2/2017
25 – 48

KURZMELDUNG
DSGVO-Strafen
Viktoria Haidinger

DATENSCHUTZ KONKRET

Recht | Projekte | Lösungen

Chefredaktion: Rainer Knyrim

Datenschutz-Management

Das Problem liegt oft im Detail
Interview mit Maximilian Wellner und Simone Holz, Datenschutzexperten bei Greiner Holding

Praxisprojekt: Datenschutz-Management-System bei den ÖBB
Martin Leiter/Hans-Jürgen Pollirer

Compliance am Beispiel Datenschutz
Markus Oman/Robert Reitmann/Siegfried Gruber

DSGVO: Benötigt Ihr Unternehmen einen Datenschutzbeauftragten?
Thomas Schweiger

Checkliste Löschkonzept
Hans-Jürgen Pollirer

Zielgerichtete Werbung in sozialen Netzwerken
Julia Spitzbart/Ermano Geuer

Auskunftsrecht – Ablehnung der Auskunft
Andreas Schweitzer

ISSN 2313-5409

dako.manz.at

MANZ

Österreichische Post AG Info.Mail Entgelt bezahlt Retouren an Verlag Manz, Gutheil Schoder Gasse 17, 1230 Wien

Thomas Schweiger
Rechtsanwalt Schweiger & Partner Rechtsanwälte OG

Benötigt Ihr Unternehmen ab 25. 5. 2018 einen Datenschutzbeauftragten?

Das künftige EU-Datenschutzrecht – Teil 10. Nicht die Größe des Unternehmens oder die Anzahl der Datensätze ist entscheidend für die Bestellung eines Datenschutzbeauftragten (DSB), sondern die Kerntätigkeit des Unternehmens, die Art der Datenverarbeitung und die Art der verarbeiteten Daten. Der Beitrag untersucht diese Kriterien und führt typische Beispiele von Unternehmen dafür an.

Allgemeines

Ein Unternehmen, welches personenbezogene Daten verarbeitet, benennt einen DSB, wenn die *„**Kerntätigkeit** […] 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 […] in der **umfangreichen Verarbeitung besonderer Kategorien von Daten** […] besteht“* (Art 37 Abs 1 lit b und c DSGVO).

Diese Verpflichtung wird durch die DSGVO für das österr Recht in Art 37 mit 25. 5. 2018 neu eingeführt. **Nicht** die **Größe des Unternehmens** oder die **Anzahl der Datensätze** ist **entscheidend** für die Bestellung eines DSB (*„250 Mitarbeiter“* im Entwurf 2012; *„5.000 betroffene Personen“*[1] im Entwurf 2014), sondern

- die **Kerntätigkeit** des Unternehmens,
- die **Art der Datenverarbeitung** und
- die **Art der verarbeiteten Daten** (in der Folge „bestellungsrelevante Datenverarbeitung“).

Aufgrund einer **Öffnungsklausel**[2] kann Österreich zusätzliche Möglichkeiten zur Bestellung eines DSB vorsehen.[3] Die Artikel-29-Datenschutzgruppe hat sich in einer Richtlinie auch mit DSB[4] befasst.

Ausgangspunkt der Beurteilung ist das unternehmerische Tun.

Kerntätigkeit

Die bestellungsrelevante Datenverarbeitung muss die **„Kerntätigkeit“** des Unternehmens darstellen, um die Verpflichtung zur Bestellung eines DSB zu begründen. Eine Aussage dazu findet sich nur in ErwGr 97 DSGVO: *„Im privaten Sektor bezieht sich die Kerntätigkeit eines Verantwortlichen auf seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit.“*

Entscheidend ist die **Haupttätigkeit** eines Unternehmens: Wenn es **unbedingt notwendig** ist, personenbezogene Daten zu verarbeiten, um die Haupttätigkeit des Unternehmens auszuüben, dann stellt auch die Datenverarbeitung eine Haupttätigkeit dar. Eine weitere Anknüpfungsmöglichkeit ist der Marktauftritt und der mit der konkreten Tätigkeit generierte Umsatz.[5]

Ausgangspunkt der Beurteilung ist das **unternehmerische Tun** selbst. Der Zweck

[1] www.datenschutz-grundverordnung.eu/grundverordnung/art-35-ds-gvo/?action=discussion (19. 11. 2016). [2] Vgl zum deutschen Recht *Härting*, Datenschutz-Grundverordnung, Das neue Datenschutzrecht in der betrieblichen Praxis (2016) Rz 10, bzw www.datenschutzverein.de/wp-content/uploads/2016/11/2016–11-11_DSAnpUG-EU-BDSG-neu_Entwurf-2_Ressortabstimmung.pdf (28. 11. 2016). § 36 Abs 1 geht von einer „10-Personen-Regel“ aus, dh, dass in der Regel mindestens zehn Personen ständig mit der Verarbeitung personenbezogener Daten beschäftigt sind. [3] Siehe Art 37 Abs 4 DSGVO. Zum Zeitpunkt der Erstellung dieses Beitrags lag noch kein Umsetzungsgesetz in Österreich vor. [4] Guidelines on Data Protection Officers (DPOs); http://ec.europa.eu/information_society/newsroom/image/document/2016–51/wp243_en_40855.pdf. [5] Horn, Die neue Rolle des Datenschutzbeauftragten nach der DSGVO, jusIT 2016, 196.

der unternehmerischen Tätigkeit ist zu analysieren, um daraus abzuleiten, ob eine Kerntätigkeit eine bestellungsrelevante Datenverarbeitung umfasst. ME ist zu unterscheiden, ob das „unternehmerische Tun" (die Geschäftsprozesse) von der besonderen personenbezogenen Datenverarbeitung abhängig ist, dh ohne diese Datenverarbeitung die Tätigkeit des Unternehmens ausgeübt werden kann, oder die bestellungsrelevante Datenverarbeitung die definierten Geschäftsprozesse (lediglich) unterstützt.

Beispiele

Die Verwaltung der personenbezogenen Daten von Mitarbeitern stellt per se meistens keine Haupttätigkeit eines Produktions- oder Dienstleistungsunternehmens dar. Bei einem **Personalleasingunternehmen** jedoch, das ua die Personaldaten der Mitarbeiter verwendet, um diese Mitarbeiter am Markt als Arbeitskräfte anbieten zu können, wird auch die „Mitarbeiterdatenverwaltung" eine Haupttätigkeit darstellen.[6]

Die Tätigkeit einer **Rechtsanwaltskanzlei** umfasst als Haupttätigkeit die rechtliche Vertretung und Beratung von Personen; dabei werden personenbezogene, uU auch strafrechtlich relevante Daten oder auch Gesundheitsdaten (zB die SVNR[7]) automationsunterstützt verarbeitet. Diese Datenverarbeitung ist jedoch nur unterstützend.[8]

Eine **Pflegeeinrichtung** muss ua auch Gesundheitsdaten verarbeiten, um die Pflegeleistung ordnungsgemäß erbringen zu können. Die Datenverarbeitung ist mE als Haupttätigkeit anzusehen. In diesem Sinne geht auch *König* davon aus, dass zB bei einem **Personalverrechner** oder einem **Dienstleister**, der **Videoüberwachungen** anbietet, eine Kerntätigkeit in der Verarbeitung von Daten besonderer Kategorien gegeben ist.[9]

Umfangreich

Die bestellungsrelevante Datenverarbeitung muss „umfangreich" sein, wobei sich dazu keine Definition in der DSGVO findet. Aus ErwGr 91 ergibt sich ein Anhaltspunkt zur Interpretation dieses Tatbestandsmerkmals, wobei dieser sich mit der Datenschutz-Folgenabschätzung befasst, sodass er für die Auslegung des Worts „umfangreich" iZm der Bestellung eines DSB mE nur bedingt aussagekräftig ist.

Neue Technologien mit hohem Risiko für den Datenschutz bewirken nicht per se, dass die Datenverarbeitung als umfangreich zu beurteilen ist.

„Umfangreich" ist eine Datenverarbeitung, wenn eine **große Menge personenbezogener Daten**[10] verarbeitet wird oder die Daten eine **große Anzahl von Personen** (ErwGr 91 DSGVO) betreffen. Die Verarbeitung von Daten mit hohem Risiko (bspw aufgrund von neuen Technologien) für die Rechte und Freiheiten der betroffenen Personen bewirkt nicht per se, dass die Datenverarbeitung als umfangreich zu beurteilen ist. Es findet sich in ErwGr 91 eine **Negativabgrenzung** dahingehend, dass eine Datenverarbeitung durch Einzelpersonen (zB von Patientendaten) nicht als umfangreich gilt.

Beispiele

Die Art-29-Datenschutzgruppe geht davon aus, dass ua folgende (umfangreiche) Verarbeitungen die Verpflichtung zur Bestellung auslösen können:[11]

- Verarbeitung von **Patientendaten** oder **Kundendaten** im gewöhnlichen Geschäftsverkehr durch eine Krankenanstalt, Bank oder Versicherung;
- Verarbeitung von **Verkehrsstromdaten** von Personen, die ein öffentliches Verkehrsmittel verwenden (zB durch das Tracking von Netzkarten);
- Verarbeitung von personenbezogenen Daten für **verhaltensbasierte Werbung** durch eine Suchmaschine oder von **Inhalts-, Verkehrs- oder ortsbezogenen Daten** durch einen Telefon- oder Internetdiensteanbieter;
- Aufzeichnung von Fitnessdaten mittels tragbarer Geräte oder auch Internet-of-Things-Anwendungen mit Smart Devices (zB Stromzähler).

Die Art der Datenverarbeitung („Überwachung")

Die **konkrete Art der Datenverarbeitung** führt dazu, dass ein DSB zu bestellen ist. Wenn die Kerntätigkeit des Unternehmens in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige und systematische Überwachung**[12] **von betroffenen Personen** erforderlich machen, ist ein DSB zu bestellen (Art 37 Abs 1 lit b DSGVO).

Regelmäßig ist die Überwachung dann, wenn sie laufend oder wiederkehrend stattfindet; **systematisch**, wenn die Überwachung unter Verwendung eines technischen Systems, vorbereitet, organisiert oder methodisch, im Rahmen einer generellen Datenerhebung oder als Teil einer generellen Strategie erfolgt.[13]

Die **umfangreiche Überwachung** muss nicht der (konkrete) Zweck der Datenverarbeitung sein, sondern muss erforderlich sein, um die Verarbeitungsvorgänge durchführen zu können. Eine derartige Datenverarbeitung wird zB von **Security-Unternehmen** durchgeführt oder von **Dienstleistern**, die **GPS-Daten** aufzeichnen und für andere auswerten.

Beispiele

Eine **Bank** wickelt Zahlungsvorgänge elektronisch unter Zuhilfenahme von Datenverarbeitungsvorgängen ab, dh, sie führt Verarbeitungsvorgänge durch; dies umfasst eine der Kerntätigkeiten der Bank, da es üblich ist, die Leistungen dem Kunden in elektronischer Form (zB E-Banking, Apps) zur Verfügung zu stellen. Um diese Tätigkeit durchführen zu können, ist es nach Art (Einhaltung gesetzlicher Vorschriften), Umfang (große Anzahl von Daten betroffener Personen) und Zweck (Vertraulichkeit der Zahlungsvorgänge) nötig, die Zugriffe zu protokollieren.

Auch **Wirtschaftsauskunfteien**, **Rating-Agenturen**, **Versicherungen**, **Vergleichs-** oder **Bewertungsportalbetreiber**, **Unternehmen**, die **Big-Data auswerten**, oder **Cloud-Dienstleister** sind zur Bestellung eines DSB verpflichtet.

[6] IdS auch *König*, Der Datenschutzbeauftragte, in *Knyrim* (Hrsg), Datenschutz-Grundverordnung (2016) 234 ff. [7] Siehe ErwGr 35 DSGVO *„Zu den personenbezogenen Gesundheitsdaten […] gehören auch […] Nummern, Symbole oder Kennzeichen, die einer natürlichen Person zugeteilt wurden, um diese natürliche Person für gesundheitliche Zwecke eindeutig zu identifizieren."* [8] Vgl auch *Härting*, Datenschutz-Grundverordnung Rz 7. [9] Vgl *König* in *Knyrim* (Hrsg), Datenschutz-Grundverordnung 235. [10] Siehe Guidelines on Data Protection Officers (DPOs) 7. [11] Siehe Guidelines on Data Protection Officers (DPOs) 7. [12] Der englische Text verwendet den Begriff: *„monitoring"* (http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN; 19. 11. 2016). *König* in *Knyrim* (Hrsg), Datenschutz-Grundverordnung 234, verwendet den Begriff „Beobachtung". [13] Siehe Guidelines on Data Protection Officers (DPOs) 8.

Ein **Maschinenbauer** oder ein **durchschnittlicher Onlinehändler** eher nicht.[14]

Die Art der verarbeiteten Daten (Verarbeitung sensitiver Daten)

Es ist zu analysieren, welche **konkreten Datenarten** das Unternehmen verarbeitet. Folgende Datenarten sind für die Bestellung eines DSB entscheidend:

- besondere Kategorien von Daten (Art 9 DSGVO):
  - Daten über die rassische und ethnische Herkunft
  - Daten über politische Meinungen, religiöse, weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit
  - genetische Daten, biometrische Daten zur eindeutigen Identifizierung
  - Gesundheitsdaten, Daten zum Sexualleben oder zur sexuellen Orientierung
- Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßregeln (Art 10 DSGVO)

Es reicht jedoch nicht aus, dass derartige Daten im Unternehmen verarbeitet werden, denn dann wäre jedes Unternehmen, das Mitarbeiterdaten mit dem Religionsbekenntnis verarbeitet, dazu verpflichtet, einen DSB zu bestellen. Wie bereits oben beschrieben ist es notwendig, dass die Verarbeitung dieser (besonderen) Datenarten die „Kerntätigkeit" des Unternehmens darstellt und umfangreich ist.

Fazit & Konsequenz

Die Notwendigkeit der Bestellung eines DSB ergibt sich aus der „Kerntätigkeit" eines Unternehmens sowie aus den verarbeiteten besonderen Datenarten bzw aus der Art der Tätigkeit, sofern diese eine Überwachung von Personen erforderlich macht. Dazu ist eine gründliche Analyse der Tätigkeit sowie der Datenanwendungen notwendig. Es wird in manchen Fällen Abgrenzungsschwierigkeiten geben, insb wenn zu entscheiden ist, ob die Datenverarbeitung „umfangreich" ist. Viele Unternehmen werden wegen ihrer Branchenzugehörigkeit und Größe mit hoher Wahrscheinlichkeit einen DSB bestellen müssen, zB Banken, Versicherungen, private Krankenanstalten, Pflegeeinrichtungen oder bestimmte IT-Dienstleister.

Wenn ein Unternehmen der Verpflichtung zur „Benennung" nach Art 37 DSGVO nicht nachkommt, droht eine **Geldbuße** in Höhe von 10 Mio Euro oder bis zu 2% des gesamten erzielten weltweiten Jahresumsatzes des vorangegangenen Geschäftsjahrs – je nachdem, welcher Betrag höher ist (Art 83 Abs 4 lit a DSGVO).

PRAXISTIPPS

- **Dokumentation**

Auch die Art-29-Datenschutzgruppe ist der Ansicht, dass jedenfalls dokumentiert werden sollte, aus welchen Gründen ein Unternehmen davon ausgeht, dass die Bestellung eines DSB nicht notwendig ist, um gegenüber der Aufsichtsbehörde darlegen zu können, dass die wesentlichen Umstände bei der Beurteilung berücksichtigt wurden.[15] Es sollten sich daher alle Unternehmen mit dieser Frage auseinandersetzen, den relevanten Sachverhalt analysieren sowie diesen Vorgang und auch die Entscheidung, warum ein DSB bestellt wird oder nicht, dokumentieren.

- **Benennung eines nicht verpflichtenden DSB**

Wenn ein Unternehmen der Ansicht ist, dass kein DSB (verpflichtend) zu bestellen ist, und dennoch aus organisatorischen Gründen in der eigenen Organisation jemanden benennt, der die Aufgaben eines DSB übernimmt, dann sollte diese Person nicht als DSB (iSd DSGVO) bezeichnet werden, da damit auch die Verpflichtungen verbunden wären, die sich aus der DSGVO ergeben. Die Person könnte zB als Datenschutzmangager/in bezeichnet werden, und es sollte klargestellt werden, dass diese Person kein DSB iSd DSGVO ist.[16]

Dako 2017/20

[14] Vgl *Härting*, Datenschutz-Grundverordnung Rz 9. [15] Siehe Guidelines on Data Protection Officers (DPOs) 5. [16] Siehe Guidelines on Data Protection Officers (DPOs) 5.

Zum Thema

Über den Autor

Dr. Thomas Schweiger, LL.M. (Duke), ist Rechtsanwalt bei SMP Schweiger Mahr & Partner Rechtsanwälte OG in Linz.
Tel: +43 (0)732 79 69 00-0
E-Mail: office@s-m-p.at
Internet: www.s-m-p.at, www.it-recht.at, www.dataprotect.at

Hinweis

Dieser Beitrag ist der 10. Teil der Serie zum künftigen EU-Datenschutzrecht. Bisher erschienen sind:

- ***Knyrim*, Die Datenschutz-Grundverordnung: Entwicklung und Anwendungsbereich, Dako 2015/21;**
- ***Pollirer*, Die Datenschutz-Grundverordnung: Der Datenschutzbeauftragte, Dako 2015/37;**
- ***Pollirer*, Die Datenschutz-Grundverordnung: Die Datenschutz-Folgenabschätzung, Dako 2015/47;**
- ***Wagner*, Die Datenschutz-Grundverordnung: Die Betroffenenrechte, Dako 2015/59;**
- ***Knyrim*, Die Datenschutz-Grundverordnung: Die neuen Pflichten, Dako 2016/6;**
- ***Leissler/Wolfbauer*, Die Datenschutz-Grundverordnung: Das „One-Stop-Shop"-Prinzip, Dako 2016/23;**
- ***Haidinger*, Geltendmachung der Betroffenenrechte und das Auskunftsrecht nach der Datenschutzgrundverordnung, Dako 2016/73;**
- ***Oman*, Die Handhabung von Datenpannen iSd DSGVO, Dako 2017/3;**
- ***Pilgermair*, Datenschutz-Grundverordnung: Der neue Kinderschutz, Dako 2017/4.**