Teil 1: Datenschutzbeauftragte in Österreich – Aufgaben und Anforderungen an das Berufsbild

1. Die Rolle der/des Datenschutzbeauftragten gemäß DSGVO/DSG in Österreich

Natalie Ségur-Cabanac

1.1. Datenschutzbeauftragte – in Österreich keine neue Idee, aber nunmehr etabliert

Mit dem Inkrafttreten der DSGVO bzw des neuen DSG wurde erstmals der Beruf der/des Datenschutzbeauftragten in Österreich etabliert. Es gab früher schon erste Versuche des Gesetzgebers, diese Position gesetzlich einzuführen, welche aber dann doch nicht umgesetzt wurden. So sah eine letztlich nicht geplante Novelle zum DSG 2000 im Jahr 2008[1] im § 15a die Einführung eines betrieblichen Datenschutzbeauftragten vor. Dort war zunächst einmal eine zwingende Beratung mit dem Betriebsrat über die Bestellung einer/eines Datenschutzbeauftragten in Betrieben vorgesehen. Im Jahr 2012 wurde ein weiterer Versuch einer Novellierung des DSG 2000[2] gestartet, welcher dann in einem § 17a schon eine Regelung enthalten hätte, die eher der heutigen entspricht. Auftraggeber (heute: Verantwortliche) konnten demnach (freiwillig) eine:n Datenschutzbeauftragten für eine Periode von mindestens drei Jahren bestellen, wobei Weisungsfreiheit und Unabhängigkeit des/der Datenschutzbeauftragten bereits damals festgelegt werden sollten. Doch auch diese Novelle wurde letztlich nicht in die österreichische Rechtsordnung übernommen.

Ein Blick in unser Nachbarland Deutschland zeigt, dass das dortige Bundesdatenschutzgesetz bereits 1977 das Berufsbild der/des Datenschutzbeauftragten eingeführt hat und diese Position bereits auf einer langen Tradition und Historie beruht. Die Rolle der Datenschutzbeauftragten in Deutschland war daher schon lange vor Inkrafttreten der DSGVO fixer Bestandteil der betrieblichen Landschaft. Personen in dieser Position konnten hier bereits vor 2018 mit einem gewissen Selbstverständnis und einer durch Praxis, Judikatur und Literatur weitgehend gefestigten Rechtsstellung ihrer Arbeit nachgehen. Zwar diente die deutsche Regelung sicher als Vorbild für die Bestimmungen der Art 37 ff DSGVO,

1 Siehe ErläutME Datenschutzgesetz-Novelle 2008 182/ME 23. GP, abrufbar unter https://www.parlament.gv.at/PAKT/VHG/XXIII/ME/ME_00182/imfname_106411.pdf.

2 Siehe ErläutME Datenschutzgesetz-Novelle 2012 397/ME 24. GP, abrufbar unter https://www.parlament.gv.at/PAKT/VHG/XXIV/ME/ME_00397/index.shtml.

doch stellen sich gerade in Österreich in der Praxis doch zahlreiche Fragen, die sich wohl aus unseren nationalen Arbeitsgesetzen, aber auch aus Betriebsverfassungsrecht und Konsumentenschutzrecht ergeben. Ein Vergleich mit der deutschen Regelung liegt hier vielleicht auf der Hand, jedoch empfiehlt es sich, zunächst einmal solche Fragen mit Blick auf unsere nationalen Gegebenheiten bzw dem Regelungszweck der DSGVO zu analysieren und zu beantworten. Als Beispiel nenne ich hier die Garantenstellung, die die/den Datenschutzbeauftragte:n in Deutschland trifft, wenn er/sie Verfehlungen mit verursacht oder nicht mit entsprechendem Einsatz abzustellen versucht. Eine derartige Haftungsregelung wurde in Österreich bis dato noch nicht judiziert und kann auch sonst nicht einfach bejaht werden.

1.2. Die Bestellung bzw Benennung einer/eines Datenschutzbeauftragten

Nach Art 37 DSGVO ist zunächst nur in bestimmten Fällen ein:e Datenschutzbeauftragte:r zu bestellen, nämlich dann, wenn

- Behörden oder öffentliche Stellen mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln, Daten verarbeiten,
- die Kerntätigkeit des/der Verantwortlichen oder des Auftragsverarbeiters/der Auftragsverarbeiterin 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
- die Kerntätigkeit der/des Verantwortlichen oder des Auftragsverarbeiters/der Auftragsverarbeiterin in der umfangreichen Verarbeitung besonderer Kategorien von Daten gemäß Art 9 DSGVO oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art 10 DSGVO besteht.

Wird gegen die Bestellpflicht verstoßen, so kann dies zur Verhängung von Bußgeldern führen.

Im Gegensatz zu den Behörden und öffentlichen Stellen sind die beiden anderen Anwendungsfälle eher vage und unbestimmt formuliert. Ein wenig helfen die Leitlinien der (damals noch) Artikel-29-Datenschutzgruppe.[3] In der Praxis muss dennoch jeder Bestellung einer/eines Datenschutzbeauftragten eine Evaluierung vorangehen, in der ein Betrieb anhand zahlreicher Parameter (insbesondere: seiner konkreten Geschäftstätigkeit, der Daten, die verarbeitet werden, der Branche, in der die Tätigkeit ausgeübt wird, seiner Zielgruppe und Betroffenengruppe) dokumentiert prüft, ob die Voraussetzungen von Art 37 Abs 1 lit a und lit b DSGVO erfüllt

3 Siehe unter https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612048. Siehe auch Anhang 1.

sind oder nicht. Es sei an dieser Stelle dadrauf hingewiesen, dass die deutsche Übersetzung des Art 36 DSGVO zwar die Bezeichnung „Benennung" verwendet, im österreichischen Sprachgebrauch jedoch auch das Wort „Bestellung" erlaubt sein sollte. Ist das Ergebnis, dass ein:e Datenschutzbeauftragte:r verpflichtend zu bestellen ist, so sollte in weiterer Folge anhand der Anforderungen an die Person ebenfalls dokumentiert werden, welche Positionen im Unternehmen/in der Organisation nicht mit der Position des/der Datenschutzbeauftragten vereinbar sind.

Unternehmen/Organisationen können auch freiwillig eine:n Datenschutzbeauftragte:n bestellen, der/die dann aber denselben Rechten und Pflichten der Art 37 bis 39 DSGVO unterliegt wie ein:e verpflichtend zu bestellende:r Datenschutzbeauftragte:r.[4] Sollte dies nicht erwünscht sein, so darf eine Position, die sich zwar um Datenschutz kümmern soll, der aber nicht die Stellung einer/eines Datenschutzbeauftragten zugestanden wird, nicht die Bezeichnung „Datenschutzbeauftragte:r" bekommen. Es muss dann durch eine alternative Bezeichnung eine klare Differenzierung vorgenommen werden. Darauf sollte auch die zu besetzende Person achten und für sich ganz klar abstecken, welche Rolle ihr im Unternehmen/in der Organisation tatsächlich zukommt.

Eine Bestellung kann mündlich, sollte zwecks Nachweises aber doch schriftlich erfolgen.[5] Die Bestellung ist der zuständigen Datenschutzbehörde zu notifizieren, spätestens hier ist Schriftlichkeit geboten.

1.3. Dauer der Bestellung

Grundsätzlich enthält die DSGVO in Art 37 ff Regelungen, die direkt auf die arbeitsrechtliche Stellung der/des Datenschutzbeauftragten wirken. So sind Datenschutzbeauftragte gemäß Art 38 DSGVO in ihrer Funktion als Datenschutzbeauftragte weisungsfrei und dürfen nicht wegen der Erfüllung ihrer Aufgaben abberufen oder benachteiligt werden. Das würde übersetzt auf das österreichische Arbeitsrecht bedeuten, dass Datenschutzbeauftragte einem Motivkündigungsschutz unterliegen. Der Europäische Datenschutzausschuss (EDSA) (vormals Artikel-29-Datenschutzgruppe) hat in seinen Leitlinien zum Datenschutzbeauftragten,[6] wonach auch externe Datenschutzbeauftragte im Rahmen eines Dienstleistungsvertrages diesem besonderen Kündigungsschutz unterliegen. Um unerwünschte Bindungssituationen zu vermeiden, könnte eine befristete Bestellung (sowohl von internen als auch von externen Datenschutzbeauftragten) ratsam sein, wobei darauf zu achten ist, dass eine Befristung nicht den oben genannten Grundsätzen der Stellung von Datenschutz-

4 Eine differenzierte Rechtsansicht vertritt das LG Hamm (18 Sa 271/22), das einem freiwillig bestellten Datenschutzbeauftragten kein Sonderkündigungsrecht zugestanden hat (https://www.justiz.nrw.de/nrwe/arbgs/hamm/lag_hamm/j2022/18_Sa_271_22_Urteil_20221006.html).

5 Eine Mustervorlage enthält Anhang 3.

6 https://ec.europa.eu/newsroom/article29/items/612048.

beauftragten widersprechen darf bzw diese nicht umgangen werden dürfen.[7] Hier könnte ein Blick auf die erwähnte versuchte Novelle des DSG 2000 im Jahr 2012 helfen, wo eine Bestellfrist von mindestens drei Jahren vorgesehen war. Dies würde bedeuten, dass eine Befristung von unter drei Jahren die Unabhängigkeit beseitigen könnte, eine Betrachtung des Einzelfalls sollte aber möglich sein.

Auch wenn Datenschutzbeauftragte für die Einhaltung der DSGVO durch den/die Verantwortliche:n selbst nicht verantwortlich gemacht werden können, tragen sie doch sehr viel Verantwortung und in der Praxis kann es durchaus schwierig sein, diese Rolle in einer Organisation einzunehmen. Es braucht insbesondere einiges an Eigenmotivationsfähigkeit und Durchhaltevermögen und Kommunikationsfähigkeit, um die Aufgabe einer/eines Datenschutzbeauftragten wahrzunehmen. Im betrieblichen Alltag zeigt sich regelmäßig, dass das Datenschutzrecht zwar als wichtiger Bestandteil der Prozesse wahrgenommen wird, aber die tatsächliche Befolgung der doch zahlreichen Vorgaben nicht immer von jedem/jeder Mitarbeiter:in proaktiv beachtet wird. Eine Möglichkeit ist, die Funktion einmal für eine befristete Zeit anzutreten und sich dadurch eine allfällige Verlängerung in Disposition zu halten. Insbesondere dann, wenn jemand die Rolle des/der Datenschutzbeauftragten zusätzlich neben einer anderen Tätigkeit übernimmt, kann auch aus der Sicht des/der Datenschutzbeauftragten eine Befristung der Ernennung sinnvoll sein. Sich auf diese Position einzulassen, ist mit gewissen Risiken verbunden, steht ein:e Datenschutzbeauftragte:r doch durchaus auch unter dem Erwartungsdruck, dass das Thema „Datenschutz" im Unternehmen/in der Organisation gut läuft. Eine Befristung der Rolle der/des Datenschutzbeauftragten kann den Druck nehmen, kündigen zu müssen, wenn man in weiterer Folge nur mehr die ursprüngliche Tätigkeit im Unternehmen/in der Organisation wahrnehmen möchte.

1.4. Wer kann zum/zur Datenschutzbeauftragten bestellt werden?

Ein:e Datenschutzbeauftragte:r wird gemäß Art 37 Abs 5 DSGVO auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das die Person auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage der Fähigkeit zur Erfüllung der in Art 39 DSGVO genannten Aufgaben. Datenschutzbeauftragte müssen keine bestimmte Ausbildung

7 In Deutschland, wo es schon länger verpflichtende Datenschutzbeauftragte gibt, können folgende Parameter für eine Befristung von Datenschutzbeauftragten identifiziert werden: Es wird eine Mindestfrist verlangt, die es dem/der Datenschutzbeauftragten ermöglicht, ihre/seine Aufgaben sinnvoll wahrzunehmen. Für interne Datenschutzbeauftragte wird dabei ein Zeitraum von zwei bis fünf Jahren als ausreichend angesehen. Bei externen Datenschutzbeauftragten werden 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, die Prüfung der Eignung müsse vor der Bestellung erfolgen.

haben, auch wenn es sinnvoll ist, wenn die Person sich auf einen juristischen und/oder technischen Ausbildungshintergrund berufen kann. Das erforderliche Niveau des Fachwissens sollte sich laut EG 97 zur DSGVO „[…] *insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz für die von dem Verantwortlichen oder dem Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten*". Es wird also von der Art des Unternehmens/der Organisation und den konkreten Datenverarbeitungsvorgängen abhängen, über welche fachliche Qualifikation Datenschutzbeauftragte verfügen sollen. Der EDSA (Artikel-29-Datenschutzgruppe) spezifiziert dies in seinen Richtlinien zum Datenschutzbeauftragten[8] insofern, als er verlangt, dass Datenschutzbeauftragte Kenntnisse im nationalen und europäischen Datenschutzrecht und auch der Praxis im Datenschutzrecht inklusive eines tieferen Verständnisses der DSGVO haben sollte. Außerdem wären nach Ansicht von EDSA Kenntnisse der Branche und der Organisation des/der Verantwortlichen (und dabei insbesondere entsprechendes Wissen und Erfahrung hinsichtlich der Datenverarbeitungen des Unternehmens/der Organisation, der Informationssysteme und der Anforderungen an Datensicherheit und Datenschutzmaßnahmen) sehr hilfreich. Für Behörden und öffentliche Stellen sollte ein:e Datenschutzbeauftragte:r auch die entsprechenden Abläufe der Verwaltungsverfahren und Prozesse innerhalb der Verwaltung kennen und beherrschen können. Dieser Anforderung ist der österreichische Gesetzgeber im DSG insofern nachgekommen, als dieses für Datenschutzbeauftragte im Wirkungsbereich von Ministerien vorschreibt, dass die Personen aus dem Ministerium oder dessen nachgelagerten Stellen kommen müssen.

Ansonsten ist es einem Unternehmen/einer Organisation überlassen, eine:n Dienstnehmer:in oder eine externe Person zum/zur Datenschutzbeauftragten zu bestellen (Art 37 Abs 6 DSGVO). Dabei sind allfällige Interessenkollisionen mit der sonstigen Position und Rolle der zu benennenden Person zu berücksichtigen. Es ist also insbesondere darauf zu achten, dass die Person nicht eine Funktion innehat, in der sie Entscheidungen treffen kann, die in Konflikt mit der Kontrollverantwortung von Datenschutzbeauftragten stehen, indem sie selbst Tätigkeiten ausübt, die ihr Verantwortung über Datenverarbeitungen zukommen lässt, und sie sich damit selbst kontrollieren müsste.[9]

1.5. Aufgaben von Datenschutzbeauftragten

Die Aufgaben von Datenschutzbeauftragten lassen sich im Wesentlichen wie folgt beschreiben:

- **Kontaktaufgaben:** Der/Die Datenschutzbeauftragte ist eine zentrale Anlaufstelle für die Datenschutzbehörde in allen Fragen zu Datenverarbeitungen des

8 Diese sind in Anhang 2 abgedruckt.
9 Siehe dazu auch 8. und 10.

Unternehmens/der Organisation und arbeitet mit dieser zusammen. Er/Sie steht auch für Anfragen von Betroffenen zur Verfügung.
- **Beratungsaufgaben:** Beratung von Management sowie der Mitarbeiter:innen, die sich an den/die Datenschutzbeauftragte:n wenden.
- **Schulungsaufgaben:** Der/Die Datenschutzbeauftragte ist für die Schulung von Mitarbeiter:innen und Management zuständig.
- **Kontrollaufgaben:** Einem/Einer Datenschutzbeauftragten obliegt die Überwachung der Einhaltung der DSGVO und anderer Datenschutzvorschriften sowie der Strategien der/des Verantwortlichen oder des Auftragsverarbeiters/der Auftragsverarbeiterin im Hinblick auf die Einhaltung der DSGVO. Er/Sie ist bei der Durchführung von Datenschutz-Folgenabschätzungen (DSFA) einzubeziehen und hat regelmäßig an das oberste Management zu berichten.[10]

Bei der Bestellung einer/eines Datenschutzbeauftragten empfiehlt sich eine klare Abgrenzung seiner/ihrer Aufgaben zu sonstigen Funktionen im Unternehmen/in der Organisation, die ähnliche Aufgaben innehaben. Dies betrifft zum Beispiel die Aufgaben von Compliance-Beauftragten oder Information-Security-Beauftragten.

Bei Implementierung eines Datenschutzmanagementsystems sollte darauf geachtet werden, dass dem/der Datenschutzbeauftragten ausreichend Möglichkeit gegeben wird, im betrieblichen Alltag so mitzuwirken, dass sie/er den Überblick erhalten und vor allem behalten kann. Es liegt wiederum am/an der Datenschutzbeauftragten, sich in ihrer/seiner Tätigkeit als Berater:in und „Ermöglicher:in" zu positionieren, denn ihre/seine Rolle kann aufgrund der hohen Verantwortung, welche sich nicht zuletzt auch in den Strafen manifestiert, die mit der Verletzung der DSGVO verbunden sein können, aus Sicht der Mitarbeiter:innen schnell in die eines Neinsagers bzw Blockierers mutieren. Es bedarf in der Praxis einiges an persönlicher Überzeugungs- und Vernetzungsarbeit im Betrieb, um sich als Person, als Position kooperativ zu etablieren.

Zu betonen ist, dass Datenschutzbeauftragte nicht für die Einhaltung der DSGVO verantwortlich sind. Insofern ist es auch nicht möglich, den/die Datenschutzbeauftragte:n als Verantwortliche:n gemäß § 9 VStG zu nominieren. Die Verantwortung für die Einhaltung der DSGVO kommt dem Unternehmen/der Organisation (als Verantwortlichem/Verantwortlicher oder Auftragsverarbeiter:in) zu und nicht dem/der Datenschutzbeauftragten. Es obliegt daher dem Unternehmen/der Organisation, dafür zu sorgen, dass die DSGVO entsprechend erfüllt wird, dh, dass insbesondere die nachstehenden Anforderungen erfüllt werden:

- **Rechenschaftspflicht:** Führung eines Verfahrensverzeichnisses, Management der Auftragsverarbeiter:innen, Privacy by Design, Privacy by Default, Compliance von neuen Datenanwendungen, Durchführung von Datenschutz-Folgenabschätzungen

10 Siehe dazu auch 6.

- **Transparenz:** Etablierung eines Datenschutzmanagementsystems, Informationspflichten an Betroffene, Regeln für den Datentransfer in Nicht-EU-Länder
- **Information:** Beratung und Schulung der Mitarbeiter:innen, Fortbildungen und Ausbildung der/des Datenschutzbeauftragten
- **Externe Kommunikation:** Zusammenarbeit mit der Datenschutzbehörde, Bearbeitung und Beantwortung von Anfragen auf Geltendmachung von Betroffenenrechten, Bearbeitung und Meldung von Datensicherheitsvorfällen.

1.6. Die Stellung von Datenschutzbeauftragten

Das Gesetz stellt eine:n internen Datenschutzbeauftragte:n einer externen Person gleich.

Ist ein:e Datenschutzbeauftragte:r benannt, sind ihre/seine Kontaktdaten der Aufsichtsbehörde mitzuteilen (Art 37 Abs 7 DSGVO). Dazu genügt ein einfaches E-Mail an die österreichische Datenschutzbehörde mit Namen, Position und Kontaktdaten.

Ein:e (interne:r) Datenschutzbeauftragte:r unterliegt wie alle Dienstnehmer:innen dem Datengeheimnis gemäß § 6 DSG. Darüber hinaus treffen sie/ihn und die für sie/ihn tätigen Personen gemäß § 5 DSG weitgehende Geheimhaltungspflichten, insbesondere, was die Identität von Betroffenen betrifft, die sich an sie wenden. Datenschutzbeauftragte und deren Mitarbeiter:innen profitieren zudem von einem gesetzlichen Aussageverweigerungsrecht, das der Stelle zukommt, für die er/sie tätig ist (§ 5 Abs 2 DSG).

Datenschutzbeauftragte sind frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden. Das bedeutet im Wesentlichen, dass bereits von Anfang an sichergestellt sein muss, dass die Anforderungen des Datenschutzes bei der Einführung einer geplanten Datenverarbeitung mit berücksichtigt werden. Auch aufgrund der den/die Verantwortliche:n gemäß DSGVO treffenden Rechenschaftspflicht sowie angesichts der Anforderungen aus *data privacy by design* und *data privacy by default* ist es ratsam, standardmäßig den/die Datenschutzbeauftragte:n von Anfang an in geplante Datenverarbeitungsprozesse einzubeziehen und damit sicherzustellen, dass der DSGVO entsprochen wird. Nur so kann gewährleistet werden, dass laufende und neue Datenanwendungen den Vorgaben der DSGVO entsprechen und letztlich weiterhin betrieben werden dürfen. Das klingt einfacher, als es in der Praxis oft ist. Datenschutzbeauftragte müssen sich oft sehr anstrengen, damit sie im betrieblichen Alltag rechtzeitig einbezogen werden. Es wird auf Seiten der verantwortlichen Organisationen häufig der Fehler gemacht, den Datenschutz und die Expertise der/des Datenschutzbeauftragten als deren/dessen alleinige Bring-/Holschuld zu sehen. Vielmehr kann es nur funktionieren, wenn die Prozesse so aufgesetzt sind, dass sie als Bringschuld des Unternehmens/der Organisation wirken und so der/dem Datenschutzbeauftragten nicht

Teil 3: Datenschutzbeauftragte in KMU und kleinen Vereinen

Heidi Scheichenbauer/Natascha Windholz

1. Einleitung

Die DSGVO enthält keine allgemeine Verpflichtung zur Bestellung von Datenschutzbeauftragten, diese kann auch kleine und mittlere Unternehmen (KMU)[1] sowie Vereine (bzw andere gemeinnützige Einrichtungen) betreffen.

Verantwortliche und Auftragsverarbeiter müssen dabei grundsätzlich stets selbst einschätzen, ob sie von einer Bestellpflicht betroffen sind. Aufgrund der hohen möglichen Bußgelder[2] führt dies auch betreffend die Bestellpflicht zu einer deutlichen höheren Eigenverantwortung von KMU und Vereinen als bis zum Inkrafttreten der DSGVO am 25.5.2018.

Die bisherige Beratungspraxis zeigt, dass vor allem kleinere Einrichtungen aufgrund beschränkter Mittel häufig bei der Erfüllung datenschutzrechtlicher Anforderungen an ihre Grenzen stoßen.

Teil 3 soll eine Anleitung dafür bieten, wann von KMU und kleinen Vereinen ein Datenschutzbeauftragter bestellt werden muss, und die wichtigsten Umsetzungsschritte darstellen.

2. Allgemeines zur Benennungspflicht

Für KMU und Vereine (oder andere Verantwortliche bzw Auftragsverarbeiter[3]) sieht die DSGVO nach Art 37 DSGVO eine Bestellpflicht bei Erfüllung der folgenden Kriterien vor:

- Die Kerntätigkeit der Stelle besteht in der umfangreichen Verarbeitung von besonderen Datenkategorien oder strafrechtlich relevanten Daten.
- Die Kerntätigkeit besteht in der umfangreichen, regelmäßigen und systematischen Überwachung von Betroffenen.[4]

1 Kleinstunternehmen: bis neun Beschäftigte und bis € 2 Mio Umsatz/Jahr. Kleines Unternehmen: bis 49 Beschäftigte und bis € 10 Mio Umsatz/Jahr und kein kleinstes Unternehmen. Mittleres Unternehmen: bis 249 Beschäftigte und bis € 50 Mio Umsatz/Jahr und kein kleinstes oder kleines Unternehmen. Vgl dazu Empfehlung der Kommission vom 6. Mai 2003 betreffend die Definition der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen.

2 Art 83 Abs 4 lit a DSGVO. Ein Verstoß gegen diese Bestellverpflichtung kann mit Geldbußen von bis zu € 10 Mio bzw bis zu 2 % des gesamten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahres geahndet werden.

3 Zur Tätigkeit von Datenschutzbeauftragten im öffentlichen Bereich siehe Teil 4: 7.

4 Art 37 Abs 1 lit c DSGVO.

Die Verwendung gleich mehrerer unbestimmter Rechtsbegriffe wie „Kerntätigkeit", „umfangreiche Verarbeitung" und „umfangreiche, regelmäßige und systematische Überwachung" hat häufig Auslegungsschwierigkeiten dieser Bestimmung zur Folge.

3. Was versteht man unter der Kerntätigkeit?

Sofern kein Datenschutzbeauftragter auf freiwilliger Basis bestellt wird, ist in einem ersten Schritt eine Abgrenzung zwischen Haupt- und Nebentätigkeit vorzunehmen.[5]

Gemäß den Erläuterungen zur DSGVO (Erwägungsgründe) bezieht sich die Kerntätigkeit von KMU oder Vereinen, die sich in der Rolle von Verantwortlichen oder Auftragsverarbeitern befinden, auf ihre Haupttätigkeiten und somit nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeiten.

Die zu prüfenden Verarbeitungstätigkeiten müssen daher die Haupttätigkeit bzw ein wesentlicher Bestandteil dieser sein,[6] idR wird jene Tätigkeit die Kerntätigkeit sein, die der Verwirklichung der Ziele der jeweiligen Organisation dient. Im KMU-Bereich wird es sich um den Unternehmensgegenstand handeln, bei Vereinen um Tätigkeiten in Verbindung mit den statutengemäßen Vereinszielen.[7] Somit wird die Kerntätigkeit durch jene Bereiche charakterisiert, die für die Umsetzung der Unternehmensstrategie bzw Vereinsziele entscheidend sind, und nicht bloß routinemäßige Verwaltungs- und Erhaltungsaufgaben. Die zu beurteilenden Tätigkeiten müssen den Hauptunternehmensgegenstand bzw Hauptzweck des jeweiligen KMU/Vereins betreffen.[8]

Zudem vertritt die Artikel-29-Datenschutzgruppe bzw deren Nachfolger, der Europäische Datenschutzausschuss, die Auffassung, dass auch in Konstellationen, in denen die Zielverwirklichung nicht unmittelbar mit der Verarbeitung personenbezogener Daten verbunden ist, Verarbeitungen, die einen untrennbaren Bestandteil der Tätigkeiten von Verantwortlichen darstellen, ebenfalls zur Bestellpflicht führen können.[9] Hier wurde als Beispiel angeführt, dass die Kerntätigkeiten von Krankenhäusern in der Erbringung von Gesundheitsdienstleistungen liegen würden, diese Tätigkeit jedoch nicht ohne die Verarbeitung von personenbezogenen Daten möglich sei. Diese Verarbeitungstätigkeiten wurden als Kerntätigkeit von Krankenhäusern betrachtet.

Zu den Kerntätigkeiten von Vereinen wird jedenfalls die Mitgliederverwaltung zu zählen sein sowie Verarbeitungstätigkeiten, die im Zusammenhang mit den ideellen oder materiellen Mitteln zur Verwirklichung des Vereinszwecks erfolgen.

5 *Jaksch*, Die Bestellungspflichten eines Datenschutzbeauftragten gemäß DSGVO, ZIIR 2017, 143.
6 *Jaksch*, ZIIR 2017/2, 143.
7 *Knyrim/Löffler*, Stellung und Aufgaben von Datenschutzbeauftragten, Compliance Praxis 2017/1, 22.
8 *Jaksch*, ZIIR 2017/2, 143.
9 Art-29-Datenschutzgruppe, WP 243 rev.01, 8.

Der bloße Einsatz von Google Analytics durch einen Onlinehändler oder einen Verein auf der unternehmenseigenen Website bzw der Vereinswebsite wird mangels Qualifikation als Kerntätigkeit nicht zu dieser gehören.[10]

Grundsätzlich bedürfen datengetriebene Geschäftsmodelle aufgrund ihrer Verarbeitungsvorgänge einer genaueren Prüfung, nicht datenintensive Geschäftsmodelle werden idR zu keiner Bestellpflicht führen.[11]

3.1. Wann liegt eine umfangreiche Verarbeitung von besonderen Datenkategorien oder strafrechtlich relevanten Daten vor?

Wurden die zu untersuchenden Verarbeitungstätigkeiten der Kerntätigkeit zugeordnet, muss ein Datenschutzbeauftragter bestellt werden, wenn die Kerntätigkeit in einer umfangreichen Verarbeitung von besonderen Datenkategorien oder von strafrechtlich relevanten Daten besteht.

Im Datenschutzrecht existiert ein Konglomerat an Datenkategorien, die als besonders schutzwürdig angesehen wurden und deren Verarbeitung nur unter strengeren Anforderungen zulässig ist als die Verarbeitung von „normalen" personenbezogenen Daten, die in der Vergangenheit als sensible Daten bezeichnet wurden. Die DSGVO selbst verwendet den Begriff „sensible Daten" nicht mehr, in der Praxis ist der Terminus jedoch nach wie vor gebräuchlich. Dabei handelt es sich zunächst um die in Art 9 DSGVO genannten besonderen Kategorien von personenbezogenen Daten, also personenbezogene Daten, aus denen

- die rassische und ethnische Herkunft,
- politische Meinungen,
- religiöse oder weltanschauliche Überzeugungen oder
- die Gewerkschaftszugehörigkeit

hervorgehen.[12]

Zudem zählen zu diesen besonderen Datenkategorien auch

- genetische Daten,
- biometrische Daten,

10 *Jaksch*, ZIIR 2017, 145. Siehe zu dem Themenbereich *jedoch* auch APD/GBA (Belgien) 2.2.2022, 21/2022 in Teil 1: 8., wo IAB (Interactive Advertising Bureau Europe) auch deswegen bestraft wurde, weil sie keinen Datenschutzbeauftragten bestellt hatten. Die belgische Datenschutzbehörde stellte fest, dass das TCF (Transparency and Consent Framework) eine umfangreiche Datenverarbeitung zur Überwachung darstellt.

11 *Jaksch*, ZIIR 2017/2, 144.

12 Hier ist aufgrund der Spruchpraxis der Datenschutzbehörde, der nationalen Verwaltungs- und Zivilgerichte sowie des EuGH davon auszugehen, dass etwa auch Einstufungen wie eine mögliche politische Affinität bzw gewisse Marketingklassifikationen unter den Begriff der besonderen Datenkategorien fallen können.

- Gesundheitsdaten und
- Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

Darüber hinaus werden auch personenbezogene Daten, die in Art 10 DSGVO genannt werden, als besonders schutzwürdig betrachtet. Das sind personenbezogene Daten über

- strafrechtliche Verurteilungen und Straftaten
- oder damit zusammenhängende Sicherungsmaßregeln.

Wann eine umfangreiche Verarbeitung vorliegt, wird von der DSGVO nicht festgelegt.

Die Leitlinien zum Datenschutzbeauftragten der Art 29-Datenschutzgruppe (WP 243 rev.01)[13] nehmen dazu Stellung und führen aus, dass *„die Verarbeitung personenbezogener Daten* […] *nicht als umfangreich gelten* [sollte], *wenn die Verarbeitung personenbezogene Daten von Patienten oder* […] *betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes* […] *erfolgt*".

Weitere Anhaltspunkte dahingehend, was unter einer „umfangreichen Datenverarbeitung" zu verstehen ist, finden sich in den Leitlinien zur Datenschutz-Folgenabschätzung (DSFA) und Beantwortung der Frage, ob eine Verarbeitung im Sinne der Verordnung 2016/679 *„wahrscheinlich ein hohes Risiko mit sich bringt"*, WP 248 rev.01.[14]

Demnach sind folgende Kriterien zu berücksichtigen:

- Zahl der Betroffenen, entweder als konkrete Anzahl oder als Anteil der entsprechenden Bevölkerungsgruppe;
- verarbeitete Datenmenge bzw Bandbreite der unterschiedlichen verarbeiteten Datenelemente;
- Dauer oder Dauerhaftigkeit der Datenverarbeitung;
- geografisches Ausmaß der Datenverarbeitung.[15]

Weitere Hinweise, vor allem „numerischer Natur" (zB durch Nennung einer konkreten Zahl), sind jedoch in den Leitlinien nicht zu finden.

Als Anhaltspunkt kann eine Entscheidung der DSB betreffend ein Allergiezentrum herangezogen werden, in welchem mehrere Ärzte beschäftigt waren und die Ausnahmeregelung betreffend „einzelne" Ärzte daher nicht zur Anwendung kam. Hier stellte die Behörde fest, dass

- die Kerntätigkeit der Verantwortlichen in der Diagnostik und Behandlung von Allergien – sohin in der Verarbeitung von Gesundheitsdaten nach Art 9 Abs 1 DSGVO – bestand,

13 Siehe Leitlinien in Bezug auf Datenschutzbeauftragte („DSB") in Anhang 2.

14 Diese Leitlinien sind auf der Website der österreichischen Datenschutzbehörde unter: https://www.dsb.gv.at/documents/22758/112500/Leitlinien+zur+Datenschutz-Folgenabschaetzung-wp248-rev-01_de.pdf/2246301e-ffbb-4a03-bf23-797fee89174e abrufbar.

15 Siehe Entscheidung der DSB 16.11.2018, DSB-D213.692/0001-DSB/2018.

- zwölf Büro- bzw Labormitarbeiter, siebzehn Ärzte und zwei Ernährungsberater mit Verarbeitungstätigkeiten beschäftigt waren und
- Gesundheitsdaten von Gesetzes wegen tw mindestens zehn Jahre zu speichern sind (§ 51 ÄrzteG)

und die Organisation daher zu dem Schluss hätte kommen müssen, dass aufgrund der umfangreichen Verarbeitung sensibler Daten (besonderer Kategorien von Daten) verpflichtend ein Datenschutzbeauftragter zu bestellen gewesen wäre.

Bemerkenswert war auch, dass in dieser Entscheidung nicht auf die konkrete Anzahl der Betroffenen bzw die verarbeitete Datenmenge eingegangen wurde.

Ein weiterer Hinweis auf den Bedeutungsinhalt des Begriffs „umfangreich" ist in einer Entscheidung der DSB betreffend den Verlust eines Suchtmittelbuches zu finden. In dieser Entscheidung hatte sich die Datenschutzbehörde[16] mit den Voraussetzungen auseinanderzusetzen, unter welchen die Datenschutzbehörde von datenschutzrechtlich Verantwortlichen verlangen kann, eine nach Art 34 Abs 1 DSGVO gebotene Benachrichtigung betreffend eine Datenschutzverletzung an die Betroffenen vorzunehmen.

Der Verantwortliche meldete der Datenschutzbehörde, dass ein Suchtmittelbuch verloren gegangen sei, in dem von ca 150 Patienten in unverschlüsselter Form der Name, der körperliche Gesundheitszustand sowie die verabreichte Menge des Suchtgiftes enthalten waren. Der Verantwortliche ging im vorliegenden Fall davon aus, dass die betroffenen Patienten nicht benachrichtigt werden müssten, weil kein hohes Risiko für diese vorläge. Die DSB sah dies anders und trug dem Verantwortlichen die Benachrichtigung der Betroffenen auf. Begründet wurde dies damit, dass ein hohes Risiko für die Rechte und Freiheiten betroffener Personen bestünde, da eine umfangreiche Verarbeitung besonderer Kategorien von Daten, worunter auch Gesundheitsdaten fallen, vorliegen würde.

Dabei wurde von der Behörde somit bereits der Verlust von 150 Datensätzen als umfangreiche Verarbeitung besonderer Datenkategorien angesehen (auch wenn diese Entscheidung nicht mit einer Bestellpflicht von Datenschutzbeauftragten in Zusammenhang stand).

3.2. Was ist unter regelmäßiger, systematischer und umfangreicher Überwachung zu verstehen?

Eine Bestellpflicht entsteht zudem, wenn die Kerntätigkeit in einer regelmäßigen, systematischen und umfangreichen Überwachung von Betroffenen besteht. Das Erfordernis einer Überwachung muss sich aus Art, Umfang oder den Zwecken

16 Siehe Entscheidung der DSB 8.8.2018, DSB-D084.133/0002-DSB/2018.

einer Verarbeitungstätigkeit ergeben.[17] Hier handelt es sich regelmäßig um umfangreiche, systematische personenbezogene Auswertungen im Rahmen von Profilbildungen[18] (insbesondere von Internet-Usern).[19]

Darunter können Versicherungen fallen, die eine Beobachtung der Versicherungsnehmer vornehmen, um ihnen individualisierte Tarife anzubieten, oder Marketingmaßnahmen, die auf individuellen detaillierten Kundenprofilen beruhen und mit denen nicht alle Kunden gleich angesprochen werden.

Umfangreiche und systematische Überwachungen können etwa durch Online-Tracking-Maßnahmen erfolgen.[20]

4. Vereine, die möglicherweise eine Bestellpflicht trifft

Für Vereine kann es zu einer Vielzahl von Konstellationen kommen, in denen sich die Frage der Bestellpflicht stellt.

So kann der Betrieb von Betreuungseinrichtungen (Hospiz- oder Pflegeheime bzw andere Betreuungseinrichtungen aus dem Bereich der mobilen Pflege und Betreuung/Vertretung von Menschen mit Behinderungen oder anderen gesundheitlichen Beeinträchtigungen) oder das Betreiben von Beratungseinrichtungen das Thema Bestellpflicht eines Datenschutzbeauftragten nach sich ziehen, wenn dieser mit einer umfangreichen Verarbeitung von besonderen Datenkategorien („sensiblen Daten“) verbunden ist.

Zudem kann Vereine mit politischer, religiöser oder weltanschaulicher Ausrichtung eine Bestellpflicht treffen. Auch Vereinigungen, die sich etwa für die Rechte von Homosexuellen oder für Transgenderanliegen einsetzen, kommen für eine Bestellpflicht in Frage, ebenso wie Selbsthilfegruppen oder Vereine der Bewährungshilfe.

Bezüglich des Kriteriums der umfangreichen Verarbeitung von „sensiblen Daten“ kann aktuell auf die beiden oben angeführten rechtskräftigen Entscheidungen der Datenschutzbehörde verwiesen werden. Die Prüfung der Bestellpflicht sollte diese Entscheidungen jedenfalls berücksichtigen.

17 *Jaksch*, ZIIR 2017, 144 unter Verweis auf *Paal* in *Paal/Pauly* (Hrsg), Datenschutz-Grundverordnung (2017) Art 37 Rz 8.

18 *Jaksch*, ZIIR 2017, 144 unter Verweis auf *Jaspers/Reif*, RDV 2016, 61 (rdv-online).

19 Als typische Beispiele für eine regelmäßige und systematische Überwachung wurden etwa verfolgende E-Mail-Werbung und verhaltensbasierte Werbung angeführt *(online tracking)*. Art-29-Datenschutzgruppe, WP 243 rev.01.8. *König* nennt dazu als Beispiele Kreditauskunfteien, Banken, Versicherungen, Unternehmen, die Bewertungsplattformen und Vergleichsportale betreiben, Big-Data-Analysten und IT-Dienstleister. Siehe *König*, Der Datenschutzbeauftragte, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung 235.

20 *Jaksch*, ZIIR 2017/2, 144 mwN.