



Rollenbild der österreichischen betrieblichen und behördlichen Datenschutzbeauftragten

(VO [EU] 2016/679)

Version: 1.0
Stand: Oktober 2017

Vorwort des Vereinsvorstands

Liebe Leserin, lieber Leser,

der Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter – [Privacyofficers.at](https://www.privacyofficers.at) freut sich, das Rollenbild der österreichischen betrieblichen und behördlichen Datenschutzbeauftragten zur Verfügung stellen zu können. In der vorliegenden Version wurde das österreichische Datenschutz-Anpassungsgesetz 2018 entsprechend berücksichtigt.

Das vorliegende Werk beschäftigt sich mit den Themen der Benennung des/der Datenschutzbeauftragten (zB: „Wer muss/wer kann einen bestellen?“, „Welche Voraussetzungen in fachlicher, sozialer und sonstiger Hinsicht muss ein/e Datenschutzbeauftragte/r erfüllen?“), die Stellung des/der Datenschutzbeauftragten bei der Ausübung seiner/ihrer Funktion, wo/wie der/die Datenschutzbeauftragte organisatorisch positioniert werden sollte, Abgrenzung der Aufgaben des/der Datenschutzbeauftragten zu anderen Positionen in der Organisation, die arbeitsrechtliche Stellung des/der Datenschutzbeauftragten und natürlich auch die Aufgaben des/der Datenschutzbeauftragten.

Selbstverständlich werden auch die Datenschutzbeauftragten in Behörden und öffentlichen Stellen berücksichtigt.

Abschließend haben wir eine Mustervorlage für die Bestellung einer Person zum/zur Datenschutzbeauftragten beigefügt.

Das vorliegende Werk ist nicht statisch anzusehen, sondern als lebendes Werk, welches immer wieder einer Revision unterzogen werden wird. Auch stellt das vorliegende Rollenbild keinen Anspruch darauf, auf alle Fragen im Zusammenhang mit dem/der Datenschutzbeauftragten eine Lösung anzubieten. Unser Ziel war es, in kompakter und übersichtlicher Form auf die wichtigsten und praxisrelevantesten Punkte einzugehen und diese auszuführen.

Wir hoffen, dass das vorliegende Rollenbild den Verantwortlichen und Auftragsverarbeitern Unterstützung bei den Fragen, ob und wie ein/e Datenschutzbeauftragte/r zu bestellen ist, welche Voraussetzungen diese/r erfüllen muss, was seine/ihre Aufgaben sind, wie er/sie in die Organisation einzubinden ist bzw. eingebunden werden kann, etc.

Anregungen und konstruktive Kritik nehmen wir gerne unter office@privacyofficers.at entgegen, aktuelle Datenschutz-News finden Sie auf unserer Homepage: <https://www.privacyofficers.at/>.

Die Ausarbeitung des Rollenbildes wäre ohne den Einsatz unseres Arbeitskreises nicht möglich gewesen. Wir danken daher ganz besonders den Mitgliedern des Arbeitskreises „Rollenbild Datenschutzbeauftragte Österreich“ unter der Leitung von Dr. Natalie Ségur-Carbanac für die tatkräftige Mitarbeit und Erstellung dieses Rollenbilds.

Der Vereinsvorstand

Disclaimer: Sämtliche Inhalte wurden mit größtmöglicher Sorgfalt zusammengestellt, erfolgen jedoch ohne Gewähr. Sie stellen keine Beratungsleistung welcher Art auch immer dar und können eine entsprechende Beratung nicht ersetzen. Insbesondere deswegen wird keine Haftung hinsichtlich Richtigkeit, Vollständigkeit und Aktualität der Informationen (einschließlich des Verweises auf andere Quellen) übernommen. Der Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter Privacyofficers.at und die Verfasser schließen jegliche Haftung aus, sei es aus Vertrag, Delikt (inklusive Fahrlässigkeit) und / oder jeder anderen Rechtsgrundlage, für Verluste

oder Schäden, einschließlich entgangenen Gewinns oder sonstiger direkter oder indirekter Folgeschäden, welche durch den Gebrauch oder das Vertrauen in die in dieser Unterlage zur Verfügung gestellten Informationen oder einer etwaigen Nichtberücksichtigung bestimmter Informationen entstehen.



Dieses Werk ist lizenziert unter einer Creative Commons Namensnennung - Nicht-kommerziell - Weitergabe unter gleichen Bedingungen 4.0 International Lizenz: <https://creativecommons.org/licenses/by-nc-sa/4.0/deed.de>

Inhaltsverzeichnis

Inhaltsverzeichnis	4
Einleitung	5
1 Benennung des/der Datenschutzbeauftragten	5
1.1 Verarbeitung durch eine Behörde oder öffentliche Stelle	5
1.2 Wer kann zum/zur Datenschutzbeauftragten bestellt werden.....	7
1.3 Konstellation Verantwortlicher/Auftragsverarbeiter und Unternehmensgruppen:	8
1.4 Wie erfolgt die Bestellung des/der Datenschutzbeauftragten.....	10
1.5 Einbindung des/der Datenschutzbeauftragten in die Unternehmensorganisation	10
2 Stellung des/der Datenschutzbeauftragten	11
2.1 Unabhängigkeit und Weisungsfreiheit	11
2.2 Weisungsfreiheit	11
3 Organisatorische Positionierung des/der Datenschutzbeauftragte/n und potentielle Interessenskonflikte	12
3.1 Notwendige Ressourcenausstattung des/der Datenschutzbeauftragten	14
3.2 Verantwortung des/der Datenschutzbeauftragten.....	15
4 Abgrenzung der Aufgaben des/der Datenschutzbeauftragten zu anderen Positionen in der Organisation	16
5 Arbeitsrechtliche Stellung des/der Datenschutzbeauftragten	16
6 Aufgaben des/der Datenschutzbeauftragten	17
6.1 Kontaktaufgaben	17
6.2 Beratungs-, Überwachungs-, und Schulungsfunktionen	17
7 Datenschutzbeauftragte in Behörden und öffentlichen Stellen	19
Mustervorlage für die Bestellung einer Person zum/zur Datenschutzbeauftragten gemäß Artikel 37 DSGVO iVm § 5 DSG	A

Rollenbild der österreichischen betrieblichen und behördlichen Datenschutzbeauftragten

Einleitung

Mit der am 25. Mai 2018 in Geltung tretenden Datenschutz-Grundverordnung (EU 2016/679) kommen auf alle, die personenbezogene Daten verarbeiten, zahlreiche neue Herausforderungen zu. Eine der Schlüsselfiguren für eine erfolgreiche Durchsetzung des Datenschutzrechts ist der/die Datenschutzbeauftragte. In Österreich wird es dann neu die Funktion des/der Datenschutzbeauftragten geben, den manche Unternehmen verpflichtend benennen müssen. Der Verein Privacyofficers.at versteht sich als Interessensverband der österreichischen betrieblichen und behördlichen Datenschutzbeauftragten mit dem Ziel, dieser neuen Berufsgruppe bei der Etablierung und Durchführung ihren Aufgaben und Funktionen entsprechende Unterstützung anzubieten.

Im gegenständlichen Rollenbild wollen wir die Regelungen der DSGVO zur Funktion des/der Datenschutzbeauftragten für Österreich beschreiben und so zu einer einheitlichen Etablierung des/der Datenschutzbeauftragten in Österreich beitragen. Die in diesem Dokument formulierten Rechtsansichten sind unpräjudiziell von zukünftigen höchstgerichtlichen Entscheidungen, vielmehr sollen sie helfen, das Berufsbild des/der Datenschutzbeauftragten sowohl in der Praxis als auch in den entsprechenden Rechtsgrundlagen zu festigen. Das Rollenbild versteht sich als lebendes Dokument, das bei Bedarf von den Autoren verändert/angepasst werden wird.

1 Benennung des/der Datenschutzbeauftragten

Die DSGVO sieht in Art 37 grundsätzlich für drei Fälle die verpflichtende Bestellung eines/r Datenschutzbeauftragten vor. Sowohl der/die Verantwortliche als auch der/die Auftragsverarbeiter/in haben eine/n Datenschutzbeauftragte/n zu bestellen, wenn

- a) 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/der Verantwortlichen oder des/der Auftragsverarbeiters/in in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder
- c) die Kerntätigkeit des/der Verantwortlichen oder des/der Auftragsverarbeiters/in in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Artikel 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art 10 DSGVO besteht.

1.1 Verarbeitung durch eine Behörde oder öffentliche Stelle

Art 37 Abs 1 lit a DSGVO sieht vor, dass „Behörden und öffentliche Stellen“ (mit Ausnahme der Gerichte bei den justiziellen Tätigkeiten) Datenschutzbeauftragte zu bestellen haben.

Dabei richtet sich das Verständnis dessen, was unter „Behörden und öffentlichen Stellen“ zu verstehen ist, nach dem nationalen Recht:

Als „Behörden“ gelten in Österreich rechtlich geregelte Einrichtungen, die zur Durchführung bestimmter öffentlicher Aufgaben berufen sind, dies unabhängig von der Rechtsform. Insofern entspricht dieser Begriff weitgehend dem bereits bestehenden Begriff des „Auftraggebers des öffentlichen Bereichs“ nach § 5 Abs 2 DSG 2000, der nicht unterscheidet, ob der Auftraggeber in Form des öffentlichen oder des privaten Rechts eingerichtet ist, solange die Datenverwendung „in Vollziehung der Gesetze“ erfolgt.

Als „öffentliche Stellen“ gelten alle Stellen nach § 4 IWG. Der Begriff der „öffentlichen Stelle“ entspricht damit dem Begriff der „öffentlichen Stelle“ in Art 2 der PSI-Richtlinie 2003/98/EG,¹ die mit dem IWG in nationales Recht umgesetzt worden ist. Inhaltlich ist dieser Begriff, ohne darauf explizit Bezug zu nehmen, dem Begriff des „öffentlichen Auftraggebers“ nach § 3 Abs 1 BVergG 2006 gleichzusetzen. Zusammenfassend kann also gesagt werden, dass neben Behörden und beliehenen Unternehmen auch Unternehmen, die dem Vergaberecht unterliegen, verpflichtet sind, eine/n Datenschutzbeauftragte/n zu bestellen.

Über diese Verpflichtung hinaus empfiehlt die Art-29-Datenschutzgruppe,² dass auch Unternehmen, die „öffentliche Aufgaben“ erfüllen, d.h. Leistungen des täglichen Bedarfs für die Allgemeinheit bereitstellen, wie beispielsweise Wasser- oder Energieversorgung, Straßeninfrastruktur, etc. ebenfalls eine/n Datenschutzbeauftragte/n bestellen sollen. Dies deshalb, da die betroffene Person diesen Unternehmen gegenüber in einer vergleichbaren Situation sein wird wie gegenüber einer „Behörde oder öffentlichen Stelle“. Anzumerken ist zudem, dass die Datenschutzbehörde in ihrem Leitfaden zur DSGVO³ u.a. auf die Definition des Verantwortlichen des öffentlichen Bereichs in § 26 Abs 1 DSG verweist.

1.1. Kerntätigkeit

Für die Pflicht zur Bestellung eines/r Datenschutzbeauftragten - abseits von Behörden und öffentlichen Stellen - stellt Art 37 Abs 1 lit b und c DSGVO auf den Begriff der „Kerntätigkeit“ ab. Zu diesem damit wesentlichen Abgrenzungskriterium gibt es jedoch keine Definition in der DSGVO. Da der Begriff außerhalb der DSGVO nur in der Richtlinie 2013/36/EU⁴ und der zugehörigen Verordnung 1151/2014⁵ verwendet - und auch dort nicht definiert - wird, sowie bis dato jegliche Rechtsprechung zur autonomen Auslegung durch den EuGH fehlt, sind entsprechende Guidelines und Auslegungshilfen gerade in diesem Bereich von großer Bedeutung.

Lediglich in ErwGr 97, der zur Auslegung herangezogen werden kann, wird die Kerntätigkeit als Haupttätigkeit des Verantwortlichen im privaten Sektor umschrieben. Damit werden bloße Nebentätigkeiten ausgeschlossen. Begleitende - wenn auch notwendige - administrative Kontroll- oder sonstige Wartungsmaßnahmen sind daher nicht als Kerntätigkeit zu betrachten (z.B. begleitende Videoüberwachung im Lager einer Produktionsstätte). Dies gilt wohl generell für den Bereich der eigenen Mitarbeiterdatenverwaltung, sofern es sich bei dem Verantwortlichen nicht um einen Personalvermittler handelt. Ungeklärt bleibt aber, auf welchen Tätigkeitsschwerpunkt bzw. welche Parameter (z.B. Umsatz, Größe der Abteilung, Investitionen etc.) abzustellen ist, wenn ein Verantwortlicher in mehreren Wirtschaftsbereichen schwerpunktmäßig tätig ist.

¹ Auf diese weist auch die Art-29-Datenschutzgruppe im WP 243 rev.01, 6 (FN 11) hin.

² http://ec.europa.eu/newsroom/document.cfm?doc_id=43823 in Punkt 2 der Anlage zu WP 243 3 (Stand Juli 2017) 31 f.

⁴ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:176:0338:0436:DE:PDF>

⁵ <http://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32014R1151&from=DE>

Die Art-29-Datenschutzgruppe bietet in ihrem Working Paper 243 darüber hinaus weitere Abgrenzungskriterien, die jedoch in Summe zu einer weiten Auslegung der Anwendbarkeit führen: Kerntätigkeit sollen all jene Tätigkeiten eines Verantwortlichen sein, die "einen untrennbaren Teil" der Haupttätigkeit des Unternehmens zur Verfolgung der Unternehmensziele darstellen. Wiederum als Negativabgrenzung folgt auch die Art-29-Datenschutzgruppe der Ansicht, dass eine Verarbeitung von Mitarbeiterdaten – die bei jedem größeren Unternehmen gezwungenermaßen umfangreich und regelmäßig erfolgt – lediglich eine untergeordnete Hilfstätigkeit darstellt. Hinsichtlich des Erfordernisses der Überwachung von Personen zeigt sie allerdings auch auf, dass dies neben der klassischen Videoüberwachung insbesondere Online Tracking und Profiling für zielgruppenorientierte Werbung und E-Mail Retargeting sei.

Zusammengefasst kann die Kerntätigkeit als Schlüsseltätigkeit zur Erreichung der vom Verantwortlichen gesetzten Unternehmensschwerpunkte bzw. -ziele definiert werden. Dabei muss die Datenverarbeitung selbst nicht die Kerntätigkeit darstellen. Letztendlich läuft es auf eine Abgrenzung zwischen einer bloß beiläufigen Verarbeitung und einer solchen, die einen untrennbaren Teil zur Zielerreichung darstellt.

1.2 Wer kann zum/zur Datenschutzbeauftragten bestellt werden

Gemäß Art 27 Absatz 5 DSGVO wird der/die Datenschutzbeauftragte auf Grundlage seiner/ihrer beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er/sie auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Art 39 DSGVO genannten Aufgaben.

Der/die Datenschutzbeauftragte muss über ausreichendes Fachwissen und eine hinreichende berufliche Qualifikation im Datenschutzrecht und in der Datenschutzpraxis verfügen. Diese Anforderungen können nur von Personen erfüllt werden, die Kenntnisse in den Bereichen Recht, Organisation und Technik haben. Daneben sind Social Skills ein wesentlicher Faktor für die Ausübung der Position des/der Datenschutzbeauftragten. Auch Berufserfahrung in einem der oben genannten Bereiche (Recht, Organisation, Technik) sollte der/die Datenschutzbeauftragte vorweisen können. Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem/der Verantwortlichen oder dem/der Auftragsverarbeiter/in verarbeiteten personenbezogenen Daten richten.

Im Bereich Recht sollte ein/e Datenschutzbeauftragte/r zumindest folgende Rechtsmaterien souverän abdecken können:

- Grundrechte, insbesondere Art 8 EMRK und Art 7 und 8 GRC
- EU-Datenschutz-Grundverordnung
- Datenschutzgesetz 2018
- Geplante E-Privacy-Verordnung
- Telekommunikationsgesetz 2003, insbesondere §§ 92 bis 107 TKG 2003
- Rechtsgrundlagen für Datenverarbeitungen, Aufbewahrungs- und Lösungsfristen
- Besondere Rechtsvorschriften hinsichtlich Datenschutz (beispielsweise Gesundheitstelematikgesetz, Gesundheitstelematikverordnung)

- Arbeitsverfassungsrecht, insbesondere §§ 91, 96, 96a und 97 ArbVG
- Vertragsrecht

Im Bereich Technik sollte der/die Datenschutzbeauftragte zumindest über Basiswissen in folgenden Themenfeldern verfügen:

- Funktionsweise moderner Informations- und Kommunikationstechnologien (Internet, E-Mail, Over-The-Top-Kommunikationsdienste, Cloud-Dienste)
- Sicherheitsrisiken, insbesondere Social Engineering (z.B. Phishing) und Malware (z.B. Viren, Trojaner, Spyware, Ransomware)
- Informationssicherheits-Managementsysteme (z.B. ISO/IEC 27001:2013) und Informationssicherheitsmaßnahmen

Im Bereich Organisation sollte der/die Datenschutzbeauftragte mit folgenden Disziplinen der Management-Lehre vertraut sein:

- Audittechnik
- Betriebliche Weiterbildung bzw. Bewusstseinsbildung
- Projekt- und Prozessmanagement

Der/die Datenschutzbeauftragte sollte außerdem einen guten Überblick über seine/ihre Organisation haben und über umfangreiches Wissen hinsichtlich des Kerngeschäfts und der Kernprozesse verfügen. Damit wird es für den/die Datenschutzbeauftragte/n erheblich einfacher, Zugang zu den relevanten Datenverarbeitungsvorgängen in seiner/ihrer Organisation zu bekommen und frühzeitig bei diesbezüglichen Fragen zu beraten.

Die eben angeführten Anforderungen an zukünftige Datenschutzbeauftragte sind sehr hoch. Der/die Datenschutzbeauftragte muss umfangreiches Wissen in komplexen Gebieten haben. Für fast jede/n Datenschutzbeauftragte/n wird in den nächsten Jahren der regelmäßige Besuch von Fortbildungen unabdingbar sein. Juristen und Juristinnen werden Aufholbedarf in den Bereichen Technik und Organisation haben. Datenschutzbeauftragte mit einem anderen Ausbildungshintergrund werden ihr (datenschutz-)rechtliches Wissen ausbauen müssen. Die dazu notwendigen Ressourcen müssen die Organisationen dem/der Datenschutzbeauftragten zur Verfügung stellen.

Der/die Datenschutzbeauftragte muss wichtige "Übersetzungsarbeit" leisten. Denn er/sie wird mit technischen, juristischen und organisatorischen Problemstellungen konfrontiert sein. Deswegen wird an dieser Stelle die klare Empfehlung ausgesprochen, dass Unternehmen dem/der Datenschutzbeauftragten auch Fortbildungen im Bereich Social Skills (Kommunikations- und Konfliktlösungsfähigkeit sowie Moderations- und Mediationstechniken) ermöglichen.

Ganz allgemein dürfen derartige Fortbildungen, die vom Unternehmen finanziert bzw. ermöglicht werden nicht – wie in der Praxis üblich – an jegliche Bindungsverpflichtungen oder Rückzahlungsverpflichtungen seitens des/der Datenschutzbeauftragten gebunden werden. Dies widerspricht der zu gewährleistenden Unabhängigkeit und Weisungsfreiheit.

1.3 Konstellation Verantwortlicher/Auftragsverarbeiter und Unternehmensgruppen:

Sollte eine Datenverarbeitung im Auftragsverhältnis erfolgen, so müssen sich Verantwortliche/r und Auftragsverarbeiter/r anhand der vorgegebenen Kriterien überlegen, ob jeweils die Bestellung eines/r Datenschutzbeauftragten erforderlich ist oder ob auch nur eine/r von beiden Beteiligten dazu verpflichtet ist. Es empfiehlt sich, darüber vertraglich Klarheit zu schaffen. Dabei wird insbesondere darauf Bedacht genommen werden müssen, wo die Daten tatsächlich und wie diese verarbeitet werden, sowie wer das tatsächliche Risiko der Datenverarbeitung trägt.

Gemäß Art 37 Abs 2 DSGVO darf eine Unternehmensgruppe eine/n gemeinsamen Datenschutzbeauftragte/n ernennen, sofern diese/r von jeder Niederlassung leicht erreicht werden kann. Eine Unternehmensgruppe besteht aus einem herrschenden Unternehmen und von diesem unabhängigen Unternehmen, wobei das herrschende Unternehmen die Befugnis hat, Datenschutzvorschriften umsetzen zu lassen (vgl. Art 4 Z 19 DSGVO, ErwGr 37). In welchen Fällen eine beherrschende Stellung eines Unternehmens vorliegt, ist eine Frage des Gesellschaftsrecht und damit der jeweiligen nationalen Rechtsordnung überlassen, wobei für Österreich die entsprechenden gesellschaftsrechtlichen Bestimmungen inklusive Judikatur, insbesondere §244 UGB und § 15 AktG relevant sind.

Ziel gemeinsamer Datenschutzbeauftragter ist ebenso die leichte Möglichkeit, mit dieser/diesem Kontakt aufnehmen und dessen Beratung in Anspruch nehmen zu können. Kriterien für die angesprochene Erreichbarkeit sind daher physische und mediale Zugänglichkeit sowie das Fehlen von Sprachbarrieren. In internationalen Unternehmensgruppen wird aufgrund dieses letzten Merkmals eine vollkommene Zentralisierung der Aufgaben schwer möglich sein, weil insbesondere die Ansprechmöglichkeit für Kunden in allen Sprachen jener Länder fehlt, in welchen die Unternehmensgruppe ansässig ist, sowie die Kommunikation des/der Datenschutzbeauftragten mit der Behörde in der Amtssprache des jeweiligen Landes kaum möglich sein wird.

Auch Behörden und öffentliche Stellen können eine/n gemeinsame/n Datenschutzbeauftragte/n bestellen. Kriterium ist hier, dass die Größe und Organisationsstruktur dieser Behörden bzw. öffentlichen Stellen zu berücksichtigen ist. Dies deutet darauf hin, dass insbesondere ein gleiches Portfolio an gesetzlich übertragenen Aufgaben diese gemeinsame Ernennung fördern soll, wie das etwa bei Gemeinden, Bezirkshauptmannschaften oder kleineren Bezirksgerichten der Fall ist.

Die Formulierung des Art 37 Abs 2 DSGVO deutet darauf hin, dass die geforderte Ernennung des/der Datenschutzbeauftragten gegenüber der Aufsichtsbehörde durch das herrschende Unternehmen der Unternehmensgruppe ausreicht.

Der/die Datenschutzbeauftragte kann entweder intern aus den Reihen der eigenen Mitarbeiter/innen bestellt werden (interne/r Datenschutzbeauftragte/r) oder es kann eine externe Person bzw. ein externes Unternehmen mit dieser Rolle betraut werden (externe/r Datenschutzbeauftragte/r). Sämtliche Personen dieses externen Unternehmens, das mit Aufgaben des/der Datenschutzbeauftragten betraut ist, müssen alle Erfordernisse der DSGVO erfüllen (z.B. darf für keine dieser Personen ein Interessenkonflikt mit anderen Aufgaben bestehen). Umgekehrt müssen all diese Personen im selben Ausmaß durch die DSGVO geschützt sein (z.B. keine Beendigung des Auftragsvertrags wegen der Tätigkeit als Datenschutzbeauftragte/r). Im Hinblick auf Rechtssicherheit und gute Organisation wird empfohlen, in solchen Teams von

Datenschutzbeauftragten, die aufgrund unterschiedlicher Fähigkeiten und Stärken effizienter zusammen arbeiten können, die Aufgaben im Team klar (z.B. vertraglich oder durch Richtlinien) zuzuteilen und eine Person als Hauptkontakt bzw. Zuständigen für jede Anfrage zu definieren (Guidelines on Data Protection Officers, S 12). Der/die externe Datenschutzbeauftragte wird im Rahmen seiner/ihrer Tätigkeit selbst Zugriff auf personenbezogene Daten des jeweiligen Auftraggebers haben (vgl. Art. 38 Abs 2 DSGVO). Offen bleibt, ob dadurch zusätzlich ein eigenes Auftragsverarbeitungsverhältnis begründet wird – mit allen Konsequenzen (Abschluss eines Auftragsvertrages etc.). Dies würde sich wohl mit der Weisungsfreiheit und Unabhängigkeit des/der (externen) Datenschutzbeauftragten nicht vereinbaren lassen.

Auch ein/e gemeinsame/r Datenschutzbeauftragte/r von Verantwortlichen und Auftragsverarbeitern ist denkbar, wird aber dort in Interessenskonflikten seine Grenzen finden, wo die Beratungs- und Kontrolltätigkeit durch unterschiedliche Interessenslagen (z.B. in der Risikobewertung eines Vorhabens) erschwert oder unmöglich gemacht wird. Solche Konstellationen müssen daher im Einzelfall unter Berücksichtigung von potentiellen Interessenskonflikten entschieden werden.

1.4 Wie erfolgt die Bestellung des/der Datenschutzbeauftragten

Es empfiehlt sich in jeden Fall eine schriftliche Bestellung vorzunehmen. Eine Vorlage für eine Bestellung eines/r Datenschutzbeauftragten findet sich in Anlage 1 dieses Dokuments.

Die Kontaktdaten des/der Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen. Zur Veröffentlichung eignet sich am besten die Nennung von Kontaktdaten auf der Unternehmenswebseite bzw. für die Mitarbeiter auf der Intranetseite. Es ist hier nicht unbedingt notwendig, persönliche Telefonnummern oder E-Mail-Adressen des/der Datenschutzbeauftragten anzugeben. Es ist sicherzustellen, dass Betroffene über die angegebenen Kontaktdaten (allgemeine Telefonnummer, allgemeine E-Mail-Adresse des/der Datenschutzbeauftragten, wie z.B. datenschutzbeauftragte/r@xvzat) einfach den/die Datenschutzbeauftragte erreichen und auch in Dialog treten können.

Die Person des/der Datenschutzbeauftragten ist der Datenschutzbehörde gegenüber zu nennen. Hier benötigt die österreichische Datenschutzbehörde nach Rücksprache eine kurze Information über den Namen des Unternehmens und den Namen der bestellten Person, wobei eine formlose Benachrichtigung per E-Mail an die Datenschutzbehörde (dsb@dsb.gv.at) genügt.

1.5 Einbindung des/der Datenschutzbeauftragten in die Unternehmensorganisation

Die DSGVO lässt sowohl die Bestellung eines/r internen Dienstnehmers/in als auch eines/r externen Dienstleiters/in (Art 37 Abs 6 DSGVO). In der Praxis sollte jedenfalls sichergestellt sein, dass der/die Datenschutzbeauftragte möglichst effektiv seiner/ihrer Aufgabe nachkommen kann. Es kann durchaus sinnvoll sein, die Aufgaben des/der Datenschutzbeauftragten auf mehr als eine Person aufzuteilen. Zu denken wäre hierbei etwa an die Bestellung eines/r externen Datenschutzbeauftragten und gleichzeitige Nominierung einer internen Ansprechperson, die dann gemeinsam das Thema Datenschutz im Unternehmen adressieren und wahrnehmen. Die Kombination aus internen und externen Experten kann durchaus auch positive Nebeneffekte, etwa durch die Kombination von tieferer Kenntnis der Organisation von innen mit dem objektiven Einblick von außen, haben. Externe Dienstleister, die mehrere datenverarbeitende Verantwortliche

und/oder Auftragsverarbeiter/innen betreuen, können wiederum ihre Erfahrungen mit verschiedenen Branchen und Unternehmen in die Arbeit mit dem einzelnen Verantwortlichen einbringen. Auch ohne Einbindung von externen Beratern kann eine Aufteilung der Aufgaben sinnvoll aufgesetzt werden, indem z.B. ein Gremium von Experten aus verschiedenen Unternehmensbereichen aber auch mit verschiedenen Aufgaben im Unternehmen (Compliance, Informationssicherheit, Personalmanagement, Betriebsrat etc.) als Unterstützung für den/die Datenschutzbeauftragten gebildet wird.

2 Stellung des/der Datenschutzbeauftragten

Der/die Datenschutzbeauftragte ist eine Schlüsselfigur für eine erfolgreiche Umsetzung der Vorgaben der DSGVO in Europa. Insofern gesteht die DSGVO dem/der Datenschutzbeauftragten entsprechende Besonderheiten zu, wenn es um die Stellung in der Organisationsstruktur und in der Einbindung in die unternehmerischen Entscheidungsfindungen geht, die in irgendeiner Art und Weise mit dem Schutz personenbezogener Daten in Zusammenhang stehen. Der/die Datenschutzbeauftragte ist entsprechend frühzeitig einzubinden und die Organisation hat seine/ihre Unabhängigkeit und Weisungsfreiheit sicherzustellen (siehe dazu Art 39 DSGVO).

2.1 Unabhängigkeit und Weisungsfreiheit

Der/Die Datenschutzbeauftragte ist laut Art 38 Ziffer 3 DSGVO weisungsfrei bezüglich der Erfüllung seiner/ihrer Aufgaben und darf aus Gründen, die sich im Zusammenhang mit der Erfüllung seiner/ihrer Aufgaben stehen, nicht abberufen oder benachteiligt werden. Diese Privilegien sollen dafür sorgen, dass der/die Datenschutzbeauftragte seine/ihre Aufgaben ohne Beeinflussung durchführen kann. Es ist dabei unbedeutend, ob die Bestellung des/der Datenschutzbeauftragten freiwillig oder verpflichtend erfolgt. Für Unternehmen ergibt sich daraus die Notwendigkeit, eine/n mögliche/n externe/n oder interne/n Datenschutzbeauftragte/n genau zu prüfen, bevor diese/r mit der Aufgabe betraut wird. Um als Unternehmen trotz der Bindung an eine/n Datenschutzbeauftragte/n auf Änderungen des Unternehmensumfeldes reagieren zu können, empfiehlt es sich, die Bestellung des/der Datenschutzbeauftragten zeitlich zu befristen. Die bisherige Rechtsprechung in Ländern, in denen es bereits verpflichtende Datenschutzbeauftragte gibt, insbesondere Deutschland, verlangt dafür allerdings eine Mindestfrist, die es dem/der Datenschutzbeauftragten ermöglicht, seine/ihre Aufgaben sinnvoll wahrnehmen zu können. Für interne Datenschutzbeauftragte wird dabei ein Zeitraum von zwei bis fünf Jahren als ausreichend angesehen. Bei externen Datenschutzbeauftragten wird ein Erstvertrag mit einer Laufzeit von einem bis zwei Jahren und danach Verträge mit vier Jahren Laufzeit empfohlen. Eine kürzere Befristung im Sinne einer Probezeit wurde nicht anerkannt. Somit muss die Prüfung der Eignung bereits vor der Bestellung gründlich erfolgen.

2.2 Weisungsfreiheit

Arbeitsrechtliche Implikationen

Grundsätzlich besteht ein Weisungsrecht des/der Arbeitgebers/in gegenüber dem/der Arbeitnehmer/in. Das ist ein Kernelement von Arbeitsverhältnissen und die letzte Ebene im arbeitsrechtlichen Stufenbau.

Es dient u.a. der Konkretisierung von Arbeitsverhältnissen wie Arbeitszeit, Arbeitsort und den Inhalt der auszuführenden Tätigkeiten. Des weiteren zählen Regelungen zu Überstunden, Aufteilung der Arbeitszeit, Pausenregelungen, Urlaub, Betriebsferien, Qualität der Arbeit, Ordnungsverhalten (z.B. Rauchverbot oder Art der Kleidung) etc. dazu.

Der/die Arbeitnehmer/in kann die Befolgung einer Weisung verweigern, wenn diese gegen ein Gesetz verstößt oder er/sie in sonstiger Weise schikaniert wird. Bisher von Weisungen im österr. Arbeitsrecht ausgenommen sind Sicherheitsvertrauenspersonen, Betriebsrat, Vorstand und die Geschäftsführung.

Das Weisungsrecht in der Justiz ist im Gegenzug gesetzlich genau geregelt; Weisungen der Oberstaatsanwaltschaft und des Bundesministers für Justiz dürfen nur schriftlich und mit Begründung ergehen.

Datenschutzrechtliche Implikationen

Art 38 Abs 3 DSGVO regelt das Weisungsrecht gegenüber einem/r Datenschutzbeauftragten. Der/Die Verantwortliche muss sicherstellen, dass der/die Datenschutzbeauftragte bei der Erfüllung seiner/ihrer Aufgaben weisungsfrei bleibt. Der/die interne Datenschutzbeauftragte ist damit nur im Datenschutzbereich vom Weisungsrecht des Arbeitgebers freigestellt. Alle anderen Weisungen, welche nicht in diesem Zusammenhang (Arbeitszeit und –ort, Urlaub etc.) stehen, sind davon nicht umfasst

Die Art-29-Datenschutzgruppe erteilt keine allgemeine Empfehlung, wie die Weisungsfreiheit des/der Datenschutzbeauftragten grundsätzlich gehandhabt werden soll, sie gibt aber einige konkrete Hinweise.

Art 38 DSGVO gemeinsam mit ErwGr 97 gibt vor, dass diese Weisungsfreiheit bewusst nur für den Bereich des/der Datenschutzbeauftragten besteht.

Dies bedeutet, dass nur dort keine Weisungen erteilt werden dürfen, wo es um die Erfüllung der Aufgaben als Datenschutzbeauftragte/r geht. Insbesondere wird auf Seite 15 der Guidelines on Data Protection Officers der Art-29-Datenschutzgruppe hingewiesen, dass man dem/der Datenschutzbeauftragten nicht vorschreiben kann, wie er/sie eine Untersuchung in einem Beschwerdeverfahren anlegen soll, oder wie und wann er/sie die Aufsichtsbehörde kontaktieren soll. Dies liegt daher alleine in der Entscheidungsfreiheit des/der Datenschutzbeauftragten. Des Weiteren darf ein/e Datenschutzbeauftragte/r nicht angewiesen werden, wie datenschutzrechtliche Regeln zu interpretieren sind oder zu welcher Beurteilung er/sie gelangen soll.

Der Verantwortliche bleibt somit immer verantwortlich für die Compliance der Datenschutzgesetze und -verordnungen. Sind Entscheidungen des Verantwortlichen datenschutzrechtswidrig, so muss der/die Datenschutzbeauftragte Zugang zur höchsten Managementebene haben, um seine/ihre Meinung und Einschätzung zu erläutern.

3 Organisatorische Positionierung des/der Datenschutzbeauftragte/n und potentielle Interessenskonflikte

Der/die Datenschutzbeauftragte kann neben seinen/ihren eigenen Tätigkeiten auch andere Aufgaben übernehmen. Dabei ist darauf zu achten, dass diese Aufgaben nicht zu einem

Interessenkonflikt führen.⁶ Der/die Datenschutzbeauftragte soll unabhängig und weisungsfrei sein. Er/sie überwacht die Einhaltung der Datenschutzvorschriften im Unternehmen oder der Behörde. Stehen übertragene Aufgaben im Interessenskonflikt zur Tätigkeit als Datenschutzbeauftragte/r, widerspricht das seiner/ihrer unabhängigen Stellung. Es darf nicht dazu kommen, dass der/die Datenschutzbeauftragte sich selbst kontrollieren muss.

Bei Übertragung anderer Aufgaben ist auch darauf zu achten, dass dem/der Datenschutzbeauftragten genug Zeit zur Erfüllung seiner/ihrer Tätigkeit bleibt und er/sie somit über die ausreichenden Ressourcen zur sinnvollen Wahrnehmung seiner/ihrer Aufgaben verfügt.

- Interessenskonflikte können⁷ insbesondere in folgenden Fällen bestehen:
 - Leitung von Behörden und Unternehmen
 - Leitung IT
 - Leitung Personal
 - Leitung Recht
 - Leitung Marketing
 - Nachforschungsorgane wie Compliance Officer oder Interne Revision: Werden diese mit Durchführung konkreter Kontrollmaßnahmen beauftragt, kann das zu Interessenskonflikten führen. Um ihren Prüfaufgaben nachzukommen, haben Nachforschungsorgane Interesse an einem möglichst uneingeschränkten Zugang zu Daten und Datenverarbeitungen. Das ist etwa der Fall, wenn die Interne Revision im Rahmen ihrer Tätigkeit umfangreiche Auswertungen von personenbezogenen Daten oder Protokolldaten benötigt. Bei der Abwägung, ob bei Nachforschungsorganen ein Interessenkonflikt besteht, ist auch zu berücksichtigen, ob diese in ihrer Tätigkeit weisungsfrei sind oder nicht.
 - Beschäftigte, wenn sie Datenverarbeitungsprozesse bestimmen oder wesentlich beeinflussen können (z.B. in der IT oder im Personalwesen)
 - Organisationseinheiten mit besonders umfangreicher Verarbeitung von personenbezogenen Daten oder bei Verarbeitung besonderer Kategorien personenbezogener Daten gemäß Art. 9 DSGVO (z.B. Zuständigkeit für Big-Data-Anwendungen)
 - Betriebsrat: Beim Betriebsrat ist es strittig, ob ein Interessenkonflikt besteht. Hier muss genau abgewogen werden. Es besteht die Gefahr, dass nach arbeitsrechtlichen Vorgaben entschieden wird und dies zu einem Interessenskonflikt mit Datenschutz führt. Laut DSGVO ist der/die Datenschutzbeauftragte vom/von der Verantwortlichen oder Auftragsverarbeiter/in möglichst frühzeitig einzubeziehen. Im Falle des Betriebsrats ist nicht gewährleistet, dass dieser alle Informationen zum Thema Mitarbeiterdatenverarbeitung frühzeitig erhält. Zudem besteht die Rolle eines Betriebsrats darin, alle Arbeitnehmer/innen zu vertreten, der/die Datenschutzbeauftragte hat darüber hinaus die Interessen von Unternehmen und sonstigen Betroffenen wahrzunehmen.

⁶ Art 38 Abs 6 DSGVO

⁷ Wir zeigen potentielle Interessenskonflikte auf, die jeweils im Einzelfall zu prüfen und abzuwägen sind und dann je nach Ergebnis vorliegen oder nicht.

Darüber hinaus ist es sinnvoll zu dokumentieren, wo Interessenskonflikte bestehen. Auch sollte festgehalten werden, wie viel Zeit die Tätigkeit als Datenschutzbeauftragte/r in Anspruch nimmt. Diese Parameter sind bei der Besetzung der Stelle entsprechend zu berücksichtigen.

3.1 Notwendige Ressourcenausstattung des/der Datenschutzbeauftragten

Der/Die Verantwortliche und der/die Auftragsverarbeiter/in sind verpflichtet, die/den Datenschutzbeauftragte/n bei der Erfüllung der in Art 39 DSGVO aufgezählten Pflichten zu unterstützen, indem sie ihm/ihr die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und Zugang zu allen relevanten Informationen zur Verfügung stellen. Es ist daher in jedem Fall unzulässig, zur Vorbeugung vor unangenehmen Empfehlungen, die/den Datenschutzbeauftragte/n nicht oder nur selektiv in geplante Datenverwendungen einzuweihen. Gleichzeitig ist dies auch nicht praktikabel und würde die Position des/der Datenschutzbeauftragten gewissermaßen ad absurdum führen.

Ressourcen, die zur Verfügung gestellt werden müssen, umfassen auch Mitarbeiter/innen, Budget, Räumlichkeiten. Weder für die Mitarbeiter- bzw. Mitarbeiterinnenanzahl noch die Budgetgröße gibt es allgemeine Regelungen – es kommt hier im Einzelfall auf die Unternehmenstätigkeit und die Zahl und Komplexität der Fragestellungen in der Praxis an.

Folgender Anhaltspunkt kann aber für Großunternehmen herangezogen werden: Der deutsche Bundesbeauftragte für Datenschutz und Informationsfreiheit empfiehlt für öffentliche Stellen ab einer Zahl von 1.000 Beschäftigten die vollständige Freistellung einer Person. Für Klein- und Mittelunternehmen, Einzelunternehmer bzw. Start-Ups für Dienste der Informationsgesellschaft stellt diese Zahl kein Maß dar. Hier ist umgekehrt zu erwägen, den/die designierte/n Datenschutzbeauftragte/n, der/die nicht voll ausgelastet ist, mit nicht unvereinbaren weiteren Aufgaben auszustatten.

Neben den personellen Ressourcen sieht die Art-29-Datenschutzgruppe in den Guidelines on Data Protection Officers, S 13f, folgende Themen im Fokus:

- Aktive Unterstützung des/der Datenschutzbeauftragten durch die Führungskräfte der Organisation (z.B. des Vorstands)
- Unterstützung in Form eines Budgets und Infrastruktur (Büroräumlichkeiten bzw. Ausstattung)
- Kommunikation der Bestellung und der Kontaktdaten des/der Datenschutzbeauftragten an alle Arbeitnehmer, um dessen Existenz und Funktion bekannt zu machen
- Zugang zu anderen Unternehmensbereichen wie Human Resources, Recht, IT, Informationssicherheit etc., um dem/der Datenschutzbeauftragten die notwendige Unterstützung und Information zu geben
- Ständige Fortbildung, insb. was die Entwicklungen im Datenschutzbereich betrifft (z.B. via Seminare, Interessensgruppen, Workshops etc.)

Je komplexer bzw. sensibler die Datenverarbeitung einer Organisation ist, desto mehr Ressourcen müssen der/dem Datenschutzbeauftragten zur Verfügung gestellt werden. Die Datenschutzfunktion muss in Relation zur Datenverarbeitung und dem damit einhergehenden Risiko für die Betroffenen effizient und ausreichend ausgestattet sein.

Hinsichtlich der Ressourcen zur Erhaltung des Fachwissens gibt es ebenso keine detaillierten Vorgaben – auch hier hängt letztlich viel von der Unternehmenspraxis ab. Dies wird wohl nur für interne, d.h. aus dem Unternehmen oder der Unternehmensgruppe selbst bestellte Datenschutzbeauftragte und nicht für externe Dienstleister/innen gelten. Im (nicht beschlossenen) Entwurf zur Novelle des österreichischen DSG 2000 aus dem Jahr 2012 (§ 17a Abs 8 des Entwurfs einer DSG-Novelle 2012) war der/dem Datenschutzbeauftragten eine Ausbildung von 40 Stunden zur Verfügung zu stellen, in jedem weiteren Jahr eine solche im Ausmaß von 20 Stunden. Diese Gedanken können freilich auch nach der DSGVO als – unverbindliche – Stütze für die praktische Ausgestaltung dienen.

3.2 Verantwortung des/der Datenschutzbeauftragten

Der/die Datenschutzbeauftragte ist als beratendes Organ in allen Fragen des Datenschutzes konzipiert. Neben den in Art 39 DSGVO genannten Aufgaben kann der/die Datenschutzbeauftragte auch weitere Aufgaben übernehmen, solange dies nicht zu Unvereinbarkeiten führt.

Bestünden diese „weiteren Aufgaben“ in Management-Aufgaben im Zusammenhang mit der Verwendung personenbezogener Daten, käme der/die Datenschutzbeauftragte somit in die Situation, sich selbst beraten zu müssen, was mit dem Konzept des unabhängigen, mit institutionellen Garantien ausgestatteten Datenschutzbeauftragten in Konflikt steht.

Das bedeutet, dass der/die Datenschutzbeauftragte daher niemals Entscheidungen darüber, wie personenbezogene Daten verwendet werden (inklusive die konzerninternen Vorgaben dazu), treffen kann und dass eine entsprechende Entscheidungsbefugnis automatisch zu einem Interessenkonflikt zwischen dem „Berater“ und dem „Entscheider“ führen muss.

Das bedeutet weiter, dass der/die Datenschutzbeauftragte niemals zum „verantwortlichen Beauftragten“ nach § 9 VStG bestellt werden kann, soweit es um Verstöße gegen Datenschutzrecht geht, weil dafür die gesetzliche Voraussetzung die „entsprechende Anordnungsbefugnis“ ist, die es dem Bestellten ermöglicht hätte, den Verstoß gegen Verwaltungsstrafrecht (hier Datenschutzrecht) abzuwenden.⁸ Dies steht jedoch in krassem Widerspruch zur Rolle des/der Datenschutzbeauftragten

Verantwortlich für die Einhaltung der DSGVO ist der/die Verantwortliche bzw. der/die Auftragsverarbeiter/in. Nur diese kann Adressatin der Strafen/Geldbußen gemäß 83ff DSGVO sein.⁹

Dem/der Datenschutzbeauftragten kommen also ausschließlich folgende Aufgaben zu:

- Kontaktaufgaben: Der/die Datenschutzbeauftragte ist erste Anlaufstelle für die Datenschutzbehörde in allen Fragen zu Datenverarbeitungen der Organisation und arbeitet mit dieser zusammen

⁸ Siehe dazu auch den Leitfaden zur DSGVO der Österreichischen Datenschutzbehörde (S. 32 f) unter <https://www.dsb.gv.at/documents/22758/116802/DSGVO-2016-Leitfaden.pdf/93d6cb80-8d8e-433d-a492-a827e3ed81a2>.

⁹ Siehe dazu Art 5 Abs 2 DSGVO: „Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können („Rechenschaftspflicht“).“ Sowie Art 24 iVm EG 74 DSGVO.

- Beratungsaufgaben: Hier geht es um die Beratung von Management, Mitarbeitern und auch von Betroffenen, die sich an den/die Datenschutzbeauftragten wenden
- Schulungsaufgaben: Der/die Datenschutzbeauftragte ist für die Schulung von Mitarbeitern und Management zuständig
- Kontrollaufgaben: Dem/der Datenschutzbeauftragten obliegt die Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften sowie der Strategien des/der Verantwortlichen oder des/der Auftragsverarbeiters/in im Hinblick auf die Einhaltung der DSGVO. Der/die Datenschutzbeauftragte ist bei der Durchführung von Datenschutzfolgeabschätzungen einzubeziehen und hat regelmäßig an das oberste Management zu berichten.

4 Abgrenzung der Aufgaben des/der Datenschutzbeauftragten zu anderen Positionen in der Organisation

Wir empfehlen eine klare Beschreibung der Aufgaben des/der Datenschutzbeauftragten. Die Aufgaben, die ein/e Datenschutzbeauftragte/r im Rahmen einer Datenschutzorganisation wahrzunehmen hat, überschneiden sich per se schon mit bereits bekannten Rollen in einer Organisation, wie z.B. Compliance und Information Security. Die Art-29-Datenschutzgruppe¹⁰ fordert sogar Grundkenntnisse des/der Datenschutzbeauftragten in diesen Gebieten. Um sowohl negative als auch positive Kompetenzkonflikte zu vermeiden, sollten die Aufgaben dieser Funktionen sehr genau beschrieben und den jeweiligen verantwortlichen Personen in einer Organisation zugewiesen werden. Eine Zusammenarbeit dieser Personen ist in der Praxis jedenfalls zu empfehlen.

5 Arbeitsrechtliche Stellung des/der Datenschutzbeauftragten

Der Gesetzgeber hat im Datenschutz-Anpassungsgesetz 2018¹¹ keine Regelung hinsichtlich einer arbeitsrechtlichen Sonderstellung des/der Datenschutzbeauftragten vorgesehen. Es ist aber aufgrund der Vorgaben in Art 38 Abs 3 DSGVO davon auszugehen, dass dem/der Datenschutzbeauftragten ein sogenannter Motivkündigungsschutz zukommt, wie ihn das österreichische Recht in andere Fällen kennt: Hier gibt es gesetzlich verankert Personen mit besonderem Kündigungsschutz¹². Bei diesen Beschäftigten ist eine Kündigung nur mit Zustimmung des Gerichts/Bundessozialamts zulässig. Eine derartige Bestimmung gibt es für Datenschutzbeauftragte nicht. Um Datenschutzbeauftragten dieselbe Rechtsstellung in Bezug auf Kündigungs- und Entlassungsschutz zu gewähren, bräuchte es wohl eine ausdrückliche gesetzliche Regelung. Diese fehlt. Am ehesten vergleichen lässt sich die Stellung des/der Datenschutzbeauftragten wohl mit der der Sicherheitsvertrauensperson¹³. Diese ist ebenfalls per Gesetz weisungsfrei gestellt. Wird eine Sicherheitsvertrauensperson gekündigt oder entlassen, so

¹⁰ http://ec.europa.eu/newsroom/document.cfm?doc_id=43823

¹¹ BGBl I 2017/120.

¹² Besonderer Kündigungsschutz kommt werdenden Mütter sowie Mütter und Väter, die eine Karenz oder eine Teilzeitbeschäftigung aus Anlass der Geburt in Anspruch nehmen (Elternteilzeit), Betriebsrätinnen/Betriebsräte oder diesen gleichgestellte Personen, Präsenz- und Zivildienstpflichtige sowie Frauen im Ausbildungsdienst, Begünstigt Behinderten und Opferbefürsorgten sowie Hausbesorgern zu.

¹³ Verordnung des Bundesministers für Arbeit und Soziales über die Sicherheitsvertrauenspersonen (SVP-VO) StF: BGBl. Nr. 172/1996, geändert durch BGBl. II Nr. 324/2014

kann sie die Kündigung bzw. Entlassung bei Gericht anfechten, wenn sie wegen ihrer Tätigkeit für die Sicherheit und den Gesundheitsschutz der Arbeitnehmer erfolgt ist. Es ist fraglich, ob sich ein/e Datenschutzbeauftragte ohne gesetzliche Grundlage ebenfalls auf diesen Rechtsschutz berufen wird können. Wir gehen davon aus, dass Art 38 Abs 3 DSGVO nur dann voll direkte Wirkung entfalten kann, wenn dem/der Datenschutzbeauftragten auch tatsächlich diese Stellung im Rahmen von Kündigungs- und Entlassungsszenarien zugestanden wird. So müsste der/die gekündigte/entlassene Datenschutzbeauftragte/r bei Gericht eine widerrechtlich ausgesprochene Kündigung/Entlassung anfechten dürfen.

Externe Datenschutzbeauftragte

Nicht außer Acht gelassen werden darf die Ansicht der Art-29-Datenschutzgruppe, die den besonderen Kündigungsschutz auch auf die Beziehung zwischen Auftraggeber und externen/r Datenschutzbeauftragten auf Basis eines Dienstleistungsvertrages erweitert. Auch wenn fraglich ist, ob das in der Praxis tatsächlich von den zuständigen Gerichten so bestätigt werden wird, ist es rechtlich stringent, dass auch die DSGVO selbst keine Unterscheidung bei der Regelung von Art 38 Abs 3 DSGVO vornimmt. Um hier unnötige Vertragsbindungskonflikte zu generieren, empfiehlt sich gerade bei externen Datenschutzbeauftragten eine befristete Beauftragung (siehe dazu auch Punkt 2.1).

6 Aufgaben des/der Datenschutzbeauftragten

6.1 Kontaktaufgaben

Der/die Datenschutzbeauftragte ist die zentrale Ansprechperson für die Datenschutz- bzw. Aufsichtsbehörde. Hierbei wird besonders darauf zu achten sein, wie sich der/die Datenschutzbeauftragte gegenüber der Datenschutzbehörde präsentiert, wobei der/sie darauf zu achten hat, tatsächlich nur eine Koordinierungs- und Drehscheibenrolle wahrzunehmen und nicht darüber hinaus auch als „Vertretung“ der Organisation des/der Verantwortlichen aufzutreten. Letzteres würde mit der Stellung des/der Datenschutzbeauftragten als unabhängige und weisungsfreie Beratungsstelle kollidieren. Der/die Datenschutzbeauftragte sollte daher tunlichst vermeiden, persönliche Rechtsansichten oder Wahrnehmungen von Sachverhalten als solche klar zu kommunizieren und nicht den Eindruck erwecken, hier Meinungen des Unternehmens äußern bzw. vertreten zu wollen. Gleichzeitig sollte er/sie aber auch regelmäßig intern abgestimmt sein, um strategische Überlegungen nicht zu torpedieren.

6.2 Beratungs-, Überwachungs-, und Schulungsfunktionen

Der/die Datenschutzbeauftragte hat außerdem eine Beratungs-, Überwachungs- sowie eine Schulungsfunktion im Unternehmen:

Beratung

Der/die Datenschutzbeauftragte informiert und berät somit

- das Management,
- die mit der Verarbeitung von personenbezogenen Daten beschäftigten Mitarbeiter/innen
- alle Mitarbeiter/innen als betroffene Personen
- den Betriebsrat (wenn vorhanden) z.B. bei entsprechenden Betriebsvereinbarungen

- auf Anfrage die Verantwortlichen bei der Durchführung der Datenschutz-Folgenabschätzung.

Überwachung

Der/die Datenschutzbeauftragte überwacht die Einhaltung aller datenschutzrechtlichen Bestimmungen, wie

- DSGVO
- Andere Datenschutzvorschriften der EU (z.B. Datenschutzrichtlinie für elektronische Kommunikation)
- Nationale Gesetze (z.B. Datenschutzgesetz, Telekommunikationsgesetz, Arbeitsverfassungsgesetz, E-Commerce Gesetz, Gesundheitstelematikgesetz etc.)

Diese Überwachungspflicht betrifft die Prüfung der relevanten Prozesse und Verfahren zur Erfüllung der Forderungen der DSGVO, wie

- Prozesse zur Wahrnehmung der Betroffenenrechte
- Prozess zur Unterrichtung der Öffentlichkeit und der betroffenen Personen
- Entwicklungsprozesse (data protection by design)
- Prüfung der Zulässigkeit der Verarbeitung bei neu zu implementierender Software

Diese Überwachungspflicht betrifft aber auch die Prüfung der geforderten Dokumente und Verträge, wie

- Verzeichnisse
- Auftragsverarbeitungsverträge
- EU Standardvertragsklauseln bei Datenübermittlung in Drittländer
- Datenschutzerklärungen und rechtswirksame Zustimmungserklärungen
- Verpflichtung der Mitarbeiter zur Einhaltung des Datenschutzes
- Interne Richtlinien zum Umgang mit ITAssets

Sonderaspekte der Überwachung sind die Prüfung der technischen Maßnahmen¹⁴.

Die Überwachungstätigkeit wird unabhängig von der Unternehmensgröße am besten mit einem mindestens jährlich vom/von der Datenschutzbeauftragten durchzuführenden oder von ihm/ihr beauftragten Datenschutzaudit wahrgenommen. Das Ergebnis des Audits geht als Bericht an die Geschäftsleitung und enthält auch die aufgrund der gefundenen Abweichungen durchzuführenden Maßnahmenvorschläge.

Aktive Tätigkeit

Der/die Datenschutzbeauftragte soll aktiv bei der Ausarbeitung und eventuell auch bei der Abhaltung der Awareness-Schulungen mitwirken.¹⁵

¹⁴ Siehe dazu die Checkliste von Privacyofficers.at unter <https://www.privacyofficers.at/privacyofficers-at-veroeffentlicht-checkliste-zur-umsetzung-der-dsgvo/>

¹⁵ Anmerkung: Bei mittleren und kleineren Unternehmen sind diese Verfahren und Dokumente selten vorhanden. Hier wird vermutlich der/die Datenschutzbeauftragte sinnvollerweise bei der Erstellung der Dokumente mitwirken.

Zusammenarbeit mit der Aufsichtsbehörde; Anlaufstelle für die Aufsichtsbehörde.

7 Datenschutzbeauftragte in Behörden und öffentlichen Stellen

Die Ausführungen in diesem Dokument gelten im Wesentlichen auch für Benennung, Stellung und Aufgaben von Datenschutzbeauftragten in öffentlichen Stellen. Das DSG Anpassungsgesetz 2018 sieht einige wenige Besonderheiten für die „öffentlichen“ Datenschutzbeauftragten vor: So sind auch sie ausdrücklich weisungsfrei gestellt und sollen unabhängig ihre Aufgabe wahrnehmen können (§ 5 Abs 2 DSG). Im Wirkungsbereich von Ministerien und diesen nachgelagerten Stellen müssen Datenschutzbeauftragte direkt aus diesen Einrichtungen kommen, die Bestellung von anderen, auch von externen Datenschutzbeauftragten ist hier jedenfalls unzulässig.¹⁶ Schließlich wird den Datenschutzbeauftragten im öffentlichen Bereich durch § 5 Abs 3 DSG gesetzlich aufgetragen, einen regelmäßigen Erfahrungsaustausch im Hinblick auf die Gewährleistung eines einheitlichen Datenschutzstandards zu pflegen.¹⁷

Die Datenschutzbeauftragten im öffentlichen Bereich haben einen Sitz im Datenschutzrat (§ 21 Absatz 6 DSG).

Datenschutzbeauftragte haben an das oberste Management zu berichten. Im öffentlichen Bereich ist davon auszugehen, dass dies jeweils der/die Minister/in selbst ist oder die vergleichbare oberste Organfunktion in einer Verwaltungsorganisation (Bund, Länder, Gemeinden).

¹⁶ Auch wenn sich das mit der Ansicht der Art-29-Datenschutzgruppe in ihrer Richtlinie zum Datenschutzbeauftragten deckt, wonach ein/e Datenschutzbeauftragte/r von Behörden und öffentliche Stellen auch die entsprechenden Kenntnisse der Verwaltungsverfahren und Prozesse innerhalb der Verwaltung kennen und können sollte, sehen wir keine Veranlassung, externe Datenschutzbeauftragte hier gesetzlich auszuschließen. Auch letztere könnten derartiges Wissen und Erfahrung mitbringen.

¹⁷ Hier weisen wir auf die regelmäßigen Netzwerktreffen und internen Vereinsseminare von Privacyofficers.at hin.

**Mustervorlage für die Bestellung einer Person zum/zur Datenschutzbeauftragten gemäß
Artikel 37 DSGVO iVm § 5 DSG**

Bestellung zum/zur Datenschutzbeauftragten gemäß Artikel 37 Abs 1 DSGVO iVm § 5 DSG
Datenschutz-Grundverordnung (EU 2016/679).

Herr/Frau [*Namen einfügen*]_____ wird mit Wirkung ab [*Datum*] zum/zur
Datenschutzbeauftragten im Sinne von Artikel 37 ff DSGVO bestellt.

Die Bestellung bezieht sich auf das Unternehmen/die Organisation/die Behörde [*Namen einfügen*].

Die Bestellung erfolgt auf unbestimmte Zeit /befristet bis [*Datum einfügen*].

Die Bestellung zum/zur Datenschutzbeauftragten kann jederzeit aus wichtigem Grund oder auf
Verlangen der Aufsichtsbehörde widerrufen werden. Die Bestellung endet in jedem Fall spätestens
mit Beendigung des zwischen Herrn/Frau [*Name einfügen*] und [*Name des Dienstgebers einfügen*]
bestehenden (Dienst)vertrages.

Auf die Geheimhaltungspflicht (unbeschadet sonstiger Verschwiegenheitspflichten) und das
Aussageverweigerungsrecht bei der Erfüllung Ihrer Aufgaben gemäß § 5 DSG darf hingewiesen
werden.

[Unterschrift Geschäftsleitung]

Ich nehme hiermit meine Bestellung zum/zur Datenschutzbeauftragten entsprechend dem
obenstehenden Inhalt an.

Ich nehme hiermit zur Kenntnis, dass gemäß Art 37 Abs 7 DSGVO die Kontaktdaten des
Datenschutzbeauftragten (E-Mail-Adresse, Telefonnummer und Anschrift) vom Dienstgeber zu
veröffentlichen sind und diese auch der Datenschutzbehörde mitgeteilt werden müssen.

Ort, Datum

[Unterschrift Datenschutzbeauftragte/r]