JOHANNES KEPLER
UNIVERSITÄT LINZ

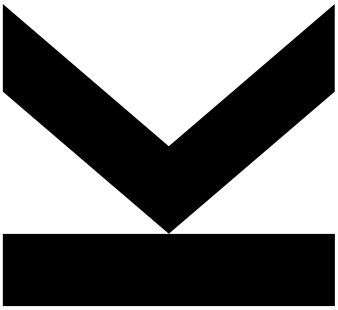
Eingereicht von
Alisa Pincotan

Angefertigt am
Institut für Europarecht

Beurteiler / Beurteilerin
Assoz. Univ.-Prof. Dr. Franz Leidenmühler

Dezember 2018

Die Rolle des Datenschutz-beauftragten nach der DSGVO



Diplomarbeit

zur Erlangung des akademischen Grades

Magistra der Rechtswissenschaften

im Diplomstudium

Rechtswissenschaften

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
www.jku.at
DVR 0093696

JOHANNES KEPLER
UNIVERSITÄT LINZ

EIDESSTATTLICHE ERKLÄRUNG

Ich erkläre an Eides statt, dass ich die vorliegende Diplomarbeit selbstständig und ohne fremde Hilfe verfasst, andere als die angegebenen Quellen und Hilfsmittel nicht benutzt beziehungsweise die wörtlich oder sinngemäß entnommenen Stellen als solche kenntlich gemacht habe.

Die vorliegende Diplomarbeit ist mit dem elektronisch übermittelten Textdokument identisch.

Feldkirchen, Dezember 2018

Alisa Pincotan

GENDERERKLÄRUNG

Zum besseren Verständnis und zur leichteren Lesbarkeit gilt in diesem Text bei allen personenbezogenen Bezeichnungen die gewählte Form für beide Geschlechter.

DANKSAGUNG

Zu Beginn möchte ich mich bei Herrn Assoz. Univ.-Prof. Dr. Franz Leidenmühler für seine kompetente und freundliche Betreuung bedanken.

Desweiteren möchte ich meiner Familie (Ioan, Lidia und Cosmin Horj) großen Dank aussprechen, weil sie mich Jahre lang motiviert und unterstützt haben und nie den Glauben an mich verloren haben.

Auch meiner Chefin, Carmen Schwarz, möchte ich Danke sagen, für die Hilfe und das Verständnis während der Studienzeit und für die Möglichkeit, Beruf und Studium zu vereinen.

Der größte Dank gilt aber meiner Tochter Emely, denn weil sie stets ein so braves und intelligentes Kind war und ist, konnte ich trotz Familie und Beruf, dass Studium erfolgreich beenden.

Abkürzungsverzeichnis

Abs	Absatz
Art	Artikel
BDSG	Bundesdatenschutzgesetz
B-VG	Bundes-Verfassungsgesetz
bzw	beziehungsweise
DHG	Dienstnehmerhaftpflichtgesetz
DSBA	Datenschutzbeauftragte
DSFA	Datenschutz-Folgenabschätzung
DSG 2000	Datenschutzgesetz
DSGVO	Datenschutz-Grundverordnung
DSMS	Datenschutzmanagementsystem
DSRL	Datenschutzrichtlinie
ErwGr	Erwägungsgrund
etc	et cetera
EU	Europäische Union
f	folgende
ff	fortfolgende
gem	gemäß
leg cit	legis citate
lit	litera
ISMS	Informationssicherheitsmanagementsystem
IT	Informationstechnik
IWG	Informationsweiterverwendungsgesetz

RL	Richtlinie(-n)
S	Seite
TKG	Telekommunikationsgesetz
usw	und so weiter
uvm	und vieles mehr
vgl	vergleiche
WP 29	Die Art-29-Datenschutzgruppe
zB	zum Beispiel
Z	Ziffer

Inhalt

I. Einleitung

Die Datenschutz-Grundverordnung (DSGVO) gilt seit dem 25.05.2018 unmittelbar in allen Mitgliedstaaten der Europäischen Union (EU). Dies bedeutet, dass in Österreich das Datenschutzgesetz 2000 (DSG 2000) und in Deutschland das alte Bundesdatenschutzgesetz (BDSG) nicht mehr zur Geltung kommen. Nicht außer Acht zu lassen ist die Tatsache, dass der europäische Gesetzgeber den Mitgliedstaaten zahlreiche Öffnungsklauseln zur Verfügung gestellt hat. Österreich hat diese genutzt und zwei große Novellen herausgebracht. Einerseits kam 2017 das Datenschutz-Anpassungsgesetz 2018 heraus, andererseits beschloss die Regierung kurz vor dem In-Kraft-Treten der DSGVO das Datenschutz-Deregulierungs-Gesetz 2018, welches gleichzeitig mit der EU-Verordnung wirksam wurde.[1]

Eine Überarbeitung des Datenschutzrechts wurde nötig, weil es in den letzten zwanzig Jahren zu einem Wandel in der Technologie kam. Der Datenschutz muss sich in der heutigen Zeit unter anderem mit Big Data, Industrie 4.0 etc auseinandersetzen. Dies ist einige Dezennien zuvor noch keine Thematik gewesen.

Die EU passte mit den neuen Verordnungen den Datenschutz de facto an den Fortschritt der Digitalisierung an. Des Weiteren wollte die EU mit dieser Verordnung die Unterschiede bereinigen, die mit der vorherigen RL entstanden sind, weil jeder Mitgliedstaat diese sehr individuell umgesetzt hatte und der Datenschutzlevel sehr unterschiedlich war. Dieses Ziel konnte man nur mit einer Verordnung erreichen, welche nicht erst durch ein nationales Gesetz umgesetzt werden musste.[2]

Man hört des Öfteren die Metapher, dass Daten das Öl des einundzwanzigsten Jahrhunderts sein sollen. Sowohl der Vorstandschef der Deutschen Telekom *Timotheus Höttges* als auch die deutsche Bundeskanzlerin *Angela Merkel* stellen derartige Vergleiche in ihren Diskursen an.

[1] Vgl *WKO*, EU-Datenschutz-Grundverordnung (DSGVO), abrufbar unter: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html (02.07.2018).
[2] Vgl *1&1 Guide*, Datenschutz-Grundverordnung (DSGVO), abrufbar unter: https://www.1und1.at/digitalguide/websites/online-recht/datenschutz-grundverordnung-regeln-fuer-unternehmen/ (02.07.2018).

Anhand dieser Redewendung merkt man, dass Daten an Wichtigkeit gewonnen haben. Früher hat man Geld mit Öl gemacht, in der heutigen Zeit hingegen unweigerlich mit Daten.[3]

Der Zeitpunkt der Initiierung der DSGVO konnte nicht besser sein. Genau jetzt, wo große Konzerne wie Google, Facebook etc mit nur einem Klick auf Daten zugreifen können und die Freiwilligkeit nicht sehr eindeutig ist, wenn die Konsequenz daraus wäre, dass Personen aus der digitalen Welt ausgeschlossen werden, sollten Sie Ihre Daten nicht freigeben. Die EU hat den ersten Schritt gesetzt, um das Gleichgewicht zwischen Benutzern und den großen Internetgiganten herzustellen, damit die Grundrechte jedes Einzelnen nicht in Gefahr sind. Natürlich bedarf es nicht nur in der EU einer solchen Reform, sondern auf der ganzen Welt. Ob das realistisch ist, wird sich in den nächsten Jahren zeigen.[4]

Im Zuge dieser Arbeit wird anfänglich die Geschichte des Datenschutzes aufgearbeitet. Gefolgt werden die historischen Ausführungen von Erörterungen diverser Begrifflichkeiten in der DSGVO mit Unterschieden zum DSG 2000.

Der Schwerpunkt dieser Diplomarbeit liegt bei den diversen Aspekten des Datenschutzbeauftragten (DSBA). Gleichermaßen werden auch Themen, wie die Datenschutzfolgenabschätzung (DSFA) und die Betroffenenrechte, näher besprochen und erklärt.

[3] Vgl *Spitz*, Daten - das Öl des 21. Jahrhunderts? (2017), 1ff.
[4] Vgl *Giegerich*, ZEuS 3/2016, 302ff.

II. Datenschutz-Grundverordnung allgemein

A. Historie

Vor dem 25.05.2018 galt die Datenschutzrichtlinie 95/46/EG als Sekundärrechtsakt. Diese wurde durch die DSGVO ersetzt.[5] Als RL war sie nicht unmittelbar wirksam, sondern musste durch einen nationalen Rechtsakt umgesetzt werden.[6] Dies tat Österreich, indem es die RL durch das DSG 2000 realisierte.[7] Die Initiative für diese Reform kam von der Europäischen Kommission, die eine öffentliche Konsultation zum Entwurf des Themas Datenschutz anregte. Der Fokus richtete sich vor allem auf die Tatsache, dass durch die Digitalisierung und Globalisierung der Datenschutz unbedingt verbessert werden musste. Des Weiteren kam die DSGVO mit der Empfehlung, den Datenschutz durch eine Verordnung zum Schutz der Verarbeitung personenbezogener Daten und den freien Datenverkehr zu regeln. Somit sollte die Einigkeit in den Mitgliedstaaten gegeben sein.[8]

Die Republik Österreich zeigte bei den Verhandlungen, dass Sie großen Wert auf Datenschutz legt. Dies spiegelte sich wieder, indem Österreich bei diversen Verhandlungen und Diskussionen sehr aktiv mitwirkte. Österreich stimmte im schriftlichen Verfahren am 08.04.2016 jedoch gegen die DSGVO. Aus seiner Sicht fanden sehr viele wichtige Problemstellungen keine Lösung und war mit dem Ergebnis nicht zufrieden.[9]

Nach zahlreichen Jahren mühsamer Verhandlungen erfolgte schlussendlich die Unterzeichnung der beiden Akte am 27.04.2016, die dieses Datenschutzpaket bilden. Am 04.05.2016 wurde die DSGVO im EU-Amtsblatt kundgemacht und ersetzt die RL 95/46/EG. Zwanzig Tage nach der Veröffentlichung ist diese mit 25.05.2016 in Kraft getreten. Die Umsetzungsfrist endete am 24.05.2018.[10]

---

[5] Vgl *Fercher/Riedl*, DSGVO: Entstehungsgeschichte und Problemstellungen aus österreichischer Sicht, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 7.
[6] Vgl *eur-lex.europa.eu*, Richtlinien der Europäischen Union, abrufbar unter: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=LEGISSUM%3Al14527 (03.07.2018).
[7] Vgl *Fercher/Riedl*, DSGVO: Entstehungsgeschichte und Problemstellungen aus österreichischer Sicht, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 16f.
[8] Vgl *Fercher/Riedl*, DSGVO: Entstehungsgeschichte und Problemstellungen aus österreichischer Sicht, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 7ff.
[9] Vgl Fercher/Riedl, DSGVO: Entstehungsgeschichte und Problemstellungen aus österreichischer Sicht, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 17.
[10] Vgl *Fercher/Riedl*, DSGVO: Entstehungsgeschichte und Problemstellungen aus österreichischer Sicht, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016), 16.

Zusammenfassend besteht dieses Reformpaket nicht nur aus der Verordnung (EU) 2016/679, sondern auch aus der „*Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.04.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates*".[11]

B. Anwendungsbereich

1. Verordnung

Wie schon erwähnt, ist der Datenschutz nicht mehr in einer RL verankert, sondern in einer Verordnung. Dies bedeutet, dass die DSGVO unmittelbar in allen Mitgliedstaaten anwendbar ist und es keiner nationalen Regelung bedarf, ausgenommen dort, wo die Verordnung den Mitgliedstaaten einen Spielraum erlassen hat.[12]

2. Sachlicher Anwendungsbereich

Die DSGVO gilt für die gesamte oder teilweise automatisierte sowie für die nichtautomatisierte Verarbeitung personenbezogener Daten, welche in einem Dateisystem gespeichert sind oder gespeichert werden sollen.[13]

Unter dem Begriff der Verarbeitung gem Art 4 Z 2 leg cit versteht man jedes Verfahren, automatisiert oder nicht, und jegliche Tätigkeit im Zusammenhang mit personenbezogenen Daten, wie zB das Erheben, das Erfassen, die Organisation, das Ordnen, das Löschen uvm von Daten.

Wie der erste Teil des Art 2 Abs 1 DSGVO besagt, dass die ganze oder teilweise automatisierte Verarbeitung von dieser Verordnung erfasst ist. Was damit genau gemeint ist, wurde bis heute nicht deutlich ausformuliert.

---

[11] RL (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27.April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates, ABl L 2016/119, 89.
[12] Vgl *Knyrim*, Die Datenschutz-Grundverordnung: Entwicklung und Anwendungsbereich (Teil I), Dako 2015/21, 33. https://rdb.manz.at/document/rdb.tso.LIdako20150205 (05.7.2018).
[13] Vgl Art 2 Abs 1 DSGVO.

Es gibt die Möglichkeit, eine Parallele zum DSG 2000 zu finden. Man nimmt § 4 Z 7 DSG 2000 und passt diesen an die Norm an. Das bedeutet, dass eine Verarbeitung ganz oder teilweise automatisiert ist, wenn Sie ohne Hilfe der Informationstechnik (IT) nicht vorgenommen werden kann.

Wird der ganze Verarbeitungsablauf nur technisch durchgeführt, spricht man von einer automatisierten Verarbeitung. Sollte eine Tätigkeit wie das Speichern automatisch durch ein IT-System geschehen und eine andere Tätigkeit, wie der Abgleich, manuell erfolgen, dann liegt eine teilweise automatisierte Verarbeitung im Sinne des Art 2 Abs 1 zweiter Fall leg cit vor.[14]

Auch die nichtautomatisierte Verarbeitung im Dateisystem ist von der DSGVO erfasst. Gem Art 4 Z 6 leg cit versteht man unter einem Dateisystem,[15] „*jede strukturierte Sammlung personenbezogener Daten, welche nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen, geografischen Gesichtspunkten geordnet geführt wird*“.[16]Unter strukturierter Sammlung versteht man, dass die personenbezogenen Daten eine gewisse inhaltliche Regelung haben und nach bestimmten Kriterien geordnet sind, um den Zugang zu diesen Daten zu erleichtern.[17] Im ErwGr 15 wird auf dieses Problem eingegangen und dort ist zu finden, dass Akten und -sammlungen, welche unstrukturiert sind, eben nicht von der DSGVO erfasst sind.[18]

Außerdem sind von der DSGVO nur natürliche Personen betroffen. Nicht von Relevanz sind die Staatsbürgerschaft und der Aufenthaltsort des Menschen.[19]

Ausgenommen vom sachlichen Anwendungsbereich sind Tätigkeiten betreffend:

a. nationaler Sicherheit,
b. Außen- und Sicherheitspolitik der EU,
c. Familie und Privates,
d. Ermittlung, Aufdeckung oder Verfolgung von Delikten oder deren Exekution.[20]

[14] Vgl *Bergauer* in: *Knyrim*, Personenbezogene Daten. Begriff und Kategorien, 44f.
[15] Vgl *Bergauer* in: *Knyrim*, Personenbezogene Daten. Begriff und Kategorien, 45.
[16] Art 4 Z 6 DSGVO.
[17] Vgl *Bergauer* in: *Knyrim*, Personenbezogene Daten. Begriff und Kategorien, 45.
[18] Vgl VO (EU) 679/2016 ABl L 2016/119, 15.
[19] Vgl VO (EU) 679/2016 ABl L 2016/119, 14.
[20] Vgl Art 2 Abs 2 DSGVO.

3. Räumlicher Anwendungsbereich

Die Neuerungen betreffen jedes Unternehmen in jeder Branche, das Personendaten verarbeitet und eine Niederlassung in der EU hat. Nicht von Bedeutung ist die Tatsache, ob die Daten innerhalb der EU oder in einem Drittland verarbeitet werden. Die Rechtsform des Unternehmens ist irrelevant, solange beispielsweise die Tochtergesellschaft die Tätigkeit tatsächlich durch eine feste Einrichtung in der EU ausübt. Darüber hinaus gilt die DSGVO auch für die Verarbeitung der Personendaten betroffener Menschen, die ihren Aufenthaltsort in der EU haben.

Gleichermaßen gilt die DSGVO, wenn der Verantwortliche oder Auftragsverarbeiter und dessen Niederlassung außerhalb des Gebietes der EU ist und dieser Waren oder Dienstleistungen innerhalb der EU anbietet oder das Verhalten natürlicher Personen beobachtet.[21]

C. Begrifflichkeiten

1. Datenkategorien

Es werden von der DSGVO drei Arten von Daten geschützt:

a. Personenbezogene Daten,
b. Daten besonderer Kategorie (sensible Daten),
c. strafrechtliche Daten.[22]

Personenbezogene Daten gem Art 4 Z 1 leg cit sind Angaben zu Betroffenen, deren Identität bestimmt oder bestimmbar ist[23]. Diese bestehen aus drei Komponenten. Der erste Bestandteil ist die Verarbeitung. Er bezieht sich auf den sachlichen Anwendungsbereich. Dieser wurde bereits ausführlich besprochen. Werden solche Daten verarbeitet, muss eine Verbindung zu einer natürlichen Person aufgezeigt werden, indem das Datum etwas über die Person aussagt oder man das benutzte Datum diesem Menschen zuordnen kann (Inhaltskomponente). Die Identitätskomponente ist dann gegeben, wenn mit diesem Datum ein Mensch

[21] Vgl *Hladjk*, sachlicher und räumlicher Anwendungsbereich der DSGVO, in *Knyrim* (Hrsg), Datenschutz-Grundverodnung (2016), 40f.
[22] Vgl *Bergauer* in*: Knyrim*, personenbezogene Daten. Begriff und Kategorien, 43ff.
[23] Vgl Art 4 Z 1 DSGVO.

identifiziert werden kann. Sind alle drei Bestandteile gegeben, spricht man von personenbezogenen Daten im Sinne der DSGVO.[24]

Die neue Verordnung schützt nach Art 9 DSGVO im speziellen die besonderen Kategorien personenbezogener Daten und nach Art 10 DSGVO die strafrechtsbezogenen Daten. Im DSG 2000 findet man oft den Begriff der sensiblen Daten. Der Begriff sensible Daten als solcher wird auch jetzt noch verwendet, weil nach dem ErwGr 10 diese zwei Wörter die gleiche Bedeutung haben.[25]

Sensible Daten finden sich im Art 9 der DSGVO und werden taxativ aufgezählt:

a. Rassische und ethnische Herkunft,
b. politische Meinung,
c. religiöse oder weltanschauliche Überzeugung,
d. Gewerkschaftszugehörigkeit,
e. genetische Daten,
f. biometrische Daten,
g. Gesundheitsdaten,
h. Daten zum Sexualleben,
i. Daten zur sexuellen Orientierung.[26]

Im Art 4 DSGVO bekommen Gesundheitsdaten, biometrische und genetische Daten eine neue Definition. Laut Art 4 Z 15 leg cit sind das Daten, welche auf den Gesundheitszustand einer natürlichen Person hinweisen, zB Informationen über Krankheiten, Abhängigkeiten und klinische Behandlungen einer Person. Die Herkunft der Daten ist nicht relevant. Außerdem versteht man unter diesem Begriff die Informationen, die man benötigt, um eine Gesundheitsleistung zur Verfügung zu stellen, etwa die Sozialversicherungsnummer, welche jeder natürlichen Person zugeteilt wird, um diese hundertprozentig identifizieren zu können.[27]

Die genetischen Daten haben als neue Kategorie Eingang in das Recht gefunden und sind im Art 4 Z 14 leg cit näher definiert. Das sind Informationen von erblichen Merkmalen, über die man durch diverse Analysen, wie beispielsweise mittels einer Nukleinsäure-Analyse gelangt. Diese Rubrik ist deshalb so sensibel, weil aus diesen

[24] Vgl *Bergauer* in: *Knyrim*, personenbezogene Daten. Begriff und Kategorien, 63.
[25] Vgl *Bergauer* in*: Knyrim*, personenbezogene Daten. Begriff und Kategorien, 56; Vgl VO (EU) 679/2016 ABl L 2016/119, 10.
[26] Vgl Art 9 Abs 1 DSGVO.
[27] Vgl *Bergauer* in: *Knyrim*, personenbezogene Daten. Begriff und Kategorien, 57f.

Daten sowohl der Gesundheitszustand als auch die rassische und ethnische Herkunft herausgefiltert werden können.[28]

Dies gilt auch für biometrischen Daten gem Art 4 Z 14 DSGVO. Von diesen Informationen kann man ebenso auf den Gesundheitszustand bzw auf die rassische und ethnische Herkunft schließen. Jene Daten geben Auskunft über die biologischen Eigenschaften eines Menschen. Infolgedessen kann eine natürliche Person eindeutig identifiziert werden bzw wird Ihre Identität belegt. Beispiele dafür sind die Netzhautanalyse oder der Iris-Scan.[29]

Anonyme Daten werden von der DSGVO nicht erfasst, wenn überhaupt kein Bezug zum Menschen vorhanden ist. Sollte dieser Bezug existieren, es aber kaum denkbar ist, dass diese natürliche Person identifizierbar ist, werden diese Daten von der DSGVO nicht erfasst.[30]

2. Grundsätze

Bei der Verarbeitung von personenbezogenen Daten müssen nach Art 5 DSGVO gewisse Grundsätze eingehalten werden. Diese Prinzipien bauen auf der DSRL auf und sind in Österreich im § 6 Abs 1 DSG 2000 zu finden. Nur der Grundsatz in Art 5 Abs 1 lit f DSG wurde in die DSGVO aufgenommen und die Zweckbindung nach Art 5 Abs 1 lit b DSGVO durch einen Kompatibilitätstest erweitert. In Art 5 DSGVO werden die folgenden Prinzipien aufgezählt:[31]

a. „*Rechtmäßigkeit,*
b. *Verarbeitung nach Treue und Glauben,*
c. *Transparenz,*
d. *Zweckbindung,*
e. *Datenminimierung,*
f. *Richtigkeit,*
g. *Speicherbegrenzung,*
h. *Integrität und Vertraulichkeit und,*
i. *Rechenschaftspflicht.*“[32]

[28] Vgl *Bergauer* in: *Knyrim,* personenbezogene Daten. Begriff und Kategorien, 58; Vgl VO (EU) 679/2016 ABl L 2016/119, 34.
[29] Vgl *Bergauer* in: Knyrim, Personenbezogene Daten. Begriff und Kategorien, 58f.
[30] Vgl *Bergauer* in: *Knyrim*, Personenbezogene Daten. Begriff und Kategorien, 63.
[31] Vgl *Kastelitz* in: *Knyrim*, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, 99f.
[32] Art 5 DSGVO.

3. Rechtmäßigkeit der Datenverarbeitung

Um die unter Abschnitt II.C.1 *Grundsätze* genannten Daten verarbeiten zu können, muss der Grundsatz der Rechtmäßigkeit erfüllt sein. Dieser ist dann gegeben, wenn die Verarbeitung aufgrund einer konformen rechtlichen Grundlage gem Art 6 Abs 1 DSGVO erfolgt ist, wie:

a. die Einwilligung der betroffenen Person,
b. die Erfüllung eines Vertrages oder vorvertraglicher Maßnahmen,
c. die Erfüllung gesetzlicher Verpflichtung,
d. die Protektion lebenswichtiger Interessen von Personen,
e. die Erfüllung einer Aufgabe im öffentlichen Interesse oder Ausübung durch die öffentliche Gewalt,
f. das berechtigtes Interesse des Verantwortlichen oder eines Dritten.[33]

Für die Verarbeitung von sensiblen und strafrechtlichen Daten gibt es zusätzlich Voraussetzungen. Informationen laut Art 10 DSGVO dürfen nur unter behördlicher Aufsicht oder auf Grundlage des EU bzw des innerstaatlichen Rechts verwendet werden. Grundsätzlich ist das Benützen von Daten gem Art 9 DSGVO verboten. Es gibt in Abs 2 DSGVO Erlaubnistatbestände, die das trotzdem zulassen, wie zB:

a. eine ausdrückliche Einwilligung,
b. eine gesetzliche Grundlage,
c. Daten wurden öffentlich gemacht.[34]

D. Akteure der Datenschutz-Grundverordnung

1. Verantwortliche und Auftragsverarbeiter

Im DSG 2000 werden die Begriffe des Auftraggebers gem § 4 Z 4 DSG 2000 und des Dienstleisters laut § 4 Z 5 und §§ 10 f DSG 2000. Diese Begriffe sind in der DSGVO

[33] Vgl *Kastelitz* in: *Knyrim*, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, 101ff; Vgl Art 6 Abs 1 lit a - f DSGVO.
[34] Vgl *Kastelitz* in: *Knyrim*, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten, 112f; Vgl Art 9 DSGVO; Vgl Art 10 DSGVO.

durch den Verantwortlichen gem Art 4 Z 8 DSGVO und den Auftragsverarbeiter laut Art 4 Z 7 DSGVO ersetzt worden.[35]

Auftragsverarbeiter nach der DSGVO ist eine „*natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, welche personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet*".[36] Der wichtigste Punkt dabei ist, dass der Auftragsverarbeiter nur tätig wird, wenn er einen Auftrag vom Verantwortlichen bekommt, Daten zu verarbeiten. In der DSGVO ist nicht näher präzisiert worden, was mit Auftrag gemeint ist. Würde dies genauer ausgelegt werden, könnte man darunter subsumieren, dass Personen, welche dem Verantwortlichen zuzurechnen sind, beispielsweise ein Angestellter oder Arbeiter, eben kein Auftragsverarbeiter im Sinne der DSGVO sind. Es besteht eine eigenständige Beziehung zum Unternehmen in einer eigenständigen Position.[37]Der Auftragsverarbeiter hat keine Entscheidungsbefugnis und ist an die Weisungen des Verantwortlichen gebunden.[38]

Verantwortlicher im Sinne der DSGVO ist die „*natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet*".[39] Aus Art 4 DSGVO geht hervor, dass die Entscheidungskompetenz als die tatsächliche Fähigkeit alleine oder gemeinsam mit einem anderen Verantwortlichen darüber zu entscheiden, was mit den jeweiligen Daten passiert, ein Hauptkriterium ist. Eine gemeinsame Verarbeitung im Sinne der DSGVO ist dann vorhanden, wenn zwei oder mehrere Verantwortliche einheitlich über Mittel und Zweck der Verarbeitung entscheiden.[40]

In der Praxis ist es von hoher Relevanz zu unterscheiden, ob ein Auftragsverarbeitungsverhältnis oder eine gemeinsame Tätigkeit gem Art 26 DSGVO vorliegt. Die Regelungen der DSGVO für diese zwei Beziehungen sind gänzlich verschieden und sie haben andere Anforderungen. Ebenso ist die Vertragsbasis eine grundsätzlich andere.[41]

---

[35] Vgl *Geuer/Reinisch*, Abgrenzungsfragen zur Zusammenarbeit der verschiedenen Akteure der Datenschutz-Grundverordnung, jusIT 2018, 98.
[36] Art 4 Z 8 DS-GVO.
[37] Vgl *Fritz in Jahnel* (Hrsg), Datenschutzrecht (2017) Der Auftragsverarbeiter im Fokus der DS-GVO, 11.
[38] Vgl *Geuer/Reinisch*, Abgrenzungsfragen zur Zusammenarbeit der verschiedenen Akteure der Datenschutz-Grundverordnung, jusIT 2018, 98.
[39] Art 4 Z 7 Datenschutz-Grundverordnung.
[40] Vgl Art 26 Datenschutz-Grundverordnung.
[41] Vgl *Fritz in Jahnel* (Hrsg), Datenschutzrecht (2017) Der Auftragsverarbeiter im Fokus der DS-GVO, 11.

2. Betroffener

Der Hauptakteur in Bezug auf die DSGVO ist die betroffene Person selbst, deren personenbezogene Daten gem Art 4 Z 1 leg cit verarbeitet werden. In den bisherigen Ausführungen wurde bereits erörtert, dass nur natürliche Personen betroffen sein können und Behörden und Unternehmen nicht.[42]

3. Empfänger

Laut Art 4 Z 9 DSGVO kann ein Empfänger sowohl eine natürliche als auch eine juristische Person sein, dem personenbezogenen Daten offengelegt werden. Nicht von Bedeutung ist, ob es sich um einen Dritten handelt oder nicht. Empfänger können daher auch Auftragsverarbeiter gem Art 4 Z 8 leg cit sein.[43]

4. Dritte

Der Dritte wird in der DSGVO als eine natürliche oder juristische Person definiert, die jedoch nicht der Verantwortliche, der Auftragsverarbeiter oder der Betroffene selbst sein kann. Er ist also jemand, für den die personenbezogenen Daten von Relevanz sind.[44]

5. Aufsichtsbehörde

Im Art 4 Z 21 wird die Aufsichtsbehörde als unabhängige Stelle bezeichnet, die vom jeweiligen Staat eingerichtet wird. Gem Art 51 Abs 1 leg cit ist die Hauptaufgabe der Aufsichtsbehörde, die Observation der Anwendung der DSGVO, damit keine Grundrechte und -freiheiten der natürlichen Person verletzt werden. Nach Art 52 leg cit DSGVO sind die Aufsichtsbehörden völlig weisungsfrei und unterliegen nur der Kontrolle durch die Gerichte.[45]

6. Kontrollorgan des Verantwortlichen

Ein weiterer Akteur in Zusammenhang mit der DSGVO ist der DSBA. Für die vorliegende Diplomarbeit ist er der Haupthandelnde. Im folgenden Kapitel wird der DSBA unter mehreren Aspekten näher betrachtet.

---

[42] Vgl Art 4 DSGVO.
[43] Vgl *Selk* in: *Knyrim*, Verzeichnis von Verarbeitungstätigkeiten (Art 30): Wer muss es haben, wie hat es auszusehen, 192; Vgl Art 4 DSGVO.
[44] Vgl Abs 4 DSGVO.
[45] Vgl *Flendrovsky* in: *Knyrim*, Die Aufsichtsbehörde, 282; Vgl Art 4 DSGVO.

III. Der Datenschutzbeauftragte

Der Verantwortliche wie auch der Auftragsverarbeiter sind in gewissen Fällen nach Art 37 Abs1 leg cit DSGVO verpflichtet einen DSBA zu bestellen. Diese Obligation besteht vor allem für sämtliche Behörden und öffentlichen Stellen, aber nicht nur, denn auch alle sonstigen Institutionen und Unternehmen, deren Kerntätigkeit in der umfangreichen, systematischen Überwachung von Personen besteht oder die in großem Umfang sensible Daten verarbeiten, müssen einen DSBA bestellen. Einrichtungen haben die Möglichkeit freiwillig einen DSBA zu benennen.

Der DSBA ist kein neuer Akteur in der DSGVO. Er wurde schon in der RL 95/46/EG bedacht, jedoch gab es in dieser keine Pflicht einen zu ernennen. Zum einen unterstützen die DSBA den Verantwortlichen bei der Rechenschaftspflicht, zum anderen treten diese als Vermittler zwischen der Aufsichtsbehörde, der betroffenen Person und den Verantwortlichen auf.

Für die Einhaltung der DSGVO ist nicht der DSBA verantwortlich, diese Aufgabe trifft den Verantwortlichen oder den Auftragsverarbeiter. Gleichzeitig müssen die beiden genannten gute Konditionen schaffen, sodass der DSBA seiner Arbeit richtig ausüben kann.

A. Benennung eines Datenschutzbeauftragten

1. Obligatorische Benennung

Art 37 Abs 1 leg cit normiert in welchen drei Fälle ein DSBA zu benennen ist:[46]

a. Wenn „*die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird, mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln,*
b. *die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige*

[46] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 4f.

und systematische Überwachung von betroffenen Personen erforderlich machen, oder

c. *die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Artikel 10 besteht*."[47]

Während Behörden immer einen DSBA bestellen müssen, orientiert sich bei Unternehmen dies an ihrer Haupttätigkeit.[48]

1.1 Behörde und öffentliche Stelle

Die DSGVO beinhaltet keine Erklärung, was unter Behörde und öffentliche Stelle zu verstehen ist. Die Art-29-Datenschutzgruppe (WP 29) ist der Meinung, dass jeder einzelne Staat diese Begriffe selbst nach seinem Recht auslegen solle. Sie beinhalten also alle bundes- und landesweiten Behörden, aber auch andere Einrichtungen, die dem öffentlichen Recht unterliegen, sind davon erfasst.[49] Eine Behörde ist eine öffentliche Institution, die zur Abwicklung von Aufgaben berechtigt ist. Die öffentliche Stelle hingegen ist nicht so leicht auszulegen, hierbei muss auf bereits bestehende Gesetze zurückgegriffen werden. Im Informationsweiterverwendungsgesetz (IWG) wird in § 4 Z 1 die öffentliche Stelle als[50]:

a. „*der Bund,*

b. *bundesgesetzlich eingerichtete Selbstverwaltungskörperschaften,*

c. *Einrichtungen auf bundesgesetzlicher Grundlage wie Stiftungen, Privatstiftungen, Fonds und Anstalten sowie sonstige Körperschaften des öffentlichen Rechts,*

d. *Unternehmungen im Sinne des Art. 126b Abs. 2 B-VG, des Art. 127 Abs. 3 B-VG und des Art. 127a Abs. 3 B-VG,*

[47] Art 37 Abs 1 DSGVO.
[48] Vgl *König*, Der Datenschutzbeauftragte im Unternehmen, ecolex 2018, 490.
[49] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 6.
[50] Vgl *König* in: *Knyrim*, Der Datenschutzbeauftragte, 233.

e. *Verbände, die sich überwiegend aus zwei oder mehreren öffentlichen Stellen gemäß lit. a bis d zusammensetzen*“[51] definiert.

Das bedeutet, dass zB die Landesregierung als Behörde und der ORF oder die ASFINAG als öffentliche Stellen fungieren.[52]

1.2 Kerntätigkeit des Datenschutzbeauftragten

Gem Art 37 DS-GVO müssen jeder Verantwortliche und Auftragsverarbeiter einen DSBA benennen, wenn die Kernaufgabe eines Unternehmens aus der umfangreichen, systematischen und immer wiederkehrenden Beobachtung von Betroffenen besteht oder wenn die Kerntätigkeit in der Verarbeitung von besonderer Kategorien von Daten gem Art 9 und 10 DSGVO liegt.

Es stellt sich daher die Frage, wie diese Kerntätigkeit definiert werden sollte. In ErwGr 97 wird sie so festgelegt, dass sich die Kernaufgabe des Verantwortlichen nicht auf seine Nebentätigkeiten bezieht, sondern nur auf die Haupttätigkeit.[53] Was das wiederum bedeutet, wurde im Gesetz nicht klar ausgelegt, aber es wird davon ausgegangen, dass die wichtigsten Geschäftsprozesse des Unternehmens damit gemeint sind.[54] So werden zB die Personalverwaltung oder eine Mitarbeiterüberwachung eines normalen Unternehmens nicht als dessen Haupttätigkeit, sondern als Nebentätigkeit bewertet werden und folglich müsste man in diesen Fällen keinen DSBA normieren.[55] Wenn aber die Verarbeitung von Daten ein nichttrennbarer Teil der Tätigkeit des Verantwortlichen oder Auftragsverarbeiters ist, dehnt sich diese auch auf die Kerntätigkeit aus. ZB ist die Haupttätigkeit eines Krankenhauses Menschen zu behandeln und zu versorgen. Dazu muss das Spital die Gesundheitsdaten des Patienten aufnehmen, damit es seinen Aufgaben effizient nachgehen kann. Deshalb ist eine der Kerntätigkeiten eines Krankenhauses das Verarbeiten von sensiblen Daten und deswegen wäre ein DSBA zu benennen.[56] Weitere Beispiele für Unternehmen, die einen DSBA zu bestellen haben, sind Banken, Versicherungen etc.[57]

[51] § 4 Z1 IWG.
[52] Vgl *König* in: *Knyrim*, Der Datenschutzbeauftragte, 233.
[53] Vgl *König* in: *Knyrim*, Der Datenschutzbeauftragte, 234.
[54] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 8.
[55] Vgl *König* in: *Knyrim*, Der Datenschutzbeauftragte, 234f.
[56] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 8.
[57] Vgl *König* in: *Knyrim*, Der Datenschutzbeauftragte, 234f.

1.3 Umfangreiche Verarbeitung

Laut Art 37 Abs 1 lit c DSGVO haben Unternehmen einen DSBA zu ernennen, wenn sie umfangreich sensible oder strafrechtliche Daten verarbeiten. In der DSGVO selbst ist nicht definiert, was unter umfangreich zu subsumieren ist. Die WP 29 empfiehlt bei der Beurteilung folgende Punkte zu bedenken:

a. die Nummer der Personen, die davon erfasst sind,
b. die Masse an Daten, welche verarbeitet wird,
c. der Zeitrahmen, in dem die Tätigkeit erfolgt,
d. die geographische Lage der Verarbeitung.[58]

Aus dem ErwGr 91 lässt sich ableiten, wann eine Verarbeitung von Daten eben nicht umfangreich ist. Das ist dann der Fall, wenn zB ein einzelner Arzt Gesundheitsdaten seiner Patienten verarbeitet. Werden diese hingegen von einem Krankenhaus verwendet, muss ein DSBA bestellt werden.[59]

1.4 Regelmäßige und systematische Überwachung

Auch die Auslegung von regelmäßig und systematisch ist nicht aus der DSGVO selbst zu entnehmen, sondern aus den ErwGR. Denn in ErwGr 24 wird erwähnt, was unter dem Kontrollieren von Betroffenen zu verstehen ist. Das ist jede Art der Überwachung und Erstellung eines Profiles im Netz, auch wenn dies nur für Werbung erfolgt. Es ist zu beachten, dass dies nicht nur für die Beobachtung im Internet gilt, sondern für jede Art von Verfolgung.

Die WP 29 sagt, dass regelmäßig dann gegeben ist, wenn mindestens eines der folgenden Argumente zutrifft[60]:

a. „*fortlaufend oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommend,*
b. *immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretend*
c. *ständig oder regelmäßig stattfindend*“.[61]

[58] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 9.
[59] Vgl *König* in: *Knyrim*, Der Datenschutzbeauftragte, 235; Vgl VO (EU) 679/2016 ABl L 2016/119, 91.
[60] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 10.

Der Begriff systematisch ist laut WP 29 dann vorhanden, wenn mindestens eine der angeführten Eigenschaften zutrifft[62]:

a. „*systematisch vorkommend,*
b. *vereinbart, organisiert oder methodisch,*
c. *im Rahmen eines allgemeinen Datenerfassungsplans erfolgend,*
d. *im Rahmen einer Strategie erfolgend*".[63]

Vor allem folgende Tätigkeiten erfüllen die regelmäßige und systematische Überwachung: Telekommunikationsdienstleistungen, Analysieren des Risikos bei der Kreditvergabe etc.

2. Fakultative Benennung

Außer in den bereits genannten Fällen können der Verantwortliche, der Auftragsverarbeiter oder Vereinigungen bzw Verbände, die Verantwortliche oder Auftragsverarbeiter vertreten, nach Art 37 Abs 4 auch freiwillig einen DSBA benennen.[64] Der fakultativ ernannte DSBA muss die gleichen Voraussetzungen wie der obligatorische im Unternehmen erfüllen. Trifft das nicht zu, kann man nicht von einer gesetzlichen Benennung ausgehen, sondern nur von einer internen Vorschrift innerhalb des Unternehmens.

3. Datenschutzbeauftragter des Auftragsverarbeiters

Der Art 37 DSGVO gilt gleichermaßen für Verantwortliche wie für Auftragsverarbeiter. Es kann sein, dass eine dieser Parteien die Voraussetzungen für eine obligatorische Benennung erfüllt und die andere Partei nicht. Außerdem kann es vorkommen, dass beide einen DSBA ernennen müssen. Ein Beispiel: Ein kleines Unternehmen, welches sich mit dem Vertrieb von Möbel beschäftigt, benötigt eine Dienstleistung eines Auftragsverarbeiters, dessen Kerntätigkeit darin besteht, Website-Analysen zu erstellen. Da es sich hier um eine kleine Firma handelt, wird der Begriff der umfangreichen Verarbeitung nicht erfüllt sein. Beim Auftragsverarbeiter wird das anders sein, weil er

[61] Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 10.
[62] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 10.
[63] Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 10.
[64] Vgl *König,* Der Datenschutzbeauftragte im Unternehmen, ecolex 2018, 491.

sehr viele Kunden hat, für die er Dienstleistungen durchführt, und wenn all diese Kunden zusammengezählt werden, würde eine umfangreiche Verarbeitung von personenbezogenen Daten vorliegen. Der Auftragsverarbeiter ist daher zur Benennung eines DSBA verpflichtet und das kleine Unternehmen – als Verantwortlicher – hat keinen zu bestellen.[65]

4. Gemeinsamer Datenschutzbeauftragter

Nach Art 37 Abs 2 DSGVO kann eine Gruppe von Unternehmen einen gemeinsamen DSBA ernennen, wenn[66] „*von jeder Niederlassung aus der Datenschutzbeauftragte leicht erreicht werden kann*".[67] Die Erreichbarkeit kann so ausgelegt werden, dass der DSBA in der Besorgung seiner Aufgaben als Ansprechperson für die betroffene Person aber auch für die Aufsichtsbehörde gilt. Deshalb muss er die Erreichbarkeit innerhalb des Unternehmens und extern garantieren.[68] Dies umfasst nicht unbedingt die physische Präsenz, sondern es sind alle Möglichkeiten in Betracht zu ziehen wie Skype, Telefonie, E-Mail etc.[69] Auf diese Weise sollen die Kontaktdaten des DSBA im Sinne der DSGVO für jeden Beteiligten zur Verfügung stehen.[70]

Ein anderes wesentliches Merkmal eines gemeinsamen DSBA ist die Sprache. Es dürfen keine Sprachhindernisse innerhalb der Unternehmensgruppe und zu den Mitarbeitern bzw zu der Aufsichtsbehörde vorhanden sein.[71]

Laut Art 37 Abs 3 können auch öffentliche Stellen und Einrichtungen einen gemeinsamen DSBA benennen unter Berücksichtigung ihrer Größe und Struktur. Wie bereits erläutert, gilt hier dasselbe in Hinblick auf die Kommunikation und Sprache.

DSBA haben sehr viele Angelegenheiten zu erledigen, weshalb der Verantwortliche oder der Auftragsverarbeiter die Verantwortung dafür tragen muss, dass der DSBA, trotz der mehreren in seinen Bereich fallenden öffentlichen Stellen und Einrichtungen, seine Aufgabe erfüllen kann.[72]

---

[65] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 11.
[66] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 12.
[67] Art 37 Abs 2 DSGVO.
[68] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 12.
[69] Vgl *König in:* Knyrim, Der Datenschutzbeauftragte, 236.
[70] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 12.
[71] Vgl *König in:* Knyrim, Der Datenschutzbeauftragte, 236.
[72] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 12f.

5. Fähigkeiten und Fachwissen des Datenschutzbeauftragten

Vorerst ist abzuklären, wo der DSBA seinen Sitz haben kann. Nach Abschnitt 4 der DSGVO bedarf es der sicheren Erreichbarkeit des DSBA. Die WP 29 empfiehlt, dass der DSBA seinen Sitz innerhalb der EU hat. Nicht von Relevanz ist, ob der Verantwortliche oder Auftragsverarbeiter seine Niederlassung innerhalb der EU hat. Es ist trotzdem unter Umständen möglich einen DSBA außerhalb der EU zu haben, wenn der Verantwortliche oder Auftragsverarbeiter seinen Sitz nicht in der EU hat.[73]

Laut Art 37 Abs 5 wird der DSBA „*auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben*“.[74]

- Fachwissen

  Dieser Begriff ist in der DSGVO nicht genau definiert, es müssen jedoch die Sensitivität, die Komplexion und das Volumen der Daten, die verarbeitet werden, miteinander in Harmonie sein. Der DSBA wird mehr Unterstützung brauchen und ihm wird ein höheres Fachwissen abverlangt, wenn zB eine Tätigkeit, bei der Informationen verarbeitet werden, schwierig und komplex ist oder sensible Daten umfangreich benutzt werden. Zudem ist von Relevanz, ob Informationen regelmäßig an Lokationen außerhalb der EU geschickt werden oder dies nur manchmal passiert.[75]

- Berufliche Qualifikation

  Es ist Angelegenheit des DSBA, auf die Einhaltung aller datenschutzrechtlichen Anweisungen in der betroffenen Einrichtung hinzuwirken, daher ist juristisches Know-how obligat. Außerdem muss der DSBA dafür sorgen, dass die Datensicherheit laut DSGVO eingehalten wird. Man wird nicht umhinkommen, die technischen IT-Systeme zu prüfen. Um solche Audits durchführen zu können, ist es nötig Kenntnisse in der Informatik zu haben. Auch betriebswirtschaftliche

[73] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 13.
[74] Art 37 Abs 5 DSGVO.
[75] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 13.

Fähigkeiten sind erwünscht bzw Kenntnisse im Bereich der Organisation, in dem der DSBA tätig ist, weil in diesem Fachwissen erheblich die Arbeit erleichtert.

Auch soziale Qualifikationen, wie zB Zuverlässigkeit oder Genauigkeit, spielen eine große Rolle, aber auch methodische Fähigkeiten, wie zB Prüfungsmethodik oder Projektmanagement sind erforderlich.

Neben dem theoretischen Wissen sollte die als DSBA berufene Person über praktische Erfahrung verfügen, man geht hier von mindestens zwei Jahren aus.[76]

6. Interner und externer DSBA

Nach Art 37 Abs 6 DSGVO kann der DSBA entweder ein Mitarbeiter der Einrichtung sein (interner DSBA) oder als externer Dienstleister beauftragt werden. Keine dieser Varianten kann als besser oder schlechter bezeichnet werden. Bei beiden Arten gibt es sowohl Vor- als auch Nachteile.

Der interne DSBA hat den Vorteil, dass er das Unternehmen bzw die Behörde/öffentliche Stelle, das Personal, den internen Zyklus und das IT-System schon kennt. Außerdem kann er mit ständiger Präsenz und Verfügbarkeit dienen und somit ist die reibungslose interne Kommunikation besser gesichert. Durch den direkten Kontakt fördert er die Kooperation mit anderen Abteilungen und er ist hinsichtlich der Unternehmensorganisation immer am neusten Stand.[77]

Der Dienstleistungsvertrag des externen DSBA kann sowohl mit einer natürlichen als auch mit einer juristischen Person erfolgen, die nicht zur Organisation des Verantwortlichen oder Auftragsverarbeiters gehört. Äußert wichtig ist, dass Interessenskonflikte ausgeschlossen werden können, indem jeder Mitwirkende der Organisation, welcher der Beschäftigung des DSBA nachgeht, alle Anforderungen erfüllt, die in Abschnitt 4 DSGVO verlangt werden.

Genauso wesentlich ist das Faktum, dass jeder DSBA durch die Normen der DSGVO geschützt werden muss. ZB sollte ein Dienstleistungsvertrag mit einem externen DSBA nicht ohne Grund in Hinsicht auf seine Arbeit gekündigt werden können, aber auch der

[76] Vgl *Horn*, jusIT 2016/91, 201.
[77] Vgl *Horn*, jusIT 2016/91, 200.

interne DSBA soll nicht einfach entlassen werden können, weil er seiner Tätigkeit als Beauftragter nachgegangen ist.[78]

7. Kontaktdaten

Nach Art 37 Abs 7 DSGVO müssen der Verantwortliche und Auftragsverarbeiter die Kontaktdaten des DSBA veröffentlichen und die Daten dann an die Aufsichtsbehörde weiterleiten.[79]

Durch diese Pflicht soll gewährleistet werden, dass sich die betroffenen Personen, die sich nicht ausschließlich innerhalb der Organisation befinden, direkt an den DSBA herantreten können. Auch die Datenschutzbehörde kann sich auf diesem Weg unmittelbar an den DSBA wenden, ohne mit einem andren Bereich der Organisation in Kontakt treten zu müssen.

Die Kontaktdaten sollen jene Informationen enthalten, die der Aufsichtsbehörde wiels auch der betroffenen Person die Chance geben, sich in simpelster Art beim DSBA zu melden. Das sollte per Post, aber auch per Telefon oder Email, möglich sein. Eine weitere Möglichkeit zur Kommunikationserleichterung wäre, eine individuelle Hotline oder ein Kontaktformular, das unmittelbar an den DSBA weitergeleitet wird, einzurichten.

In der DSGVO wird nicht vorgeschrieben, dass in den bekanntgegebenen Daten, der Name des DSBA anzugeben ist, der Gesetzgeber überlässt dies den Verantwortlichen oder Auftragsverarbeitern und den DSBA.

Die Bekanntgabe des Namens des DSBA bei der Aufsichtsbehörde ist laut Art 39 Abs 1 DSGVO zwingend notwendig.[80]

B. Rechtstellung des Datenschutzbeauftragten

1. Einbindung und Unterstützung

Gem Art 38 haben der Verantwortliche und der Auftragsverarbeiter die Pflicht, dass sie den DSBA der Vorschrift entsprechend und rechtzeitig in datenschutzrechtlichn Fragen

[78] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 14.
[79] Vgl Art 37 DSGVO.
[80] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 15.

und Angelegenheiten einbeziehen. Diese frühzeitige Einbindung und Unterrichtung des DSBA hat den Vorteil, dass die Verordnung von Beginn an korrekt eingehalten wird und sollte deshalb bei jeder Organisation einen Standardprozess darstellen. Bei der DSFA wird in der DSGVO explizit erwähnt, dass der DSBA sehr früh einzubinden ist und der Verantwortliche den Vorschlag des DSBA bei der Abwicklung der DSFA zu bedenken hat.

Außerdem ist es wichtig, dass der DSBA innerhalb der Organisation, aber vor allem von den Abteilungen, die Daten verarbeiten, als Kommunikationspartner anerkannt wird.

Die Organisation sollte sich exemplarisch bemühen, dass

- der DSBA regelmäßig zu den Managementsitzungen eingeladen wird;
- er bei Datenschutzangelegenheiten, welche eine Entscheidung benötigen, stets zu Rate gezogen wird;
- der Standpunkt des DSBA stets ernst genommen wird. Sollte die Einrichtung anderer Meinung als der DSBA sein, empfiehlt sich eine detaillierte Dokumentation darüber.
- bei Verletzung der DSGVO der DSBA sofort miteinzubeziehen ist.

Alle Organisationen sind laut Art 38 Abs 2 verpflichtet, ihren DSBA zu unterstützen,[81] „*indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen*“.[82] Das umfasst vor allem:

- den Support des DSBA durch das obere Management;
- die Befürwortung von genügend Zeit für die Verwirklichung seiner Aufgaben. Von Relevanz ist das besonders dann, wenn der hausinterne DSBA nicht Vollzeit angestellt ist oder der externe DSBA noch anderen Verpflichtungen nachgeht;
- die Gewährung von adäquaten Finanzmitteln und die Beistellung von genügend Mitarbeitern, Räumlichkeiten, Ausrüstung etc;

[81] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 16.
[82] Artikel 37 Abs 2 DSGVO.

- die Bekanntgabe der Existenz und Rolle eines DSBA in der gesamten Einrichtung;
- das Zur-Verfügung-Stellen von anderen Abteilungen, wie zB Human Ressource, Legal, IT usw, sodass der DSBA von diesen Neuigkeiten, Support und Vorschläge bekommen kann;
- die Weiterbildung des DSBA. Dieser sollte die Chance bekommen immer auf dem neuesten Stand in Bezug auf die DSGVO zu sein. Der DSBA sollte so motiviert werden, sein Wissen in diesem Bereich dauernd zu erweitern, indem er an verschiedenen Veranstaltungen teilnimmt.
- In einer größeren Organisation kann es sein, dass es notwendig ist, dass ein ganzes DSBA-Team zusammengestellt wird. Wenn dies der Fall sein sollte, dann sollten die Rollen innerhalb des Teams klar definiert sein.

Je schwieriger und empfindlicher die Verarbeitungstätigkeiten von Daten sind, desto mehr Mittel müssen den DSBA bereitgestellt werde, damit diese die Anforderungen der DSGVO erfüllen können.[83]

2. Unabhängigkeit und Weisungsfreiheit

„*Der Verantwortliche und der Auftragsverarbeiter stellen sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält*“[84] und im ErwGr 97 wird noch erläutert, dass der DSBA in seiner Funktion und bei der Besorgung seiner Pflichten völlig unabhängig sein muss.

Das heißt, dass der DSBA bei der Wahrnehmung seiner Aufgaben keine Anordnungen nach Art 39 DSGVO annehmen muss, wie zB das Resultat ausschauen sollte, wie der DSBA mit einer Beschwerde umzugehen hat, oder wann die Aufsichtsbehörde hinzuzuziehen ist. Die Unabhängigkeit des DSBA bezieht sich nur auf die Aufgaben laut Art 39 DSGVO.

Es trägt trotzdem immer der Verantwortliche bzw der Auftragsverarbeiter die Verantwortung bei der Einhaltung der Vorschriften nach der DSGVO. Sind der DSBA

[83] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 17.
[84] Art 38 Abs 3 DSGVO.

und die anderen zwei Akteure nicht gleicher Meinung, sollte der DSBA die Chance haben, der obersten Leitung seine abweichende Meinung zur Kenntnis zu bringen. Denn in Art 38 Abs 3 DSGVO wird noch einmal verdeutlicht, dass der DSBA[85] „*unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters*“[86] zu berichten hat.

Letzten Endes darf dem DSBA aufgrund seiner Stellung nicht als DSBA gekündigt oder er in irgendeiner Art benachteiligt werden. Einem abberufenen DSBA wird es in der Realität schwerfallen zu beweisen, dass er aufgrund seiner Tätigkeit gekündigt worden ist. Zum jetzigen Zeitpunkt gibt es keinen besonderen Kündigungsschutz bei der Erfüllung dieser Tätigkeit.[87]

3. Interessenskonflikte

„*Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Der Verantwortliche oder der Auftragsverarbeiter stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen*“.[88]

Wie Art 38 Abs 6 DSGVO besagt, darf der DSBA auch andere Positionen wahrnehmen, aber nur wenn diese zu keinem Interessenkonflikt mit seiner Funktion als DSBA führen. Vor allem sollte der DSBA nicht solch eine Funktion innehaben, bei der er Mittel und Zweck von der Verarbeitung von Daten bestimmt.

Solche Funktionen, die einen Interessenkonflikt darstellen könnten, sind speziell Leitungsfunktionen, wie zB Leiter der Einrichtung, der Rechtsabteilung, des Personalwesens, oder der IT-Abteilung.

Auch bei der Erledigung von Aufgaben durch den externer DSBA kann es zu Interessenkonflikten kommen und das besonders dann, wenn dieser den Verantwortlichen oder Auftragsverarbeiter vor Gericht wegen dem Datenschutz vertritt.

Abhängig von der Bedeutung der Organisation, vom Tätigkeitsfeld und Aufbau kann es für den Verantwortlichen und Auftragsverarbeiter empfehlenswert sein:

- die Funktionen zu nennen, welche nicht mit denen des DSBA vereinbar sind;

[85] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 17f.
[86] Art 38 Abs 3 DSGVO.
[87] Vgl *Horn*, jusIT 2016/91, 199.
[88] Art 38 Abs 6 DSGVO.

- interne Vorgaben aufzustellen, um gerade solche Interessenkonflikte zu vermeiden;
- eine Aufklärung über mögliche Interessenkonflikte zu betreiben;
- ein Statement abzugeben, dass sich der DSBA in seiner Position eben in keinem Konflikt befindet;
- dass die Stellenausschreibung des DSBA, egal ob intern oder extern, um einer Kontroverse aus dem Weg zu gehen, genauestens und exakt ausformuliert wird.

C. Aufgaben des Datenschutzbeauftragten

1. Überwachung, Unterrichtung und Beratung

Damit der DSBA seinen Aufgaben effizient nachgehen kann, müssen die Personalangaben und die Kontaktdaten des Individuums in der ganzen Organisation bekannt gegeben werden. Der Belegschaft der Einrichtung muss die Anordnung gegeben werden, bei Fragen oder Konzepten mit DSGVO-Inhalten, früh genug an den DSBA heranzutreten und diesen bei offenen Problemstellungen zu konsultieren. Dieses Ziel kann durch interne RL, Anweisungen oder Mitarbeiterinformation erreicht werden.

Außer dieser Tätigkeit hat der DSBA noch die Pflicht, die Beachtung der datenschutzrechtlichen Vorschriften zu überprüfen. Das betrifft nicht allein die DSGVO, sondern auch andere datenschutzrechtliche Bestimmungen in diversen Rechtshandlungen der EU, wie zB die anstehende E-Privacy-Verordnung oder in nationalen Rechtsakten das § 107 TKG 2003. Diese Kontrolltätigkeit beansprucht die periodische Überwachung von Arbeitsabläufen, Datenverarbeitungstätigkeiten, IT-Systemen, Anweisungen vom Dienstgeber, diverse Vereinbarungen, wie auch technische und organisatorische Maßnahmen, die Bearbeitung der Betroffenenrechte sowie die Verarbeitungstätigkeiten beim Verzeichnis.

Außerdem hat der DSBA die Aufgabe das Datenschutzkonzept der Organisation zu kontrollieren und bei Bedarf neue Anregungen für Verbesserungen abzugeben. Neben dem Datenschutzkonzept sollte auch ein Datenschutzmanagementsystem (DSMS) eingeführt werden. Besonders in größeren Einrichtungen ist ein dokumentiertes DSMS nicht wegdenkbar, ohne dass alle datenschutzrelevanten Vorschriften eingehalten

werden. Denkbar wäre auch eine Kombination aus einem DSMS und einem Informationssicherheitsmanagementsystem (ISMS) nach ISO/IEC 27001.

Die Unterrichtung der Mitarbeiter der Organisation durch den DSBA ist ebenfalls unerlässlich. Dies kann zB durch E-Learning-Tools, Awareness-Kampagnen, aber auch durch Zusendung von Newsletter oder Informationsfolder erfolgen. Auch die Betroffenenrechte sind nicht außer Acht zu lassen, denn dort muss der DSBA schätzen, wie hoch das Risiko einer Verarbeitung und der Schutzbedarf der Daten der natürlichen Personen ist und im Zuge dessen treffen ihn hier Kontroll- und Überwachungspflichten, damit das Risiko für die betroffenen Personen so gut wie möglich reduziert werden kann.

Zuletzt sollte der DSBA bei der DSFA hinzugezogen werden, auch ohne Anfrage, und dieser kontrolliert ihre richtige Ausführung.[89]

2. Verzeichnis

In Art 30 DSGVO ist geregelt, dass jeder Verantwortliche wie auch Auftragsverarbeiter ein Verzeichnis über die Verarbeitungstätigkeiten verpflichtend zu führen hat und dieses muss von der Aufsichtsbehörde jederzeit in elektronischer oder schriftlicher Form abrufbar sein.[90]

Der Zweck der Führung eines solchen Verzeichnisses ist im ErwGr 82 definiert:[91] „*Zum Nachweis der Einhaltung dieser Verordnung sollte der Verantwortliche oder der Auftragsverarbeiter ein Verzeichnis der Verarbeitungstätigkeiten, die seiner Zuständigkeit unterliegen, führen*“.[92]

In Art 30 Abs 5 DSGVO sind die Ausnahmen aufgezählt, wann ein solches Verarbeitungsverzeichnis nicht zu führen ist. Wenn eine Organisation mehr als 250 Mitarbeit hat, ist jedenfalls ein Verzeichnis zu führen. Bei unter 250 Mitarbeiter muss man zusätzliche Kriterien beachten. Man muss nur dann kein Verzeichnis über die Verarbeitungstätigkeiten führen, wenn die Verarbeitung:

a) nicht regelmäßig erfolgt,

[89] Vgl *Horn*, jusIT 2016/91, 197f.
[90] Vgl *Selk* in: *Knyrim*, Verzeichnis von Verarbeitungstätigkeiten (Art 30), 183ff.
[91] Vgl *Selk* in: *Knyrim*, Verzeichnis von Verarbeitungstätigkeiten (Art 30), 182.
[92] VO (EU) 679/2016 ABl L 2016/119, 81.

b) zu keinem Risiko für die Grundrechte und Freiheiten der natürlichen Personen führt,

c) keine Daten besonderer Kategorien oder strafrechtliche Daten beinhaltet.[93]

Nach Art 30 Abs 1 DSGVO hat das Verzeichnis folgende Angaben zu enthalten:

- Name und Kontaktdaten des Verantwortlichen/Vertreters und des DSBA;
- Zweck der Verarbeitung, denn personenbezogene Daten dürfen nur für einen eindeutigen und legitimen Zweck erhoben werden und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden;
- Darstellung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- Kategorien von Empfängern und Empfänger im Drittland;
- gegebenenfalls Übermittlung von Daten ins Drittland und Dokumentierung geeigneter Garantien;
- wenn möglich, Angaben zu den vorgesehenen Fristen der Datenlöschung;
- wenn möglich, Angaben zu den technischen und organisatorischen Maßnahmen.[94]

Das Verarbeitungsverzeichnis sollte als ein Hilfsmittel angesehen werden, in dem sich die Einrichtungen einen Überblick über alle Verarbeitungstätigkeiten der Fachabteilungen verschaffen können. Auf das Verzeichnis laut Art 30 DSGVO kann der Verantwortliche oder Auftragsverarbeiter nicht verzichten, wenn er alle Datenschutzvorschriften einhalten will.[95]

- Funktion des DSBA in Zusammenhang mit dem Verzeichnis

Rechtlich ist es nicht verboten, dass der Verantwortliche oder Auftragsverarbeiter die Aufgabe des Erstellens und Führens des Verzeichnisses dem DSBA überträgt. Die Verantwortlichkeit kann aber nicht übergeben werden, denn letztlich haftet trotzdem der Verantwortliche der Einrichtung. Durch dieses Verzeichnis hat der DSBA die Möglichkeit seine Aufgaben besser wahrzunehmen. Er kann es als Hilfsmittle verwenden, um so die

[93] Vgl Art 30 Abs 5 DSGVO.
[94] Vgl Art 30 Abs 1 DSGVO.
[95] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 22f.

Einhaltung der Datenschutzbestimmungen zu kontrollieren, aber auch die Unterrichtung und das Consulting des Verantwortlichen und Auftragsverarbeiters sind effizienter.[96]

3. Datenschutzfolgenabschätzung

Auch wenn die Verarbeitung von personenbezogenen Daten wegen einer rechtlichen Grundlage erfolgt, können für die Grundrechte und -freiheiten der betroffenen Person Gefahren entstehen.

Infolgedessen hat die DSGVO ein Hilfsmittel zur Darstellung, Minimierung und Analysierung von Risiken erschaffen, die DSFA.[97]

Gem Art 35 Abs 1 DSGVO ist dann eine DSFA zwingend durchzuführen, wenn für die Rechte der natürlichen Person durch die Verarbeitungstätigkeit ein hohes Risiko besteht. Eine solche erhöhte Gefahr besteht laut Art 35 Abs 3 DSGVO jedenfalls bei:

- Profiling, wenn es zu einer Rechtswirkung kommt,
- Verarbeitung von Daten nach Art 9 und 10 DSGVO, und
- methodischen und enormen Observationen von öffentlichen Räumen.[98]

Eine DSFA ist ebenso dann erforderlich, wenn die Aufsichtsbehörde gem Art 35 Abs 5 DSGVO eine Liste mit Verarbeitungstätigkeiten veröffentlicht, welche ein solches Risiko beinhalten („Black List“). In Österreich hat der Gesetzgeber im November 2018 eine solche Liste veröffentlicht. Diese Anführung von Verarbeitungstätigkeiten, bei denen eine DSFA vorzunehmen ist, stellt das Gegenstück zur schon seit Mai 2018 existierenden „White List“ dar, die Verarbeitungsvorgänge listet, die keine DSFA erfordern.[99]

In Art 35 Abs 7 DSGVO wird genau definiert, welche Kriterien eine DSFA zu beinhalten hat:

- die methodische Erläuterung der Verarbeitungstätigkeiten und deren Zwecke,

---

[96] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 22.
[97] Vgl *DSK,* Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO abrufbar unter: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_5_Datenschutz-Folgenabschaetzung.pdf (21.11.2018).
[98] Vgl *dataprotect*, Datenschutz-Folgenabschätzung (DSFA) abrufbar unter: https://www.dataprotect.at/leistungen/dsfa/ (21.11.2018).
[99] Vgl *Dorda*, "BLACK LIST" DER DATENSCHUTZBEHÖRDE ERLASSEN abrufbar unter: http://www.dorda.at/publications/black-list-der-datenschutzbeh%C3%B6rde-erlassen (21.11.2018).

- eine Charakterisierung der Unerlässlichkeit und Angemessenheit der Verarbeitungstätigkeiten im Zusammenhang mit den dafür gegeben Zwecken,
- eine Bewertung der Gefahren für die Grundrechte und -freiheiten der natürlichen Person,
- die Maßnahmen, die gesetzt werden, um diese Risiken zu minimieren.[100]

Wenn im Zuge der DSFA festgestellt wird, dass ein solches erhöhtes Risiko für die betroffene Person besteht und man dieses nicht durch das Setzten von Maßnahmen minimieren kann, so besteht die Pflicht vor Beginn der Verarbeitungstätigkeit die Aufsichtsbehörde darüber zu informieren. Sollte die Aufsichtsbehörde zu dem Entschluss kommen, dass der Verantwortliche oder Auftragsverarbeiter das Risiko nicht ordnungsgemäß ermittelt oder eingedämmt hat, gibt diese die Möglichkeit dem Verantwortlichen oder dem Auftragsverarbeiter binnen acht Wochen eine schriftliche Empfehlung auszufolgen und kann dann ihren Befugnissen gem Art 36 Abs 2 DSGVO nachgehen.[101]

- Funktion des Datenschutzbeauftragten bei der Datenschutz-Folgenabschätzung

Wie bereits erläutert, ist es die Angelegenheit des Verantwortlichen oder des Auftragsverarbeiters und nicht des DSBA eine DSFA durchzuführen. Der DSBA kann und soll diese Akteure bei dieser Aufgabe unterstützen. In der DSGVO gibt es zwei Art, die von dieser Aufgabe sprechen. Im ersten Fall besagt Art 35 Abs 2 DSGVO, dass der Verantwortliche bei der DSFA sich den DSBA zu Hilfe holen soll. Art 39 Abs 1 lit c überträgt dem DSBA die Pflicht die[102]: „*Beratung – auf Anfrage – im Zusammenhang mit der Datenschutz- Folgenabschätzung und Überwachung ihrer Durchführung gemäß Artikel 35*“[103], zu managen. Der DSBA sollte aber auf jeden Fall bei den folgenden Aufgaben hinzugezogen werden:

- bei der Unsicherheit, ob eine DSFA durzuführen ist oder nicht,
- wenn sich die Frage stellt, wie eine solche DSFA auszusehen hat,

[100] Vgl Art 35 Abs 7 DSGVO.
[101] Vgl Art 36 DSGVO.
[102] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 20.
[103] Vgl Art 39 Abs 1 lit c DSGVO.

- welche Maßnahmen gesetzt werden müssen, um die Gefahr für die Rechte der natürlichen Personen abzuwenden,
- bei der Überprüfung, ob die DSFA korrekt erfolgt ist und sie den Vorgaben der DSGVO entspricht.

Sollte der Verantwortliche dem Rat des DSBA nicht folgen, sollte die Begründung schriftlich festgehalten werden.[104]

4. Der Datenschutzbeauftragte als zentrale Anlaufstelle für die Aufsichtsbehörde und den Betroffenen

Der DSBA ist verpflichtet mit der Aufsichtsbehörde gem Art 39 Abs1 lit d und e DSGVO zu kooperieren und weil er auch als Anlaufstelle für diese gilt, müssen laut Art 37 Abs 7 DSGVO, Name und Kontaktdaten des DSBA bekanntgegeben werden. Durch dieses Prozedere wird garantiert, dass der DSBA alle Schriftstücke und Ansuchen von der Aufsichtsbehörde direkt bekommt und daraufhin alle Anfragen zeitgerecht beantworten kann.

Der DSBA ist gem Art 39 Abs 1 lit e DSGVO berechtigt, sich direkt an die Aufsichtsbehörde zu wenden, wenn es Problemstellungen gibt, die unklar sind, nicht von Relevanz ist die Tatsache, ob ein Konsultationsverfahren nach Art 36 DSGVO angestrebt wurde oder nicht. Bei solchen Ansuchen muss der DSBA die Interessen des Verantwortlichen berücksichtigen und sollte das Bekanntgeben von Rechtsverletzungen umgehen, nur um sie intern kompensieren zu können.

Der DSBA ist nicht nur die Anlaufstelle für die Aufsichtsbehörde, sondern laut Art 38 Abs 4 DSGVO auch für den Betroffenen. Der DSBA muss die betroffenen Personen über ihre Rechte nach der DSGVO beraten und sie können sich jederzeit über die Verarbeitung ihrer Daten informieren. Auch bei dieser Tätigkeit sind die Kontaktdaten des DSBA gem Art 37 Abs 7 DSGVO zu veröffentlichen.

[104] Vgl Art-29-Datenschutzgruppe, Stellungnahme 12/2014, WP 243 rev.01, 20f.

D. Haftung

Wie schon des Öfteren in dieser Arbeit erörtert wurde, muss der DSBA auf das Einhalten der datenschutzrechtlichen Bestimmungen hinwirken und den Verantwortlichen bzw dessen Beschäftigte fachkundig beraten. Er ist ein Beratungs- und Kontrollorgan. Diese genannten Tätigkeiten sind aber sehr fehlerträchtig und risikobehaftet und dadurch können potentielle Schäden zB durch:

- falsche Empfehlungen,
- falsche Hinweise gegenüber dem Verantwortlichen über datenschutzrechtliche Schritte,
- Unkenntnis der Aufsichtspraxis,
- keine Handlung bei verpflichtenden Kontrollen,
- nicht ausreichende Schulungen.
- Missachtung der Verschwiegenheitspflichten entstehen.[105]

Die Frage, die sich stellt, ist, ob der DSBA direkt sanktioniert werden kann, wenn er seine Aufgaben gem Art 39 DSGVO nicht wahrnimmt. Die Verletzung des Art 39 DSGVO wird gem Art 83 Abs 4 lit a DSGVO mit einer Geldstrafe bestraft. Dies gilt aber nur, sofern es die Verpflichtungen des Verantwortlichen oder Auftragsverarbeiters betrifft. Somit kann nicht dem DSBA die Sanktion auferlegt werden, sondern dem Unternehmen bleibt die Verantwortung, dass alle datenschutzrechtlichen Vorgaben eingehalten werden.[106] Dem Unternehmen bleibt also nur die Möglichkeit zu regressieren, was aber abhängig von der Stellung des DSBA ist. Dem internen DSBA kommen die Haftungsprivilegien des DHG zugute, weil er zum Unternehmen in einem Dienstverhältnis steht. Für den externen DSBA gelten die arbeitsrechtlichen Haftungsprivilegien nicht und er haftet in vollen Umfang, außer es wurde etwas anderes vereinbart.[107]

Die letzte offene Frage ist, ob der DSBA auch eine Verantwortlichkeit gegenüber der betroffenen Person hat bzw schadenersatzpflichtig wird. Die vertragliche Haftung wird

[105] Vgl *Datenschutzbeauftragte*, Haftung des Datenschutzbeauftragten abrufbar unter: https://www.datenschutzbeauftragter.co.at/2011/03/haftung-des-datenschutzbeauftragten/ (25.11.2018).
[106] Vgl *König* in: *Knyrim*, Der Datenschutzbeauftragte, 240f; Vgl Art 83 Abs 4 lit 1 DSGVO.
[107] Vgl *Datenschutzbeauftragte*, Haftung des Datenschutzbeauftragten abrufbar unter: https://www.datenschutzbeauftragter.co.at/2011/03/haftung-des-datenschutzbeauftragten/ (25.11.2018).

ausgeschlossen, weil keine Beziehung zum Verletzten besteht. Denkbar wäre jedoch eine deliktische Haftung, wenn zB der DSBA gegen seine Verschwiegenheitspflicht verstoßen würde.[108]

[108] Vgl *Datenschutzbeauftragter* INFO, Die persönliche Haftung des internen betrieblichen Datenschutzbeauftragten abrufbar unter: https://www.datenschutzbeauftragter-info.de/die-persoenliche-haftung-des-internen-betrieblichen-datenschutzbeauftragten/ (25.11.2018).

IV. Resümee

Zusammenfassend kann festgestellt werden, dass der DSBA durch die neue DSGVO ein neues Rollenbild bekommen und an Wichtigkeit gewonnen hat. Einrichtungen, welche einen DSBA bestellen müssen, und jene, die es freiwillig tun, werden durch diesen eine große Unterstützung bekommen.

Die Verantwortung, die datenschutzrechtlichen Vorgaben einzuhalten, werden der Verantwortliche und der Auftragsverarbeiter trotzdem nicht an den DSBA abgeben können. Denn schlussendlich haften sie selbst für Verletzungen des Art 39 DSGVO und auf den DSBA kann man nur eingeschränkt zurückgreifen. Daher sollte der DSBA nicht als jener angesehen werden, der alleine zur Verantwortung gezogen wird, sondern er sollte als Berater und Kontrollorgan verstanden werden, der das Unternehmen beim Bewältigen dieser Verordnung hilft. Man sollte somit bei der Auswahl des DSBA sehr vorsichtig sein und sich absichern, dass er das erforderliche Fachwissen und die berufliche Qualifikation hat und man sollte ihm die nötigen Ressourcen für die effiziente Erfüllung seiner Aufgaben zur Verfügung stellen.

Auch sollte bedacht werden, dass durch die erfolgreiche Zusammenarbeit mit dem DSBA das Datenschutzlevel der Einrichtung steigt und auf diese Weise die Wahrscheinlichkeit, dass von der Aufsichtsbehörde Sanktionen zu erwarten sind oder von einem Betroffenen auf Schadenersatz geklagt wird, deutlich sinkt.

V. Literatur- und Materialienverzeichnis

1&1 Guide, Datenschutz-Grundverordnung (DSGVO). In: https://www.1und1.at/digitalguide/websites/online-recht/datenschutz-grundverordnung-regeln-fuer-unternehmen/ (02.07.2018).

Art-29- Datenschutzgruppe, Leitlinien in Bezug auf den Datenschutzbeauftragten vom 05.034.2017, WP 243. In: https://www.dsb.gv.at/documents/22758/112500/Leitlinien_in_Bezug_auf_Datenschutzbeauftragte.pdf/d241f0fd-6908-44fd-a12a-0f861e7a1dfb (25.11.2018)

Bergauer, Personenbezogene Daten. Begriff und Kategorien, in Knyrim (Hrsg), Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU, Wien 2016, 43 – 63.

Dataprotect, Datenschutz-Folgenabschätzung (DSFA). In: https://www.dataprotect.at/leistungen/dsfa/ (21.11.2018).

Datenschutzbeauftragte, Haftung des Datenschutzbeauftragten. In: https://www.datenschutzbeauftragter.co.at/2011/03/haftung-des-datenschutzbeauftragten/ (25.11.2018).

Datenschutzbeauftragter INFO, Die persönliche Haftung des internen betrieblichen Datenschutzbeauftragten. In: https://www.datenschutzbeauftragter-info.de/die-persoenliche-haftung-des-internen-betrieblichen-datenschutzbeauftragten/ (25.11.2018).

Dorda, "BLACK LIST" DER DATENSCHUTZBEHÖRDE ERLASSEN. In: http://www.dorda.at/publications/black-list-der-datenschutzbeh%C3%B6rde-erlassen (21.11.2018).

DSK, Kurzpapier Nr. 5 Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO. In: https://www.datenschutzzentrum.de/uploads/dsgvo/kurzpapiere/DSK_KPNr_5_Datenschutz-Folgenabschaetzung.pdf (21.11.2018).

Fercher/Riedl, DSGVO: Entstehungsgeschichte und Problemstellungen aus österreichischer Sicht, in Knyrim (Hrsg), Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU, Wien 2016, 7-31.

Flendrovsky: Die Aufsichtsbehörden, in Knyrim (Hrsg), Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU, Wien 2016, 281-290.

Fritz in Jahnel, Der Auftragsverarbeiter im Fokus der DS-GVO, Datenschutzrecht, 2017, Seite 11– 34. In: https://rdb.manz.at/document/rdb.tso.LIjbdatsr201702?execution=e4s4&highlight=der+auftragsverarbeiter (25.11.2018).

Geuer/Reinisch, Abgrenzungsfragen zur Zusammenarbeit der verschiedenen Akteure der Datenschutz-Grundverordnung, jusIT 2018, 98 – 105.

Giegerich, Europäische Vorreiterrolle im Datenschutzrecht: Neue Entwicklungen in der Gesetzgebung, Rechtsprechung und internationaler Praxis der EU, ZEuS 3/2016, 301 – 343.

Hladjk, Sachlicher und räumlicher Anwendungsbereich der DSGVO, in Knyrim (Hrsg), Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU, Wien 2016, 39 – 41.

Horn, Die neue Rolle des Datenschutzbeauftragten nach der DS-GVO, jusIT 2016/91, 195 – 202.

Kastelitz, Grundsätze und Rechtmäßigkeit der Verarbeitung personenbezogener Daten (Art 5 – 11 DSGVO), in Knyrim (Hrsg), Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU, Wien 2016, 99 – 114.

Knyrim, Die neuen Pflichten nach der EU-Datenschutz-Grundverordnung im Überblick (Teil V), Dako 2016/6, 11 – 13.

König, Der Datenschutzbeauftragte - Die interne Beratungs- und Kontrollfunktion, in Knyrim (Hrsg), Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU, Wien 2016, 231– 242.

König, Der Datenschutzbeauftragte im Unternehmen, ecolex 2018/6, 489 – 495. In: https://rdb.manz.at/document/rdb.tso.Llecolex20180603?execution=e4s3&highlight=der+Datenschutzbeauftragte (25.11.2018).

Selk, Verzeichnis von Verarbeitungstätigkeiten (Art 30): Wer muss es haben, wie hat es auszusehen, in Knyrim (Hrsg), Datenschutz-Grundverordnung. Das neue Datenschutzrecht in Österreich und der EU, Wien 2016, 181 – 198.

Spitz, Daten - das Öl des 21. Jahrhunderts? Nachhaltigkeit im digitalen Zeitalter, Hamburg 2017, 1– 248.

WKO, EU-Datenschutz-Grundverordnung (DSGVO). In: https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html (02.07.2018).