LexisNexis

Compliance Praxis

06.03.2017 14:43

Stellung und Aufgaben von Datenschutzbeauftragten

0 Kommentare

01.03.2017 | Von Dr. Rainer Knyrim, DI Michael Löffler
Schlagworte : DSB | Artikel-29-Datenschutzgruppe | Datenschutz | Datenschutzbeauftragter
Erschienen in Compliance Praxis 2017, 22 (Heft 1)

Dieser Beitrag beleuchtet die Stellung und die Aufgaben von Datenschutzbeauftragten nach der Datenschutz-Grundverordnung und fasst die Empfehlungen der Artikel-29-Datenschutzgruppe zu Datenschutzbeauftragten zusammen.

Die Datenschutz-Richtlinie (Datenschutz-RL 95/46/EG) stellt es Mitgliedstaaten frei, Datenschutzbeauftragte (DSB) zu etablieren. Die Datenschutz-Grundverordnung (DSGVO VO 679/2016/EU) hingegen sieht teils zwingend die Bestellung von DSB vor (Art 37 ff DSGVO).

Im Zusammenhang mit der Bestellung von DSB und ihren Aufgaben enthält die DSGVO zahlreiche Begriffe, die wohl nur für den Verordnungsgeber präzise und verständlich sind. Daher hat die Artikel-29-Datenschutzgruppe [1] Richtlinien veröffentlicht, um DSGVO-Anwendern die Stellung und die Tätigkeiten von DSB zu erklären. [2] Dieser Beitrag gibt einen Überblick über DSB und fasst die wichtigsten Erkenntnisse der Art 29 Richtlinie zusammen.

1. Wann müssen DSB bestellt werden?

In folgenden vier Fällen müssen DSB bestellt werden (Art 37 DSGVO):

1. Behörden (öffentliche Stellen) müssen immer DSB bestellen;
2. die „Kerntätigkeit“ von Verantwortlichen bzw Auftragsverarbeitern besteht in der umfangreichen, regelmäßigen, systematischen Überwachung von Betroffenen;
3. die Kerntätigkeit von Verantwortlichen bzw Auftragsverarbeitern besteht in der umfangreichen Verarbeitung „sensibler“ oder „strafrechtlich relevanter“ Daten;
4. wenn europäisches oder nationales Recht die Bestellung von DSB vorschreibt.

1.1 Was meint „Kerntätigkeit“?

Kerntätigkeit meint nach der Art-29-Datenschutzgruppe jene Tätigkeit, die der Verwirklichung der Ziele von Verantwortlichen dient. Bei Unternehmen wird dies idR der Unternehmensgegenstand sein. [3] Wenn die Zielverwirklichung nicht unmittelbar mit der Verarbeitung personenbezogener Daten verbunden ist, die Verarbeitung personenbezogener Daten aber untrennbarer Bestandteil der Tätigkeiten von Verantwortlichen ist, soll ebenfalls ein DSB bestellt werden müssen.

Beispiele:

Kerntätigkeit von Krankenhäusern ist die Erbringung von Gesundheitsdienstleistungen. Ohne die Verarbeitung personenbezogener Daten wäre dies nicht möglich. Daher ist die Verarbeitung personenbezogener Daten als Teil der Kerntätigkeit von Krankenhäusern zu erachteten. Krankenhäuser müssen somit DSB bestellen, weil sie umfangreich sensible Daten verarbeiten.

Sicherheitsunternehmen haben das „Ziel“, Eigentum zu schützen. Die Kerntätigkeit besteht dabei in einer Überwachung, welche nicht ohne die Verarbeitung personenbezogener Daten erfolgen könnte. Auch Sicherheitsunternehmen müssen daher DSB bestellen.

Kein DSB muss bestellt werden, wenn lediglich unterstützende Datenverarbeitungen, wie zB die Gehaltsabrechnung, durchgeführt werden.

1.2 Wann ist eine Überwachung systematisch oder regelmäßig?

Als regelmäßig erachtet die Art-29-Datenschutzgruppe jede Überwachung, die fortlaufend, in bestimmten Intervallen/für eine bestimmte Periode erfolgt oder die wiederkehrend ist.

Systematisch sind Überwachungen, die nach einem generellen Plan oder als Teil einer (Unternehmens-)Strategie erfolgen.

Beispiele für regelmäßige und systematische Überwachung: [4]

- Die Beurteilung der Kreditwürdigkeit,
- Durchführung verhaltensbezogener Werbung,
- Datenverarbeitung durch Smart Meter oder
- das Betreiben eines Telekommunikationsnetzwerkes.

1.3 Ab wann werden umfangreich „sensible“ oder strafrechtlich relevante Daten verarbeitet?

Bei der Auslegung des Begriffs „umfangreich“ sind der Art-29-Datenschutzgruppe nach folgende Faktoren entscheidend:

- Anzahl der Betroffenen;
- Anzahl unterschiedlicher Datenarten;
- Dauer der Datenverarbeitungstätigkeit;
- geographische Auswirkung der Datenverarbeitungstätigkeit.

Beispiele für umfangreiche Datenverarbeitungen: [5]

- die Verarbeitung von Patientendaten durch ein Krankenhaus;
- die Verarbeitung von Kundendaten durch ein Versicherungsunternehmen oder eine Bank oder
- die Verarbeitung von Daten durch einen Telefon- oder Internet Service-Provider.

Nicht umfangreich ist die Verarbeitung von Daten durch einen einzelnen Arzt oder einen einzelnen Anwalt. Mangels umfangreicher Verarbeitung müssen diese keinen DSB bestellen, selbst wenn sie „sensible“ bzw strafrechtlich relevante Daten verwenden.

Trifft keiner der vier Fälle zu, die zur Bestellung von DSB verpflichten, empfiehlt die Art-29-Datenschutzgruppe, diesen Umstand zu dokumentieren. Im Fall von Kontrollen durch Aufsichtsbehörden kann es notwendig sein, nachzuweisen, warum sämtliche Bestellungskriterien auf die eigene Organisation nicht zutreffen.

Wenn sich Unternehmen dazu entschließen, „freiwillig“ einen DSB zu bestellen, sind der Art-29-Datenschutzgruppe zufolge auch auf diese die entsprechenden Bestimmungen der DSGVO anwendbar, insbesondere die Regelungen zur Unabhängigkeit, dem Kündigungsschutz und der finanziellen Ausstattung von DSB. Wenn dies nicht gewünscht ist, sondern nur einzelne DSB-Funktionen von „freiwillig“ bestellten „DSB“ wahrgenommen werden sollen, sollten diese nicht als DSB bezeichnet, sondern sollte eine andere Bezeichnung (zB Verantwortlicher für Datenschutz) gewählt werden.

2. DSB in Konzernen

Unternehmensgruppen dürfen einen gemeinsamen DSB benennen, wenn dieser von jeder Niederlassung „leicht“ erreicht werden kann (Art 37 Abs 2 DSGVO).

Die leichte Erreichbarkeit bezieht sich der Art-29-Datenschutzgruppe nach darauf, dass die Kontaktdaten des DSB innerhalb des Konzerns Mitarbeitern und Betroffenen bekannt sind. Weiters darauf, dass der DSB die Sprache(n) von Mitarbeitern, Betroffenen und Aufsichtsbehörden versteht.

3. DSB bei Verantwortlichen und bei Auftragsverarbeitern

Verantwortliche und Auftragsverarbeiter müssen eigenständig beurteilen, ob ein DSB bestellt werden muss (Art 37 Abs 1 DSGVO). Dies kann dazu führen, dass nur der Verantwortliche, nicht aber ein herangezogener Auftragsverarbeiter einen DSB bestellen muss oder umgekehrt.

Beispiel:

Ein kleines Familienunternehmen, dessen „Kerntätigkeit“ der Verkauf von Haushaltsgegenständen in einer Kleinstadt ist, bedient sich für den Betrieb ihrer Webseite eines Auftragsverarbeiters. Das Familienunternehmen selbst ist nicht verpflichtet, einen DSB zu bestellen. Wenn aber der Auftragsverarbeiter eine Vielzahl ähnlicher Kunden hat, kann deshalb in Summe eine „umfangreiche“ Datenverwendung vorliegen, die den Auftragsverarbeiter zur Bestellung eines DSB verpflichtet.

4. Anforderungen an DSB

DSB müssen über ein Fachwissen verfügen, welches den Datenverarbeitungen der Organisation entspricht und die „Fähigkeit“ besitzen, die in der DSGVO genannten Aufgaben zu erfüllen (Art 37 Abs 5 DSGVO).

„Fähigkeit“ meint der Art-29-Datenschutzgruppe nach nicht nur die persönlichen Qualitäten und das Fachwissen, [6] sondern auch die Position von DSB innerhalb der Organisation. Diese muss es ihnen ermöglichen, Einfluss auf die Datenverarbeitungen des Unternehmens auszuüben.

5. Einbindung von DSB

DSB müssen „frühzeitig“ in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden werden (Art 38 Abs 1 DSGVO). Die Art-29-Datenschutzgruppe versteht darunter einerseits, dass DSB regelmäßig an Besprechungen der mittleren und obersten Führungsebene teilnehmen müssen, andererseits, dass ihnen auch Informationen frühzeitig zur Verfügung gestellt werden müssen.

Weil der Rat von DSB bei der Durchführung von Datenschutz-Folgenabschätzungen (Art 35 Abs 2 DSGVO) eingeholt werden muss, liegt es im Interesse von Verantwortlichen, DSB frühzeitig über Datenverarbeitungen zu informieren.

6. Ressourcen von DSB

DSB müssen mit den erforderlichen Ressourcen ausgestattet werden (Art 38 Abs 2 DSGVO). Die Art-29-Datenschutzgruppe versteht darunter, dass DSB finanzielle Unterstützung (Räumlichkeiten, Arbeitsmaterial und wenn notwendig Mitarbeiter) erhalten und über ausreichende Zeit zur Aufgabenerledigung verfügen.

Ausreichende Ressourcen bedeutet der Art-29-Datenschutzgruppe nach auch eine ausreichende Unterstützung durch die Führungsebene. Denn nur bei ausreichendem Rückhalt durch Führungskräfte erhalten DSB Zugang zu den notwendigen Informationen und Unterstützung durch Schlüsselmitarbeiter. Schließlich müssen Verantwortliche sicherstellen, dass DSB laufend fortgebildet werden.

7. Befugnisse von DSB

Bei Erfüllung ihrer Pflichten dürfen DSB keine Anweisungen erhalten, welche Ergebnisse erzielt werden sollen, wie mit Beschwerden umgegangen werden soll oder ob die Aufsichtsbehörde kontaktiert werden soll (Art 38 Abs 3 DSGVO). In Angelegenheiten, in denen die DSGVO DSB keine Kompetenzen zuweist, haben diese grundsätzlich keine Entscheidungsbefugnis.

Wollen Verantwortliche entgegen den Empfehlungen von DSB handeln, empfiehlt die Art-29-Datenschutzgruppe, die Gründe für das Abweichen zu dokumentieren. Weiters sollte DSB Gelegenheit gegeben werden, ihre abweichende Meinung zu begründen. Im Fall von Behördenanfragen kann so die Entscheidungsfindung nachgewiesen werden und dargelegt werden, dass eine ausreichende Auseinandersetzung mit dem Datenschutzrecht erfolgte.

8. Unabhängigkeit von DSB; Berichtslinie

DSB dürfen wegen Erfüllung ihrer Aufgaben nicht abberufen oder sonst benachteiligt werden (Art 38 Abs 3 DSGVO). Bereits die Androhung von Nachteilen kann der Art-29-Datenschutzgruppe nach einen Verstoß gegen die DSGVO darstellen, wenn die Drohung geeignet ist, die Unabhängigkeit von DSB zu beeinträchtigen. Als *Nachteil* nennt die Art-29-Datenschutzgruppe zB das Übergehen bei Beförderungen. Sollten DSB ihre Pflichten grob missachten, können diese selbstverständlich von ihrer Position abberufen werden.

Weil die DSGVO nicht regelt, unter welchen Umständen DSB abberufen werden können, sollten in Verträgen zur Bestellung von DSB die Umstände für eine Abberufung möglichst konkret geregelt werden. Dies schafft Klarheit für den DSB und sichert damit dessen Unabhängigkeit ab.

Sehr wichtig ist, den DSB in der Organisationsstruktur korrekt zu positionieren: nach Art 38 Abs 3 DSGVO muss er direkt an die höchste Managementebene berichten. Er darf daher in seiner Funktion etwa nicht unter dem Compliance-Verantwortlichen oder dem Leiter der Rechtsabteilung positioniert werden, sondern muss separat, zB als eigene „Stabsstelle“ ausgestattet werden, die im Organigramm eine Berichtslinie direkt zur Geschäftsführung oder dem Vorstand hat. [7]

9. Interessenskonflikte von DSB

DSB dürfen grundsätzlich weitere Funktionen ausüben (Art 38 Abs 6 DSGVO). Andere Pflichten dürfen aber nicht die Unabhängigkeit von DSB beeinträchtigen.

Die Art-29-Datenschutzgruppe rät, zum DSB inkompatible Funktionen zu identifizieren und Regelungen zur Verhinderung von Interessenskonflikten aufzustellen. Funktionen wie Leiter der Personalabteilung, Leiter der Marketingabteilung oder Leiter der IT-Abteilung sind als inkompatibel zum DSB zu erachten.

10. Verzeichnis von Verarbeitungstätigkeiten

Die Führung des Verzeichnisses von Verarbeitungstätigkeiten liegt in der Verantwortung des Verantwortlichen bzw des Auftragsverarbeiters – nicht des DSB (Art 30 Abs 1 DSGVO).

Die DSGVO regelt nur Mindestaufgaben von DSB, gestattet diesen aber zusätzliche Aufgaben wahrzunehmen. Da DSB in der Praxis ohnedies ein „Verzeichnis“ von Verarbeitungstätigkeiten führen werden, um ihre Aufgaben zu erfüllen, spricht der Art-29-Datenschutzgruppe nach nichts dagegen, dass DSB im Auftrag des Verantwortlichen bzw des Auftragsverarbeiters das Verzeichnis von Verarbeitungstätigkeiten für diesen führen.

11. Persönliche Verantwortung von DSB

Die Bestellung eines DSB befreit Verantwortliche nicht davor, die DSGVO einzuhalten. Laut Art-29-Datenschutzgruppe sind es ausdrücklich die Unternehmen und nicht die DSB, die für die Einhaltung der DSGVO verantwortlich sind.

Da DSB grundsätzlich keine über die in Art 39 DSGVO geregelten Befugnisse hinausgehenden Entscheidungsbefugnisse haben, werden DSB uE nicht als „verantwortliche Beauftragte“ nach § 9

Verwaltungsstrafgesetz bestellt werden können. [8] Eine solche Benennung würde wohl auch gegen die Regelung der DSGVO verstoßen, wonach andere Aufgaben und Pflichten von DSB nicht zu einem Interessenkonflikt führen dürfen.

Für Verstöße gegen die DSGVO müssen somit die jeweiligen datenverarbeitenden Organisationen Verantwortung übernehmen. Wie genau sich der DSGVO-Strafrahmen von bis zu 20 Mio Euro bzw 4 Prozent des weltweiten Jahresumsatzes in das österreichische Verwaltungsstrafrecht fügen soll, ist noch ungeklärt. Das Verwaltungsstrafgesetz sieht nämlich vor, dass die zur Vertretung nach außen Berufenen eines Unternehmens, also der Vorstand, die Geschäftsführer oder persönlich haftende Gesellschafter strafrechtlich verantwortlich sind (§ 9 Abs 1 VStG). Die DSGVO zielt mit ihrem Strafrahmen aber ganz offensichtlich auf das Unternehmen selbst und nicht auf dessen Organe ab, weil zu befürchten steht, dass Unternehmen sonst – ähnlich dem Phänomen der sogenannten „Sitzredakteure" in Printmedien – möglicherweise „entbehrliche" Personen als „Sündenböcke" einsetzen, um die Last der Strafe vom Unternehmen auf austauschbare Personen zu verschieben. [9]

12. Zusammenfassung

Unternehmen, die DSB bestellen (müssen), werden diese eine wertvolle Unterstützung und ein Wettbewerbsvorteil [10] im Zusammenhang mit der Herstellung von DSGVO-Compliance sein. Die Verantwortung – und die laufende Arbeit – zur Einhaltung der DSGVO bleibt aber bei den „Datenverarbeitern". Diese sind es, die im Fall eines Verstoßes gegen die DSGVO mit empfindlichen Strafen rechnen müssen. DSB sollten daher weder als Feigenblatt missverstanden werden, noch als diejenigen, die für das Unternehmen die tägliche Datenschutzarbeit erledigen, um dieses von Risiko und Haftung zu befreien, sondern als kompetente Berater und Überprüfer geschätzt werden.

Fußnoten

[1] Bei der Artikel-29-Datenschutzgruppe handelt es sich um eine unabhängige Gruppe von Vertretern der Kontrollstellen der Mitgliedstaaten, welche durch Art-29-Datenschutz-RL eingesetzt wurde.
[2] Artikel-29-Datenschutzgruppe 13. 12. 2016, WP 243 (Guidelines on Data Protection Officers).
[3] Laut Erwägungsgrund 97 DSGVO bezieht sich die Kerntätigkeit im privaten Sektor auf die Haupttätigkeit und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit (siehe *Pollirer/Weiss/Knyrim/Haidinger,* DSGVO [2017] 101).
[4] *König* , Der Datenschutzbeauftragte, in *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (2016) 235, nennt hier als Beispiele: Kreditauskunfteien; Banken; Versicherungen; Unternehmen, die Bewertungsplattformen und Vergleichsportale betreiben, Big-Data-Analysten; IT-Dienstleister.
[5] *König* , Der Datenschutzbeauftragte, in *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (2016) 235, nennt hier neben Krankenhausträgern als weiteres Beispiel Anbieter von Untersuchungen von DNA-Proben.
[6] *König* , Der Datenschutzbeauftragte, in *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (2016) 238, empfiehlt – in Anlehnung an die DSG-Novelle 2012, die nicht Gesetz wurde – im ersten Jahr (zumindest) 40 Stunden Fortbildung zu ermöglichen, in den Folgejahren (zumindest) 20 Stunden.
[7] *König* , Der Datenschutzbeauftragte, in *Knyrim* (Hrsg.), Datenschutz-Grundverordnung, 238, nennt im Vorstand der AG als Berichtsempfänger beispielhaft den Chief Executive Officer oder den Chief Risk Officer, bei öffentlichen Einrichtungen den Minister, Bürgermeister oder Landeshauptmann.
[8] Auch *König* , Der Datenschutzbeauftragte, in *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (2016) 238, sieht hier einen Interessenkonflikt.
[9] Siehe dazu auch *Illibauer* , Geldbußen und andere Sanktionen, in *Knyrim* (Hrsg.), Datenschutz-Grundverordnung (2016) 344.
[10] Artikel-29-Datenschutzgruppe, Stellungnahme zur Datenschutzreform vom 15. 6. 2015, 21f (http://ec.europa.eu/justice/data-...appendix_core_issues_plenary_de.pdf).

Die Autoren

DI Michael Löffler

DI Michael Löffler, Wirtschaftsingenieur Informatik, Knyrim Trieb Rechtsanwälte;2008 – 2014 Bearbeitung von Rechtsfragen im Bereich Datenschutz und IT-Recht bei e-commerce monitoring GmbH, 2014 – 2016 juristischer Mitarbeiter bei Preslmayr Rechtsanwälte; seit 2017 juristischer Mitarbeiter bei Knyrim Trieb Rechtsanwälte.

Dr. Rainer Knyrim

RA Dr. Rainer Knyrim, Parnter, Knyrim Trieb Rechtsanwälte 2003 – 2016 Partner bei Preslmayr Rechtsanwälte; seit 01/2017 Partner von Knyrim Trieb Rechtsanwälte; Chefredakteur der Zeitschrift “Datenschutz konkret”, Autor des „Praxishandbuchs Datenschutzrecht“, Herausgeber von „Datenschutz-Grundverordnung – Das neue Datenschutzrecht in Österreich und der EU“ und Mitherausgeber des „Kommentars zum Datenschutzrecht“.