Teil 3:
Der DSBA 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 bisher.

Die bisherige Beratungspraxis zeigt, dass vor allem kleinere Einrichtungen aufgrund beschränkter Mittel häufig bei der Inangriffnahme des Projekts „DSGVO-Umsetzung" an ihre Grenzen stoßen.

Dieser Beitrag 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 35 DSGVO eine Bestellpflicht bei Erfüllung der folgenden Kriterien vor:

---

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 Kap 7.

- 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]

Die Verwendung gleich mehrerer unbestimmter Rechtsbegriffe wie „Kerntätigkeit", „umfangreiche Verarbeitung" und „umfangreiche, regelmäßige und systematische Überwachung" führt 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, 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

4 Art 37 Abs 1 lit c DSGVO.
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.

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.

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 zur Kerntätigkeit 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 sensible Daten geheißen haben. 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]

10 *Jaksch,* ZIIR 2017, 145.

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

12 Hier ist (Stand 18.8.2019) aufgrund einer Entscheidung der Datenschutzbehörde vom 11.2.2019, DSB-D213.747/0002-DSB/2019 und einer zivilgerichtlichen Entscheidung, Urteil des LG Feldkirch 7.8.2019, 57 Cg 30/19b, vorläufig davon auszugehen, dass etwa auch Einstufungen wie eine mögliche politische Affinität bzw gewisse Marketingklassifikationen unter den Begriff der besonderen Datenkategorien fallen können.

Zudem zählen zu diesen besonderen Datenkategorien auch

- genetische Daten,
- biometrische Daten,
- 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.

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 vom 16.11.2018, DSB-D213.692/0001-DSB/2018.

Als ein 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
- 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 bestellt werden hätte müssen.

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).

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

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 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 der Betrieb 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

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.

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.

4.1. Fallgruppen: Vereine, die (möglicherweise) eine Bestellpflicht aufgrund umfangreicher Verarbeitung besonderer Datenkategorien/Strafdaten trifft

- Selbsthilfevereine
- Beratungsvereine für Menschen mit gesundheitlichen Problemen
- Bewährungshilfevereine
- Politische Vereine/Gewerkschaften
- Religiöse Vereine
- Vereine mit weltanschaulicher Ausrichtung

4.1.1. Umfangreiche systematische oder regelmäßige Überwachung durch Vereine?

Die Kerntätigkeit von Vereinen wird wohl nur in Ausnahmefällen das Kriterium der umfangreichen systematischen oder regelmäßigen Überwachung erfüllen.

Vielen gemeinnützigen Vereinen ist die Durchführung ihrer Organisationszwecke häufig (zumindest zum überwiegenden Teil) nur aufgrund von Spenden möglich. Hier scheint grundsätzlich unbestritten zu sein, dass die Kerntätigkeit dieser Vereine in der Verwirklichung ihrer gemeinnützigen Ziele liegt und wohl nicht in der „umfangreichen, regelmäßigen, systematischen Überwachung von Betroffenen".

Jedoch kann man argumentieren, dass Spenden und die damit verbundene Verwaltung von Spenderdaten in Datenbanken „untrennbar" mit dem Vereinszweck verbunden sind. Die mit der Spendenwerbung in Verbindung stehenden Datenverarbeitungen könnten aufgrund einer untrennbaren Verbindung zur Kerntätigkeit des Vereins zu zählen sein. Die bloße Spendereigenschaft ist idR nicht ausreichend, um ein sensibles Datum darzustellen, somit ist regelmäßig auch keine umfangreiche Verarbeitung von besonderen Datenkategorien gegeben. Ausnahmen können sich hier etwa im Bereich von Spendern ergeben, die gleichzeitig Angebote aus dem Gesundheitsbereich nützen und deren „Patienteneigenschaft" dem Verein bekannt ist bzw bekannt sein müsste.

Bei Vereinen, die vorwiegend spendenfinanziert sind, zählt die Verarbeitung von Spenderdaten aufgrund der untrennbaren Verbindung zwischen den Organisationsmitteln und der Mittelaufbringung durch Spenden zu ihrer Kerntätigkeit. Diese besteht jedoch nicht zwangsläufig in einer *„umfangreichen, systematischen oder regelmäßigen Überwachung"* der Spender im Sinne von Art 37 DSGVO. Eine generelle Verpflichtung zur Bestellung eines DSBA scheint für gemeinnützige spendenfinanzierte Vereine nicht zu bestehen. Diese setzen jedoch teilweise Methoden des E-Mail-Retargeting ein und dies könnte ab einem gewissen Ausmaß einer umfangreichen, systematischen oder regelmäßigen Überwachung gleichkommen. Auch könnten gewisse Kommunikationsabläufe mit den Spendern als verhaltensbasierende Werbung angesehen werden. Je spezifischer die Beziehung zu den Spendern aufgebaut ist, desto eher wird daraus eine Pflicht zur Benennung eines DSBA resultieren.[21]

Bei rein zielgruppenspezifischen Auswertungen und Maßnahmen liegen keine persönlich individualisierten Werbestrategien und keine Überwachung im Sinne des Art 37 DSGVO vor.

Im Großspenderbereich muss im Einzelfall (also für den jeweiligen Verein) beurteilt werden, ob auch die erforderliche umfangreiche Überwachung vorliegt, um die Bestellpflicht auszulösen. Dabei ist zu berücksichtigen, dass Großspender im Spendersegment eines Vereins oft nur einen geringen Anteil der Spender repräsentieren, wobei das Spendenaufkommen durch diese jedoch einen wesentlichen Anteil des Spendenvolumens ausmachen kann.

Je spezifischer die Beziehung zu den Spendern aufgebaut ist, desto eher wird daraus eine Pflicht zur Benennung eines DSBA resultieren.

4.1.2. Vorgehensweise bei Prüfung der Bestellpflicht

In einem ersten Schritt kann anhand der folgenden Checkliste überprüft werden, ob eine Bestellpflicht bestehen kann:[22]

21 Siehe dazu auch *Scheichenbauer* in *Bergauer/Jahnel/Mader/Staudegger*, jusIT Spezial: DS-GVO (2018) 169 ff.

22 Siehe dazu auch *Scheichenbauer*, Datenschutz für Vereine (2018) 119.

Prüfschritte: