßen wurde. Eine maximale Höhe von 20 Mio. € oder von bis zu 4% des, vom Unternehmen gesamten weltweit erzielten, Jahresumsatzes des vorangegangenen Geschäftsjahrs werden vorgeschrieben, wenn allgemein gegen die Grundsätze der Verarbeitung inklusive Einwilligungsbedingungen, gegen die Rechte der betroffenen Person, Übermittlung personenbezogener Daten an Drittländer oder internationale Organisationen, gegen die Pflichten der Rechtsvorschriften der Mitgliedsstaaten oder gegen die Anweisungen der Aufsichtsbehörde, verstoßen wurde.

Die Strafhöhe wird also individuell an die Verhältnisse und Gegebenheiten angepasst und verschiedene Instanzen, wie die Bestimmungen der EU-DSGVO, die Mitgliedsstaaten, die Aufsichtsbehörde und der Gerichtshof haben schlussendlich Einfluss darauf. Hohe

[43] (Datenschutzgrundverordnung 2016)

Geldbußen sind dabei keine Seltenheit, allein nach ca. 1,5 Jahre, nach Umsetzung der DSGVO, wurden teils sehr hohe Strafzahlungen an Unternehmen verhängt. Die höchste je verhängte Geldstrafe im europäischen Raum, wurde bei der Fluggesellschaft „British Airways“ mit allein 204,6 Mio. € durchgeführt, aber auch die Österreichische Post AG wurde bereits mit 18 Mio. € verurteilt.[44] Allerdings kann man auch hier wieder Klage gegen das Urteil erheben und die Verhängung der Geldbuße kann selbst aus banalen Gründen, wie z.B. Formfehler, annulliert werden. Als praktisches Beispiel dient die österreichischen Post AG, bei der die Strafe an juristische Personen anstelle von natürlichen Personen gerichtet war, obwohl das Unternehmen eindeutig gegen die DSGVO verstoßen hat, da es die Parteiaffinität von Kunden an wahlwerbende Parteien verkauft hatte.[45]

5 Sensible Daten im medizinischen Bereich

5.1 Unterschied personenbezogene Daten und sensible Daten

Die personenbezogenen Daten beinhalten alle Informationen, die zur eindeutigen Identifikation einer Person führen, wie z. B. der Name, Adresse, Telefonnummer usw. Personenbezogene Daten, die zu keiner eindeutigen Identifikation einer Person führen, aber Auskunft über das Verhalten von Personen liefern, werden unter dem Begriff “pseudonymisierte Daten“ zusammengefasst. Sensible Daten sind laut DSGVO dagegen besondere Kategorien personenbezogener Daten, aus denen man die Merkmale, Eigenschaften, Überzeugungen und Meinungen einer Person direkt zuordnen kann. Darunter zählen Informationen wie die rassische und ethnische Herkunft, politische Meinungen, Religion und Weltanschauung, Mitgliedschaft in Gewerkschaften, genetische Daten, biometrische Daten, um eine natürliche Personen eindeutig zu identifizieren, Gesundheitsdaten oder Daten zum Sexualleben bzw. zur sexuellen Orientierung einer natürlichen Person.[46] Der entscheidende Unterschied zu normalen personenbezogenen Daten ist, dass sensible Daten gemäß Art.9 DSGVO generell nicht verarbeitet werden dürfen, außer in speziellen Sonderfällen wenn die Verarbeitung z.B. im Interesse der betroffenen Person liegt, wie im medizinischen Bereich, um der betroffenen Person helfen oder ihr Leben retten zu können.

[44] (Brandt 2019)
[45] (Future Zone 2020)
[46] (Marcerou 2017)

5.2 Gesundheitsdaten

Mit dem Begriff Gesundheitsdaten werden alle Daten vereint, welche sich auf die körperliche oder geistige Gesundheit einer Person beziehen. Im medizinischen Bereich sind daher alle Gesundheitsdaten als sensible Daten zu behandeln, welche laut den Bestimmungen der DSGVO nur im Interesse der betroffenen Person verarbeitet werden dürfen. Die Patientendaten werden im medizinischen Bereich auch als sensibel erachtet, da neben den normalen personenbezogenen Daten, wie der Name und Anschrift des Patienten auch Gesundheitsdaten hinterlegt sind, die Auskunft über den aktuellen Gesundheitszustand und etwaige Allergien etc. geben. Ein Streitthema bildet da die Sozialversicherungsnummer, wenn sie allein und nicht im Zusammenhang mit den kompletten Patientendaten verarbeitet wird. Die Sozialversicherungsnummer allein sagt nichts über den Gesundheitszustand der Person aus und ist daher per Definition gleichzusetzen wie Name oder Adresse der betreffenden Person und als normale personenbezogene Daten einzuordnen. Allerdings umfassen Gesundheitsdaten auch Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um deren Gesundheitszustand mit entsprechender Software klar definieren zu können.[47] Demnach werden Sozialversicherungsnummern als sensible Daten eingeordnet und dürfen nur mit dem ausdrücklichen Einverständnis der betroffenen Person verarbeitet werden.

5.3 Verarbeitung von Gesundheitsdaten

Nur unter bestimmten Voraussetzungen ist es rechtlich gestattet, Gesundheitsdaten zu verarbeiten oder zu verwenden und dies unterliegt hohen Auflagen, da gerade im medizinischen Bereich sehr viele sensible Daten durch die hohe Anzahl der Patienten und deren Daten über Erkrankungen entstehen. Gesundheitsdaten dürfen nur dann erhoben und verarbeitet werden, wenn der Patient mit einer Einwilligung zustimmt oder eine Zweckbindung verfolgt wird, um ein Ziel zu erreichen. Im medizinischen Bereich wird daher oft auf die Ausnahmeregelung mit der Rechtmäßigkeit der Verarbeitung zurückgegriffen, die die Datenverarbeitung gemäß Art.9 Abs.2 DSGVO erlaubt, wenn sie

[47] (Wko 2021a)

erforderlich ist, um das lebenswichtige Interesse der betroffenen Person oder einer anderen natürlichen Person zu schützen.[48] Das bedeutet, wenn eine Person ohnmächtig ist, darf der Arzt sie trotzdem behandeln und eine Diagnose erstellen bzw. die Behandlung durchführen, obwohl er keine Einwilligung von dem Patienten erhalten hat, weil er in der momentanen Situation nicht in der Lage ist, eine Einwilligungserklärung zu unterzeichnen. Ein weiterer Punkt schützt die rechtmäßige Verarbeitung von Gesundheitsdaten in Art.9 Abs.2 DSGVO, bei der die Verarbeitung zum Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich, legitim ist. Bei einem Verstoß kann es mitunter nicht nur zu einer Geldstrafe kommen, sondern es kann auch eine Freiheitsstrafe verhängt werden, was eine Existenzbedrohung der betroffenen Organisation bedeutet. Aus diesem Grund sollte man sich neben den Grundlagen der DSGVO, auch entsprechende organisatorische und technische Möglichkeiten überlegen, um ein Data Breach zu vermeiden. Bei der Speicherung der Daten muss z.B. eine sehr hohe Sicherheit gegeben sein, sodass der Zugang auf die Gesundheitsdaten für Unbefugte und Dritte verwehrt ist und damit Missbrauch abgewehrt werden kann. Sollte es zu einem Data Breach kommen, muss der Verantwortliche neben der Meldung an die Datenschutzbehörde, auch die betroffene Person über alle bekannten Fakten informieren und eine Risikoabschätzung durchführen, welche Folgen sich daraus ergeben können und wie die Verletzung behoben werden kann bzw. die Auswirkungen des Schadens verringert werden kann.

5.4 Informationssysteme

Als technische Hilfestellung zum Verarbeiten von personenbezogenen und sensiblen Daten bieten sich IT-gestützte Informationssysteme an, da bei einer handschriftlichen Administration eine höhere Gefahr von Manipulation der Daten ausgeht. Gut eingepflegte Informationssysteme unterstützen dabei die Sicherheit der Daten und erhalten die Grundsätze der DSGVO wie Zweckbindung, Datenminimierung und Integrität (DSGVO-Compliance).[49] Ein Archiv über alle Daten der Patienten kann angelegt werden und die

[48] (Jahnel 2019, 251)
[49] (Hanke 2018)

Zugriffsteuerung erfolgt dementsprechend durch ein Berechtigungssystem. Der entscheidende Vorteil liegt dabei auf der Nachvollziehbarkeit des Zugriffs durch ein Log. Man erkennt sämtliche Einsichtnahmen mit Datum und Uhrzeit und es wird vor allem protokolliert, wann und wer etwas an den Daten verändert hat. Die Integrität der Daten ist somit geschützt und die Organisation ist zusätzlich in der Lage auskunftsfähig zu sein, um auf Anfragen der betroffenen Person oder Dritten schnell reagieren zu können. Auf Wunsch der betroffenen Person können die Daten so auch leicht und unkompliziert verändert oder gelöscht werden, um auch eine gewisse Professionalität zu vermitteln. Um die Zweckbindung zu erhöhen, ist es sehr wichtig, das Informationssystem mit einem regelkonformen Zugriffskontrollmechanismus zu verknüpfen, wo die Rollen den entsprechenden Personen zugeordnet und definiert werden können. Dabei muss vorab geklärt werden, welche Prozesse in der Organisation vorhanden sind und es muss demnach entschieden werden, wie viele Rollen es geben soll, welche Rolle welche Zugriffe haben oder nicht haben darf und wie lang der Zugriff erlaubt ist (automatischer Log-Out nach Zeit, zusätzlich zum manuellen). Die Zugriffsrechteverteilung entscheidet dabei der Verantwortliche und er muss sicherstellen, dass ein wesentlich kleinerer Personenkreis auf die Daten Zugriff hat, als es bei den normalen personenbezogenen Daten der Fall wäre. Das fertige Informationssystem wird demnach vom Fachpersonal individuell an die Organisation angepasst und zur Verfügung gestellt.

5.5 Haftung

Der niedergelassene Arzt oder die Ärztin verarbeiten die personenbezogenen Daten und sind demnach laut DSGVO die Verantwortlichen. Wenn mehrere Ärzte eine Ordination führen, sind sie in der Regel gemeinsam verantwortlich und haften auch gemeinsam.[50] Bei großen Einrichtungen mit mehreren Ärzten, wie in einem Krankenhaus haftet die Einrichtung als Ganzes. Krankenhäuser sind daher auch verpflichtet, einen Datenschutzbeauftragten zu bestellen, um die große Datensammlung regelkonform verarbeiten zu können.

5.6 Weitergabe an Dritte

[50] (Ärztekammer Wien o. D.)

Im medizinischen Bereich ist die Weitergabe der Daten an externe Stellen alltäglich, wie z. B. für Verrechnungen mit Krankenkassen, Anfragen von exekutiven Institutionen wie Polizei, Gericht oder Staatsanwaltschaften, Informationsaustausch mit anderen Krankenhäusern oder Ärzten, um die Behandlung durchführen zu können oder auch mit der Datenaufsichtsbehörde. Weiters möchten auch die Angehörigen des Patienten über den Gesundheitszustand des Patienten Bescheid wissen. All diese Situationen müssen genau überprüft werden, ob eine Weitergabe der Daten in Ordnung ist, wie die Übermittlung geschieht und in welchem Umfang sie stattfindet.

5.6.1 Externe Stellen

Ärzte als Verantwortliche müssen gewährleisten, dass sie die vertraulichen Informationen an die zulässigen Empfänger, nur mit Hilfe von verschlüsselten elektronischen Mitteln versenden. Als Anwendungsbeispiele bieten sich einerseits das herkömmliche Fax an, welches laut Definition eine verschlüsselte sichere Übertragung ist oder mit Hilfe von speziell angefertigte Arztsoftware, wie z. B. „Elda“. Elda ist eine Software, die für die österreichischen Sozialversicherungsträger entwickelt wurde, um sicher den elektronischen Datenaustausch von sensiblen Daten zu gewährleisten, da die Daten verschlüsselt übertragen werden. Wenn z.B. ein Rettungseinsatz mit den zuständigen Sozialversicherungsträgern verrechnet werden soll, wird zuerst eine Verbindung direkt zwischen den beiden Teilnehmern per SSL-Verschlüsselung aufgebaut.[51] Dieser Kanal bildet nun einen sicheren Übertragungsweg und die sensiblen Daten können versendet werden. Die Elda Software ist mit den Vorgaben der DSGVO konform und kann ohne Bedenken für die Datenübertragung verwendet werden.[52] Die Softwarehersteller, die Zugriff auf personenbezogenen Daten haben, sind gemäß Definition der DSGVO ein Auftragsverarbeiter und haften dementsprechend bei Verstößen.

5.6.2 Angehörige

Die Weitergabe von Patienteninformation an Angehörige ist ein heikles Thema. Grundsätzlich ist laut der DSGVO eine Weitergabe der Patientendaten ohne Einwilligung

[51] (Elda 2021a)
[52] (Elda 2021b)

des entsprechenden Patienten rechtswidrig. Es dürfen keinerlei Informationen über den Gesundheitszustand sowie über den Verlauf der Behandlung oder andere Informationen, den Angehörigen mitgeteilt werden, wenn der Patient dem nicht zustimmt und volljährig ist. Ärzte und Ärztinnen unterliegen daher einer besonderen Schweigepflicht. Zuwiderhandlungen werden streng sanktioniert und der Verantwortliche wird zur Rechenschaft gezogen. Um Auskunft erteilen zu dürfen, benötigt das jeweilige Institut (Arztpraxis, Krankenhaus usw.) eine Einwilligungserklärung des Patienten, wo ausdrücklich hervorgeht, dass die medizinischen Daten des Patienten an Angehörige, Freunde oder Ähnlichem weitergegeben werden dürfen.[53] Um für einen Streitfall vorzusorgen, sollte demnach eine Einwilligungserklärung bereits im Vorhinein abgegeben werden, damit die Angehörigen, im Falle eines schweren Unfalls und Bewusstlosigkeit des Patienten, problemlos Auskunft bekommen können.

5.7 Aufbewahrungspflicht

Gemäß § 51 Abs.3 Ärztegesetz sind die Aufzeichnungen sowie die sonstigen Dokumentationen im Sinne des Abs.1 als dienliche Unterlagen mindestens 10 Jahre lang aufzubewahren, wobei Haftungsansprüche 30 Jahre lang gelten.[54] Dem Recht auf Löschung von den sensiblen Daten gemäß DSGVO kann aus diesem Grund nicht entsprochen werden und die betroffene Person kann auch keine Rechtsansprüche geltend machen.[55] Ein neuer Verantwortlicher übernimmt die vorhandene Datenbank und setzt die betroffenen Patienten davon in Kenntnis.

5.8 Corona-Pandemie

Bei bestimmten (ansteckbaren) Krankheiten, wie z.B. bei Masern oder dem Covid 19 Virus ist der Arzt verpflichtet, das Gesundheitsamt zu informieren.[56] Ein Verstoß gegen die DSGVO liegt dabei allerdings nicht vor, weil auf das öffentliche Interesse und den Schutz der nationalen Sicherheit verwiesen werden kann. Eine Verarbeitung der Daten darf allerdings nur für den Zweck, für den sie erhoben wurden (Eindämmung des Virus)

[53] (Engelbrecht 2019)
[54] (ÄrzteG 1998 2019)
[55] (Ärztekammer Steiermark o. D.)
[56] (Keyed 2020)

geschehen. Nach Ende der Pandemie sind daher die Daten wieder zu löschen.[57] Umstritten ist dabei das aktuelle Thema über den „Grünen Pass“ zur Bekämpfung der Pandemie. Der „Grüne Pass“ sollte eingeführt werden, um alle Informationen über den Corona-Status, ob man geimpft, genesen oder getestet wurde, niederzuschreiben. Der Dachverband der Sozialversicherungsträger Österreichs lehnt den „Grünen Pass“ ab, durch eine Übermittlung der Daten aus dem Verantwortungs- und Kontrollbereich der Sozialversicherung können die Sozialversicherungsträger und der Dachverband die Sicherheit dieser Daten nicht mehr garantieren.[58]

6 Wissenswertes

Durch die Entwicklung des Datenschutzes und der Einführung der DSGVO wird das Ausmaß von Datenschutzverstößen erst bewusst. Es passieren täglich neue Vergehen, die entsprechend sanktioniert und mit teils hohen Geldbußen geahndet werden.[59] Das höchste je verhängte Bußgeld ging an Facebook mit 5 Mrd. USD. Die Anzahl von Werbe-Tracker ist dagegen rückläufig.[60] Allerdings benutzen die werbetreibenden Firmen für E-Commerce auch Maßnahmen zur Cookie-Speicherung, die eine intransparente Aufklärung über die Datenverarbeitung erlauben (siehe Abbildung 4). Die Bemühungen der DSGVO motivieren auch Drittstaaten dazu, den Datenschutz in ihrem Land zu überdenken und zu verbessern, was positiv für den internationalen Datenschutz ist. Denn gerade amerikanische Firmen wie Amazon, Google oder Facebook sind nur durch Ignorierung von Datenschutz und Ausnutzung von Tracking-Methoden so groß geworden, da die USA mit ihrer Politik das Geschäftsmodell der wirtschaftstreibenden Unternehmen nicht zerstören möchte.[61] Ein Kritikpunkt geht auf das mangelnde Wissen der Europäerinnen über die Bestimmungen und Rechte der DSGVO zurück, da viele die Datenschutzerklärungen nicht vollständig durchlesen, da sie entweder zu lang oder zu schwierig zu verstehen sind. Laut EU-Justizkommissarin Věra Jourová: „Von den 60 Prozent der Europäerinnen und Europäern, die überhaupt Datenschutzerklärungen lesen, lesen jedoch lediglich 13 Prozent diese Erklärungen vollständig durch.“[62] Laut einer Eurobarometer-Umfrage kennen nur 57% von 27.000 Europäerinnen und Europäern das

[57] (Datenschutzbehörde Österreich 2020)
[58] (Salzburg24 2021)
[59] (DSGVO-Portal 2021)
[60] (T3n 2018)
[61] (ORF 2021)
[62] (Jourová 2019)

Recht auf Löschung ihrer eigenen Daten und auch die gleiche geringe Anzahl kennt die nationale Aufsichtsbehörde.[63]

7 Fazit

Die EU-DSGVO ist ein erster Schritt in die richtige Richtung, um die Persönlichkeitsrechte der Bürger zu schützen, aber noch lange nicht der letzte. Seit der DSGVO setzen sich die Unternehmen bewusster mit dem Thema des Datenschutzes auseinander und versuchen, die geforderten Maßnahmen in ihrer Organisation zu implementieren. Auch bei dem Umgang mit sensiblen Daten in Arztpraxen oder Krankenhäuser wurden entsprechende technische und organisatorische Maßnahmen gesetzt, um die Bestimmungen der DSGVO einhalten zu können. Das liegt vor allem an den hohen abschreckenden Geldbußen, die die DSGVO bei Verstößen vorsieht und bei einigen Firmen zur Insolvenz führen können. Ein gutes Beispiel für den wirksamen Einsatz der DSGVO zeigte sich bei der gewollten Einführung des „Grünen Pass“ in der Corona-Pandemie. Die Regierung wollte demnach eine Liste der Bürger mit aktuellem Corona-Status erstellen, jedoch wurde die Implementierung aus Angst vor einem Verstoß und deren Sanktionsmaßnahmen gestoppt. Europa ist mit der DSGVO zu einem Vorbild in Sachen Datenschutz geworden und inspiriert andere Länder zur Teilnahme, um ein globales Netzwerk an Datenschutz aufzubauen. Ein Schwachpunkt der DSGVO liegt in den vielen Öffnungsklauseln, in denen entweder die jeweiligen Mitgliedsstaaten nationale Gesetze ergänzen können oder auch verstoßende Unternehmen sich darauf berufen können, um einer Strafe zu entgehen (Beispielsweise ein Formfehler der österreichischen Post AG). Außerdem ist der Bereich des E-Commerce wenig betroffen, da mit einer vorhandenen Einverständniserklärung, die Datenverarbeitung und Tracking vollkommen legitim sind. Die werbetreibenden Unternehmen nutzen diesen Umstand, um sich das Einverständnis durch eine intransparente Gestaltung der Erklärung zu holen. Selbst wenn die Werbezwecke klar aufgezeigt werden, muss man diese bei einigen Webseiten sogar akzeptieren, um die Webseite nutzen zu können.

Viele Unternehmen nutzen auch einfach das geringe Wissen der Personen über die Rechte der DSGVO aus: „Wo kein Kläger, da kein Richter.“

[63] (Europäische Kommisision 2019)

Literaturverzeichnis

Amtsblatt Nr. L 281. „Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr.“ https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:de:html, 1995.

Arge Daten. „Entwicklung des österreichischen Datenschutzrechts: Informationen zur Entstehung der österreichischen Datenschutzgesetze (DSG, DSG 2000 und DSG neu) und aktuellen gesetzlichen Entwicklungen im Datenschutz.“ http://www.argedaten.at/php/cms_monitor.php?q=PUB&s=13498rlh, 2019.

ÄrzteG 1998. „§ 51 ÄrzteG 1998.“ https://www.jusline.at/gesetz/aerzteg/paragraf/51, 2019.

Ärztekammer Steiermark. „Datenschutzgrundverordnung (DSGVO) und Datenschutz-Anpassungsgesetz.“ https://www.aekstmk.or.at/601, o. D.

Ärztekammer Wien. „Datenschutzgrundverordnung FAQ.“ https://www.aekwien.at/datenschutzgrundverordnung, o. D.

Brandt, Mathias. „Statistik der Woche: Wer für DSGVO-Verstöße zahlte .“ https://www.heise.de/hintergrund/Statistik-der-Woche-4601473.html, 2019.

Bundesgesetzblatt für die Republik Österreich. „Datenschutzgesetz - DSG.“ https://www.ris.bka.gv.at/Dokumente/BgblPdf/1978_565_0/1978_565_0.pdf, 1978.

Bundesministerium. „OECD-Leitsätze für multinationale Unternehmen - österreichischer Nationaler Kontaktpunkt.“ https://www.bmdw.gv.at/Themen/International/OECD-Leitsaetze-multinationale-Unternehmen-OeNKP.html, o. D.

Bundesverwaltungsgericht Rebublik Österreich. „Datenschutz.“ https://www.bvwg.gv.at/fachbereiche/datenschutz_neu_start.html, o. D.

Bundeszentrale für politische Bildung. „40 Jahre Europäische Datenschutzkonvention.“ https://www.bpb.de/politik/hintergrund-aktuell/326057/40-jahre-europaeische-datenschutzkonvention, 2021.

Cat, Sebastian le. „Top Ten der DSGVO, #2: Der Grundsatz der Rechenschaftspflicht.“ https://www2.deloitte.com/ch/de/pages/risk/articles/gdpr-accountability-principle.html, o. D.

Dataprotect. „Wie kann die Informationspflicht gem. Art 13 DSGVO erfüllt werden?“ https://www.dataprotect.at/2018/05/04/wie-kann-die-informationspflicht-gem-art-13-dsgvo-erf%C3%BCllt-werden/, 2018.

Datenschutz Hessen. „Geschichte des Datenschutzes .“ https://datenschutz.hessen.de/ueber-uns/geschichte-des-datenschutzes, o. D.

Datenschutz Praxis. „DSGVO: Wie Sie Ihre Informationspflichten erfüllen .“ https://www.datenschutz-praxis.de/betroffenenrechte/dsgvo-wie-sie-ihre-informationspflichten-erfuellen/#:~:text=Der%20Verantwortliche%20muss%20der%20betroffenen,klaren%20und%20einfachen%20Sprache%20%C3%BCbermitteln.&text=Zudem%20muss%20ein%20Verantwortlic, 2019.

Datenschutz.org. „EU-Datenschutzrichtlinie (Richtlinie 95/46/EG) – Alte Rechtsgrundlage.“ https://www.datenschutz.org/eu-datenschutzrichtlinie/, 2021.

Datenschutzbehörde Österreich. „Information der Datenschutzbehörde zum Coronavirus (Covid-19).“ https://www.dsb.gv.at/download-links/informationen-zum-coronavirus-covid-19-.html, 2020.

Datenschutzgrundverordnung. „VERORDNUNG (EU) 2016/...DES EUROPÄISCHEN PARLAMENTS UND DES RATES.“ https://www.datenschutz-grundverordnung.eu/wp-content/uploads/2016/04/CONSIL_ST_5419_2016_INIT_DE_TXT.pdf, 2016.

Debitoor. „Datenschutzgrundverordnung (DSGVO) – Warum wird die DSGVO eingeführt?“ https://debitoor.de/lexikon/dsgvo, o. D.

Dr. Datenschutz. „Der Datenschutzkoordinator – Stellung, Aufgaben, Vor- und Nachteile.“ https://www.dr-datenschutz.de/der-datenschutzkoordinator-stellung-aufgaben-vor-und-nachteile/#:~:text=Datenschutzkoordinatoren%20werden%20gew%C3%B6hnlich%20im%20Datenschutz,bei%20seinen%20Aufgaben%20zu%20unterst%C3%BCtzen, 2017.

Dsb. „Dokumente: Formulare, Muster, Berichte, Stellungnahmen auf einen Blick.“ https://www.dsb.gv.at/dam/jcr:81630a55-648b-4689-b849-ce0732f6a1af/Meldung%20von%20Verletzungen%20des%20Schutzes%20personenbezogener%20Daten%20gem%C3%A4%C3%9F%20Art.%2033%20DSGVO%20Notification%20of%20a%20personal%20data%20breach%20(Art.%2033%20GDPR)%20.p, 2021.

Dsb. „Ihre Rechte als Betroffener.“ https://www.dsb.gv.at/aufgaben-taetigkeiten/rechte-der-betroffenen.html#:~:text=Sonstige%20Rechte-,Gem%C3%A4%C3%9F%20Art.,gegen%20die%20Datenschutz%2DGrundverordnung%20verst%C3%B6%C3%9Ft, o. D.

DSGVO-Portal. „Geldbußen für DSGVO-Verstöße.“ https://www.dsgvo-portal.de/dsgvo-bussgeld-gegen-facebook-inc.-2019-07-24-US-325.php, 2021.

Elda. „ELDA-Online: Voraussetzungen.“ https://www.elda.at/cdscontent/?contentid=10007.838844&portal=eldaportal, 2021a.

Elda. „Information DSGVO.“ https://www.elda.at/cdscontent/?contentid=10007.860485&portal=eldaportal, 2021b.

Engelbrecht, Martin. „Was sich mit der DSGVO geändert hat?“ https://www.noen.at/thema/rechtstipps/auskunftsrecht-was-sich-mit-der-dsgvo-geaendert-hat-175717703#:~:text=F%C3%BCr%20die%20Auskunft%20ist%20derzeit,die%20Einwilligung%20vorher%20erteilt%20werden, 2019.

Ennöckl, Daniel. „Wenn Richter Unionsrecht aufheben: EU-Rechtsstaat kommt einen Schritt voran.“ https://www.diepresse.com/610325/wenn-richter-unionsrecht-aufheben-eu-rechtsstaat-kommt-einen-schritt-voran, 2010.

Europäische Kommisision. „Nur jeder zehnte Deutsche liest Datenschutzerklärungen vollständig durch .“ https://ec.europa.eu/germany/news/20190613-datenschutz_de, 2019.

Europäisches Parlament. „Das Europäische Parlament: Befugnisse.“ https://www.europarl.europa.eu/factsheets/de/sheet/19/das-europaische-parlament-befugnisse, 2021.

Europarat. „Unterschriften und Ratifikationsstand des Vertrags 108.“ https://www.coe.int/de/web/conventions/full-list/-/conventions/treaty/108/signatures, 2021.

Feiler, Lukas, und Bernhard Horn. *Umsetzung der DSGVO in der Praxis.* Wien: Verlag Österreich, 2018.

Future Zone. „Datenskandal: Post muss doch keine 18 Millionen Euro Strafe zahlen.“ https://futurezone.at/netzpolitik/datenskandal-post-muss-doch-keine-18-millionen-euro-strafe-zahlen/401116806, 2020.

Gerichtshof der europäischen Union. „Der Gerichtshof erklärt den Beschluss 2016/1250 über die Angemessenheit des vom EU-US-Datenschutzschild gebotenen Schutzesfür ungültig.“

https://curia.europa.eu/jcms/upload/docs/application/pdf/2020-07/cp200091de.pdf, 2020.

Hanke, Sandra. „Einhaltung der EU-DSGVO mit ECM-System erleichtern.“ https://www.nexus-marabu.de/nachricht/einhaltung-der-eu-dsgvo-mit-ecm-system-erleichtern.html, 2018.

Ionos. „Datenschutz-Grundverordnung (DSGVO) Zusammenfassung und Checkliste.“ https://www.ionos.at/digitalguide/websites/online-recht/datenschutz-grundverordnung-regeln-fuer-unternehmen/, 2021.

Isico. „Meldung eines Datenschutzvorfalls – ein Leitfaden.“ https://www.isico-datenschutz.de/blog/meldung-datenschutzvorfall/, 2019.

Jahnel, Dietmar. „Auswirkungen der DSGVO im medizinischen Bereich.“ *Recht der Medizin*, Oktober 2019: 251.

Jourová, Věra. „Nur jeder zehnte Deutsche liest Datenschutzerklärungen vollständig durch .“ https://ec.europa.eu/germany/news/20190613-datenschutz_de, 2019.

Keyed. „Datenschutz im Krankenhaus.“ https://keyed.de/blog/datenschutz-im-krankenhaus/, 2020.

Lindeverlag. „Enstehung des Datenschutzes.“ https://www.lindeverlag.at/buch/handbuch-datenschutzrecht-17885/b/leseprobe/B100372.pdf, o. D.

Marcerou, Guillaume. „EU-Datenschutz-Grundverordnung: Sensible und nicht sensible Daten – der entscheidende Unterschied.“ https://www.criteo.com/de/blog/eu-datenschutz-grundverordnung-sensible-und-nicht-sensible-daten-der-entscheidende-unterschied/, 2017.

Oesterreich.gv.at. „Natürliche Person.“ https://www.oesterreich.gv.at/lexicon/N/215114.html, 2021.

ORF. „Europas Datenschutz als Vorbild.“ https://oe1.orf.at/artikel/684487/Europas-Datenschutz-als-Vorbild?fbclid=IwAR3LBT9-RFmr4G5IlEoyrS9UgcPl9a3SNrm96AUHF3Z2sn1hGNs6T398ybs, 2021.

Preslmayr Rechtsanwälte. „Datenschutz für juristische Personen.“ https://lindemedia.at/news/digital-monitor/datenschutz-fuer-juristische-personen, 2019.

PVE. „Pflichten des Verantwortlichen im Sinne der DSGVO .“ https://www.pve.gv.at/der-weg-zur-gruendung/rechtliche-aspekte/datenschutz-im-zusammenhang-mit-einer-primarversorgungseinheit/pflichten-des-verantwortlichen-im-sinne-der-dsgvo/, o. D.

Rechtsinformationssystem des Bundes. „Justiz (OGH, OLG, LG, BG, OPMS, AUSL): Rechtssatznummer RS0118436.“ https://www.ris.bka.gv.at/JustizEntscheidung.wxe?Abfrage=Justiz&Dokumentnummer=JJT_20080708_OGH0002_0040OB00054_08G0000_000&IncludeSelf=True, 2008.

Salzburg24. „Datensammlung durch "Grünen Pass" wird abgelehnt .“ https://www.salzburg24.at/news/oesterreich/gruener-pass-kritik-wegen-datensammlung-104053819, 2021.

Siebert, Sören, Bea Brünen, und Lev Lexow . „DSGVO: Das müssen Webseitenbetreiber und Unternehmer über die Datenschutz-Grundverordnung wissen!“ https://www.e-recht24.de/datenschutzgrundverordnung.html, 2021.

T3n. „Anzahl der Werbe-Tracker ist seit DSGVO-Einführung rückläufig.“ https://t3n.de/news/dsgvo-anzahl-der-werbe-tracker-ist-seit-dsgvo-einfuehrung-ruecklaeufig-1116767/, 2018.

Wko. „EU-Datenschutz-Grundverordnung (DSGVO): Die wichtigsten Fragen und Antworten.“ https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/datenschutz-grundverordnung-fragen-und-antworten.html, 2021a.

Wko. „EU-Datenschutz-Grundverordnung (DSGVO): Dokumentationspflicht - Verzeichnis von Verarbeitungstätigkeiten.“ https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.html, 2021d.

Wko. „EU-Datenschutz-Grundverordnung (DSGVO): Pflichten des Auftragsverarbeiters.“ https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Pflichten-des-Auftragsver.html#:~:text=Haftung&text=Ist%20mehr%20als%20ein%20Auftragsverarbeiter,Verantwortliche)%20f%C3%BCr%20den%20gesamten%20Schaden., 2021e.

Wko. „EU-Datenschutz-Grundverordnung (DSGVO): Rechtsdurchsetzung und Strafen.“ https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Rechtsdurchsetzung-und-St.html, 2021c.

Wko. „EU-Datenschutz-Grundverordnung (DSGVO): Sachlicher und räumlicher Anwendungsbereich.“ https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Sachlicher-und-raeumliche.html, 2021b.

Anhang

Schriftliche Einwilligung gemäß Datenschutz (Muster)

Muster

Die im Vertrag angegebenen personenbezogenen Daten, insbesondere Name, Anschrift, Telefonnummer, Bankdaten, die allein zum Zwecke der Durchführung des entstehenden Vertragsverhältnisses notwendig und erforderlich sind, werden auf Grundlage gesetzlicher Berechtigungen erhoben.

*Für jede darüber hinausgehende Nutzung der personenbezogenen Daten und die Erhebung zusätzlicher Informationen bedarf es regelmäßig der Einwilligung des Betroffenen. Eine solche Einwilligung können Sie im Folgenden Abschnitt **freiwillig** erteilen.*

Einwilligung in die Datennutzung zu weiteren Zwecken

Sind Sie mit den folgenden Nutzungszwecken einverstanden, kreuzen Sie diese bitte entsprechend an. Wollen Sie keine Einwilligung erteilen, lassen Sie die Felder bitte frei.

☐ Ich willige ein, dass mir die Kreditanstalt XYZ (Vertragspartner) postalisch Informationen und Angebote zu weiteren Finanzprodukten zum Zwecke der Werbung übersendet.

☐ Ich willige ein, dass mir die Kreditanstalt XYZ (Vertragspartner) per E-Mail/Telefon/Fax/SMS* Informationen und Angebote zu weiteren Finanzprodukten zum Zwecke der Werbung übersendet. (* bei Einwilligung bitte Unzutreffendes streichen)

[Ort, Datum]
[Unterschrift des Betroffenen]

Rechte des Betroffenen: Auskunft, Berichtigung, Löschung und Sperrung, Widerspruchsrecht

Sie sind gemäß § 34 BDSG jederzeit berechtigt, gegenüber der Kreditanstalt XYZ (Vertragspartner) um umfangreiche **Auskunftserteilung** zu den zu Ihrer Person gespeicherten Daten zu ersuchen.

Gemäß § 35 BDSG können Sie jederzeit gegenüber der Kreditanstalt XYZ (Vertragspartner) die **Berichtigung, Löschung und Sperrung** einzelner personenbezogener Daten verlangen.

Sie können darüber hinaus jederzeit ohne Angabe von Gründen von Ihrem **Widerspruchsrecht** Gebrauch machen und die erteilte Einwilligungserklärung mit Wirkung für die Zukunft abändern oder gänzlich widerrufen. Sie können den Widerruf entweder postalisch, per E-Mail oder per Fax an den Vertragspartner übermitteln. Es entstehen Ihnen dabei keine anderen Kosten als die Portokosten bzw. die Übermittlungskosten nach den bestehenden Basistarifen.

Abbildung 1: Mustervorlage Einwilligungserklärung
Quelle: https://www.datenschutz.org/einwilligungserklaerung/

Erteilung der Auskunft nach Art 15 DSGVO[1]

Sehr geehrte/r [*Auskunftswerberln*],

1. Ihren Antrag auf Auskunft nach Art 15 DSGVO haben wir am [*Datum*] erhalten. Sie haben darin Ihre Identität ausreichend nachgewiesen.
2. {Bei einer Beantwortung innerhalb der gesetzlichen Frist} Innerhalb der gesetzlichen Frist von einem Monat kommen wir hiermit Ihrem Antrag nach.
   {bei Fristverlängerung nach Art 12 Abs 3 DSGVO} Wie mit Schreiben vom [*Datum*] mitgeteilt, haben wir aufgrund [*entweder Komplexität des Antrages oder Anzahl Ihrer Anträge, nähere Begründung notwendig*] die Möglichkeit zur Fristverlängerung auf drei Monate in Anspruch genommen.
3. {falls keine Daten verarbeitet werden} Es werden keine Daten zu Ihrer Person verarbeitet, welche über Ihren Auskunftsantrag und die entsprechende interne Dokumentation hinausgehen.[2] {Dann weiter mit Textbaustein Nr 9}.
   {Wenn Daten verarbeitet werden}[3] Wir verarbeiten folgende Daten zu Ihrer Person:[4]
   [*es folgt eine Liste mit den konkret verarbeiten Daten*].
   Kopien/Ausdrucke der relevanten Datenverarbeitungen finden Sie im Anhang.[5]
4. Diese werden zu folgenden Zwecken verarbeitet: [*Zwecke einschließlich Rechtsgrundlagen aufzählen*]
5. {falls Daten weitergegeben werden} Die Daten werden an folgende Empfänger übermittelt: [*Empfänger bzw Empfängerkategorien einschließlich ihrem Sitzland aufzählen*[6]].
   {falls Daten in ein Drittland übermittelt werden} Die Übermittlung der Daten an jene Empfänger, die sich in einem Drittland befinden, basiert auf folgenden Garantien: [Garantien ergänzen[7]]
6. Wir speichern Ihre Daten [*Dauer oder zumindest Kriterien für Speicherdauer angeben*].
7. {falls Daten nicht bei der betroffenen Person erhoben wurden}: Wir haben Ihre Daten erhalten von ***[verfügbare Angaben zur Herkunft Ihrer Daten zB Adressverlag XY]***.
8. {falls anwendbar} Wir setzten Verfahren zur automatisierter Entscheidungsfindung / Profiling[8] ein, die Ihnen gegenüber eine rechtliche Wirkung haben oder Sie in ähnlicher Weise erheblich beeinträchtigt: [*bitte aussagekräftige Informationen über die involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen ergänzen*].
9. Ihnen stehen grundsätzlich die Rechte auf Berichtigung, Löschung, Einschränkung und Widerspruch zu. Dafür wenden Sie sich an uns. Wenn Sie glauben, dass die Verarbeitung Ihrer Daten gegen das Datenschutzrecht verstößt oder Ihre datenschutzrechtlichen Ansprüche sonst in einer Weise verletzt worden sind, können Sie sich bei der Datenschutzbehörde beschweren. In Österreich ist die Datenschutzbehörde zuständig.[9]

Abbildung 2: Mustervorlage Auskunftserteilung

Quelle: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-musterschreiben-auskunftserteilung.pdf

Verzeichnis von Verarbeitungstätigkeiten

Inhalt

I. Allgemeine Information zur Organisation
II. Verarbeitungstätigkeiten, für welche die Organisation Verantwortlicher ist
III. Verarbeitungstätigkeiten, für welche die Organisation Auftragsverarbeiter ist

I. Allgemeine Information zur Organisation

1. Name und Kontaktdaten der Organisation	
Name/Firmenwortlaut der Organisation:	
Adresse:	
E-Mail-Adresse:	
2. Name und Kontaktdaten des Datenschutzbeauftragten (sofern bestellt)	
Name:	
Adresse:	
E-Mail-Adresse:	
Telefonnummer:	

II. Verarbeitungstätigkeiten, für welche die Organisation Verantwortlicher ist

[Nachfolgende Tabelle ist für jede Verarbeitungstätigkeit zu reproduzieren]

1. Allgemeine Angaben zur Verarbeitungstätigkeit	
LfNr:	*zB 1*
Name der Verarbeitungstätigkeit:	*zB Kundenverwaltungsmanagement*

2. Allfällige gemeinsam Verantwortliche		
Firmenwortlaut	Adresse	E-Mail-Adresse
...	...	...

3. Verarbeitungszwecke
Liste der Verarbeitungszwecke, zB Erfüllung eines mit dem Kunden geschlossenen Vertrages.

4. Kategorien Betroffener
Liste der Kategorien betroffener Personen, zB Arbeitnehmer, Kunden.

5. Datenkategorien	
Datenkategorie	Speicherdauer
zB Name	*zB bis drei Jahre nach Vertragsbeendigung*
...	...

6. Kategorien von Empfängern (Verantwortliche und Auftragsverarbeiter)		
Kategorie von Empfängern	Typ (Verantwortlicher oder Auftragsverarbeiter)	Land (sofern außerhalb des EWR)
zB IT Dienstleister	*zB Auftragsverarbeiter*	*zB EWR*
zB Konzerngesellschaften	*zB Verantwortlicher*	*zB EWR, USA, Kanada*
...	...	...

7. Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen
...

III. Verarbeitungstätigkeiten, für welche die Organisation Auftragsverarbeiter ist

[Nachfolgende Tabelle ist für jede Verarbeitungstätigkeit zu reproduzieren]

1. Allgemeine Angaben zur Verarbeitungstätigkeit	
LfNr:	*zB 1*
Name der Verarbeitungstätigkeit:	*zB Hosting von Websites*

2. Verantwortliche, in deren Auftrag diese Verarbeitungstätigkeit durchgeführt wird				
Firmenwortlaut	Adresse	E-Mail-Adresse	Kontaktdaten des Datenschutzbeauftragten*	Kontaktdaten des Vertreters**
...	...	...	...	...

* Sofern der jeweilige Verantwortliche einen Datenschutzbeauftragten bestellt hat: Name, Adresse, E-Mail-Adresse und Telefonnummer

** Sofern der jeweilige Verantwortliche nicht im EWR niedergelassen ist und einen inländischen Vertreter bestellt hat: Name, Adresse und E-Mail-Adresse

3. Datenübermittlungen an Sub-Auftragsverarbeiter				
Firmenwortlaut	Adresse	E-Mail-Adresse	Kontaktdaten des Datenschutzbeauftragten*	Kontaktdaten des Vertreters**
...	...	...	...	...

* Sofern der jeweilige Sub-Auftragsverarbeiter einen Datenschutzbeauftragten bestellt hat: Name, Adresse, E-Mail-Adresse und Telefonnummer

** Sofern der jeweilige Sub-Auftragsverarbeiter nicht im EWR niedergelassen ist und einen inländischen Vertreter bestellt hat: Name, Adresse und E-Mail-Adresse

4. Beschreibung der technischen und organisatorischen Sicherheitsmaßnahmen
...

Abbildung 3: Mustervorlage Verzeichnis der Verarbeitungstätigkeiten
Quelle: (Feiler und Horn 2018, 50-52)

Abbildung 4: intransparente Tracking-Methode
Quelle: https://www.forum-verlag.com/blog-di/auskunftspflicht-dsgvo