SCHLÄGER • THODE (Hrsg.)

Handbuch Datenschutz und IT-Sicherheit

Leseprobe, mehr zum Werk unter www.ESV.info/17727

ESV ERICH SCHMIDT VERLAG

datenschutz nord GRUPPE

ESV ERICH SCHMIDT VERLAG

Handbuch Datenschutz und IT-Sicherheit

Herausgegeben von
Dr. Uwe Schläger und Jan-Christoph Thode

Unter Mitarbeit von
Dr. Christian Borchers, Conrad S. Conrad, Michael Cyl, Dr. Sebastian Ertel, Annika Freund, Clemens Grünwald, Jennifer Jähn, Dr. Irene Karper, Jan-Roman Kitzinger, Dr. Martin Klein-Hennig, Martin Kolodziej, Dr. Bettina Kraft, Dr. Sönke Maseberg, Dr. Britta Mester, Lars Meyer, Dr. Sanela Hodžić , Lea Paschke, Jan Peplow, Olaf Rossow, Jan Schirrmacher, Dr. Uwe Schläger, Felix Schmidt, Markus Schönmann, Stefan R. Seiter, Daniel Stolper, Oliver Stutz, Jan-Christoph Thode, Sven Venzke-Caprarese, Ralf von Rahden

ERICH SCHMIDT VERLAG

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Weitere Informationen zu diesem Titel finden Sie unter
ESV.info/978 3 503 17727 1

Gedrucktes Werk: ISBN 978 3 503 17727 1
eBook: ISBN 978 3 503 17728 8

Dieses Papier erfüllt die Frankfurter Forderungen der Deutschen Nationalbibliothek und der Gesellschaft für das Buch bezüglich der Alterungsbeständigkeit und entspricht sowohl den strengen Bestimmungen der US Norm Ansi/Niso Z 39.48-1992 als auch der ISO-Norm 9706.

Satz: schwarz auf weiß, Herrig & Schimschok, Berlin
Druck und Bindung: Hubert & Co., Göttingen

Vorwort

Am 25. Mai 2018 ersetzt die EU-Datenschutz-Grundverordnung das bisherige Bundesdatenschutzgesetz. Nach jahrelanger Diskussion wird damit europäisches Datenschutzrecht endlich harmonisiert, sehr zum Vorteil international tätiger Unternehmen, aber auch zum Vorteil kleinerer Online-Shops, die sich bislang innerhalb der EU nach den jeweils geltenden nationalen Datenschutzvorschriften richten mussten.

Trotz der Harmonisierung kommen auf Unternehmen neue Herausforderungen zu: Neben erweiterten Informations-, Rechenschafts- und Meldepflichten gilt es, für Verfahren mit hohen Risiken für die Persönlichkeitsrechte der Betroffenen eine Datenschutz-Folgenabschätzung durchzuführen. Auftragsverarbeiter müssen künftig ebenso wie Verantwortliche ein Verzeichnis von Verarbeitungstätigkeiten führen. Auch die Eignung technischer und organisatorischer Sicherheitsmaßnahmen muss künftig regelmäßig überprüft und dokumentiert werden. Ganz zu schweigen von den deutlich erweiterten und erhöhten Bußgeldern, die künftig von Datenschutz-Aufsichtsbehörden verhängt werden können.

Die mit der Datenschutz-Grundverordnung verbunden Neuerungen sollten für Unternehmen, die sich bislang konform zum Bundesdatenschutzgesetz aufgestellt haben, kein besonderes Problem darstellen. Wer bislang seine datenschutzrechtlichen Hausaufgaben erledigt hat, kann auf bestehenden Datenschutzstrukturen aufbauen, muss diese allerdings an einigen Stellen anpassen und gegebenenfalls erweitern. Unternehmen mit gravierenden Datenschutzdefiziten, die in der Vergangenheit eher darauf vertraut haben, nicht negativ aufzufallen, drohen allerdings nunmehr drastische Bußgelder.

Und hier setzt unser neues Datenschutz-Handbuch an: Wir, dies sind erfahrene Beraterinnen und Berater der datenschutz nord Gruppe, die seit Jahren in den Bereichen Datenschutz und Informationssicherheit als Consultant tätig sind, haben für Sie ein Datenschutz-Handbuch erstellt, das zum einen auf die neuen gesetzlichen Regelungen der Datenschutz-Grundverordnung im Detail eingeht. Zum anderen stellen wir Ihnen Best-Practice-Ansätze vor, wie den neuen gesetzlichen Vorgaben am besten entsprochen werden kann.

Das vorliegende Datenschutz-Handbuch richtet sich an betriebliche Datenschutzbeauftragte, IT-Administratoren, Unternehmensleitungen, Betriebs- oder Personalräte, aber auch an datenschutzinteressierte Beschäftigte und Kunden, die sich entweder einen Überblick über die neuen gesetzlichen Regelungen verschaffen wollen oder praxisgerechte Vorschläge zur Umsetzung der Datenschutz-Grundverordnung nachlesen möchten.

Das Datenschutz-Handbuch gliedert sich im Wesentlichen in zwei Hauptteile: Die Kapitel A bis F sind datenschutzrechtlich geprägte Kapitel, während die Kapitel G

bis J sicherheitstechnische Aspekte in den Vordergrund stellen. Nachdem wir in Kapitel A zunächst auf die neuen datenschutzrechtlichen Grundlagen eingehen, stellen wir in Kapitel B vor, wie ein betriebliches Datenschutz-Management umgesetzt werden sollte. In Kapitel C steht die gesetzeskonforme Verarbeitung von Beschäftigtendaten im Vordergrund, in Kapitel D die gesetzeskonforme Verarbeitung von Kundendaten. Kapitel E beschäftigt sich mit der Verarbeitung personenbezogener Daten im Internet, in sozialen Netzwerken und in unternehmenseigenen Intranets. Kapitel F stellt dar, in welchem Umfang Videosysteme nach der neuen Datenschutz-Grundverordnung betrieben werden können.

Der zweite Hauptteil des Handbuches beginnt in Kapitel G mit einer Darstellung der rechtlichen Grundlagen der IT-Sicherheit. In Kapitel H werden die Eckpfeiler eines Informationssicherheits-Managements beschrieben. Kapitel I stellt geeignete technisch-organisatorische Maßnahmen vor, und zwar übergreifende Maßnahmen, Infrastrukturmaßnahmen, Maßnahmen seitens der IT-Systeme, Netzwerkmaßnahmen und Maßnahmen auf Anwendungsebene. Und schließlich wird in Kapitel J beschrieben, in welcher Form Penetrationstest zur Evaluierung einer angemessenen IT-Sicherheit durchgeführt werden können.

Trotz der zahlreichen Verweise auf andere Kapitel dieses Buches sind sämtliche Hauptkapitel in sich abgeschlossen und können separat ohne Kenntnis der anderen Kapitel als Erkenntnisquelle dienen.

In diesem Sinne wünschen wir Ihnen als Herausgeber dieses Datenschutz-Handbuchs viel Spaß beim Lesen und Nachschlagen.

Bremen und Berlin, im Januar 2018

Uwe Schläger und
Jan-Christoph Thode

Inhaltsverzeichnis

TEIL B

Datenschutzmanagement im Unternehmen

Aus: Dr. Uwe Schläger und Jan-Christoph Thode,
Handbuch Datenschutz und IT-Sicherheit

1. Der betriebliche Datenschutzbeauftragte

Der betriebliche Datenschutzbeauftragte hat in den letzten Jahrzehnten gerade im Hinblick auf die dauerhaft unterbesetzten Aufsichtsbehörden im deutschen Datenschutz eine herausragende Rolle als innbetriebliches bzw. innerbehördliches Instrument des Datenschutzmanagements erlangt. Dabei ist die „Figur" des Datenschutzbeauftragten keine rein deutsche Erfindung – sie ist (vermutlich) nur aus unserer Sicht mehr und besser geeignet, Datenschutz in Unternehmen umzusetzen, als es behördliche Kontrollen, Anhörungen und Bußgelder vermögen. Das mag aber auch an der Art und Weise der Aufgabenwahrnehmung der Aufsichtsbehörden liegen, die, das darf aus vielen Jahren Erfahrung gesagt werden, häufig (Ausnahmen bestätigen auch hier die Regel!) eher an der dogmatischen Durchsetzung von Gesetzesnormen als an praxisnahen Lösungen interessiert sind – wenn diese nicht in jeder Hinsicht einer wortlautkonformen Umsetzung der Normen entsprechen. *1*

Aus Sicht jedes Datenschutzbeauftragten, ganz gleich ob die Aufgabe intern, in Voll- oder Teilzeit oder extern wahrgenommen wird, sollte daher – durchaus in Abgrenzung und auch zum Teil als Korrektiv gegenüber dem Prüfungsansatz der zuständigen Aufsichtsbehörden – Datenschutz mit Augenmaß angestrebt werden. Eine in jeder Hinsicht über das ganze Unternehmen, alle Abteilungen hinweg und ggfls. sogar konzernweit 100%ige Einhaltung und Erfüllung sämtlicher Datenschutzanforderungen ist aus Praktiker-Sicht nahezu unerreichbar. Daher werden in diesem Buch als zentraler Maßstab Best-Practice-Ansätze vorgestellt und erläutert – diesen ist die Eigenschaft des Kompromisses immanent – des Kompromisses zwischen dem, was rechtlich geboten und was innerbetrieblich und vor allem auch finanziell machbar und möglich ist. *2*

1.1. Bestellpflicht

1.1.1. Europarechtliche Regelung mit nationaler Öffnungsklausel

Lange Zeit war in den Beratungen zwischen Kommission, Rat und Parlament umstritten, ob und unter welchen Voraussetzungen überhaupt eine obligatorische Bestellung eines Datenschutzbeauftragten in den Gesetzestext aufgenommen werden sollte. Der Verordnungsgeber hat, das zeigen u.a. die Erwägungsgründe, die Bestellung eines Datenschutzbeauftragten auch nur als quasi ultima-ratio für besonders „riskante bzw. intensive, risikobehaftete" Verarbeitungen verstanden: Zentrales Instrument der internen Datenschutzkontrolle soll nach dem Verständnis und auch nach dem Kontext der Regelungen zunächst die Datenschutz-Folgenabschätzung (Art. 35) sein[1]. Erst wenn dieses Kontrollinstrument, welches ja ohnehin erst *3*

1 Vgl. dazu unten Rn. 104 ff.

bei einem vermuteten hohen Risiko der Verarbeitung für die persönlichen Rechte und Freiheiten durchzuführen ist, nicht mehr ausreicht, soll „in jedem Fall" – so die für eine Rechtsnorm ungewöhnliche Formulierung – ein Datenschutzbeauftragter bestellt werden.

4 Die Überlegungen, unter welchen Voraussetzungen dies geschehen soll, reichten während der Beratungen von Mindestumsätzen der verantwortlichen Stellen bis hin zur Festlegung bestimmter Unternehmensgrößen, die mithilfe der Mitarbeiter-Anzahl bestimmt werden sollten (250 Mitarbeiter/500 Mitarbeiter u.Ä.). Geeinigt hat man sich nun auf die nachfolgend genannten Voraussetzungen, die, um es offen zu sagen, wenig praxisnah sind, da die Kriterien so allgemein formuliert sind, dass hierunter verschiedenste Tätigkeiten subsumiert werden können – oder auch nicht.

5 Auch wird in den Formulierungen und vor allem der Öffnungsklausel in Abs. 4 deutlich, dass bis zum Schluss Uneinigkeit bei den Beratungen herrschte, ob die Grundverordnung die Voraussetzungen für die Bestellungen eines Datenschutzbeauftragten abschließend regeln sollte. Im Ergebnis hat der deutsche Gesetzgeber von der Möglichkeit der Öffnungsklausel in Art. 37 Abs. 4 DSGVO mit § 38 BDSG-neu Gebrauch gemacht und letztlich die bisherige Regelung beibehalten:

> „... benennen der Verantwortliche und der Auftragsverarbeiter eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten, soweit sie in der Regel mindestens **zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigen**. Nehmen der Verantwortliche oder der Auftragsverarbeiter Verarbeitungen vor, die einer Datenschutz-Folgenabschätzung nach **Artikel 35** der Verordnung (EU) 2016/679 unterliegen, oder verarbeiten sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung, haben sie unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen eine Datenschutzbeauftragte oder einen Datenschutzbeauftragten zu benennen."

6 Wie ist bei der Prüfung, ob ein Datenschutzbeauftragter (überhaupt) bestellt werden muss, nun vorzugehen? Die Prüfungsreihenfolge ist letztlich durch den Gesetzeswortlaut vorgegeben: Zunächst sind die Bestellpflichten des Art. 37 Abs. 1 DSGVO zu prüfen. Soweit hier keine Bestellpflicht bejaht wird, ist gem. Art. 37 Abs. 4 DSGVO in Verbindung mit Vorschriften des nationalen Rechts (s.o.) zu prüfen, ob es hier Sondertatbestände gibt, die dennoch eine Bestellpflicht vorsehen. Das nationale Recht ist hier zwar subsidiär, erfasst aber im Ergebnis einen wesentlich größeren Kreis von Unternehmen, so dass sich diese Subsidiarität in der Praxis eher gegenteilig auswirken dürfte.

7 Zunächst nun zu den Vorgaben der DSGVO: Neu ist hier neben den sonstigen Vorgaben (dazu gleich mehr), dass die Bestellpflicht nicht nur den für die Verarbeitung Verantwortlichen trifft, sondern auch den Auftragsverarbeiter. Diese Aufhebung der nach bisherigem deutschen Recht klaren Trennung zwischen verantwortlicher Stelle (und damit Adressat von Bußgeldvorschriften bei Nichtbeachtung) und Auftragsverarbeiter folgt logisch der sich durch die gesamte Grundverordnung ziehenden Quasi-Gleichstellung von verantwortlicher Stelle und Auftrags-

verarbeiter. Auch dies ist, ebenso wie das nachfolgend erläuterte grundsätzlich neue Bestell-Kriterium, aus praktischer Sicht zu begrüßen, da mittlerweile die Auslagerung von IT-Dienstleistungen und Datenverarbeitung auf Externe einen erheblich größeren Umfang eingenommen hat, als noch vor 5 bis 10 Jahren. Die zunehmend komplexere Vernetzung nicht nur von Daten, sondern auch von Anwendungen in der Cloud wird mittelfristig ohnehin wohl dazu führen, dass ein Großteil der Unternehmen keine bzw. kaum noch eigene IT mehr vorhalten. Vor diesem Hintergrund ist eine Quasi-Gleichstellung von verantwortlicher Stelle und Auftragsverarbeiter im Hinblick auf die Bestellpflicht ohne Zweifel mehr als sinnvoll.

1.1.2. Bestellpflicht nach Art. 37 DSGVO

Anders als das bisherige Bundesdatenschutzgesetz macht Art. 37 DSGVO die Bestellpflicht nicht mehr von der Anzahl der im Unternehmen mit Datenverarbeitung beschäftigten Mitarbeiter abhängig, sondern von der Art, dem Umfang und dem Zweck der Verarbeitungsvorgänge. *8*

Dieser (neue) Ansatz und die damit verbundene Abkehr vom Kriterium der Größe des Unternehmens bzw. der Anzahl der Mitarbeiter trägt der Tatsache Rechnung, dass auch zahlenmäßig kleine Unternehmen mit zeitgemäßer IT personenbezogene Daten in erheblichem Umfang verarbeiten können. Im Hinblick auf das Schutzgut des Datenschutzrechts ist dies ein sinnvoller Ansatz, da auf diese Weise die Bestellpflicht an die „Kernmaterie" gebunden wird, nämlich die eigentlich stattfindende Datenverarbeitung. Aus praktischer Sicht jedoch wird die Beantwortung der Frage, ob Unternehmen nun zur Bestellung eines Datenschutzbeauftragten verpflichtet sind, gegenüber der bisherigen deutschen Rechtslage erheblich erschwert – was letztlich an den unklaren Formulierungen des Gesetzestextes liegt. Zu den Voraussetzungen der Reihe nach: *9*

Bestellpflicht für Behörden und öffentliche Stellen

Art. 37 Abs. 1 DSGVO postuliert eine Bestellpflicht für Behörden und öffentliche Stellen mit Ausnahme von Gerichten, die in ihrer gerichtlichen Tätigkeit handeln. Diese Regelung behält im Wesentlichen die bisherige nationale Regelung des § 4f Abs. 1 BDSG-alt bei – allerdings mit dem Unterschied, dass das Kriterium „automatisierte Datenverarbeitung" nun nicht mehr fallspezifisch gilt (wie bisher im BDSG), sondern grundsätzlich vor die Klammer gezogen wurde und in Art. 2 Abs. 1 DSGVO (u.a.) Grundvoraussetzung des sachlichen Anwendungsbereiches der Verordnung überhaupt ist. *10*

Ähnlich bisheriger – vor allem landesrechtlicher – Regelungen können Behörden oder öffentliche Stellen auch gemeinsam einen Datenschutzbeauftragten bestellen, wenn dies im Rahmen ihrer Organisation und Größe möglich und praktikabel ist (Abs. 3). *11*

Die Bestellpflicht für Behörden und öffentliche Stellen gilt – und dies hat durchaus Konsequenzen für bisher bestehende Sonderregelungen einzelner Bundesländer – *12*

sowohl für Bundesbehörden und öffentliche Stellen des Bundes, aber auch für die der Länder. Und damit tritt für einige Bundesländer im Hinblick auf die Bestellpflicht eine Neuerung ein.

13 Bisher sahen die Landesdatenschutzgesetze eine uneinheitliche Regelung vor, wenn es darum ging, ob Datenschutzbeauftragte für öffentliche Stellen der Länder auch extern, d.h. auf Grundlage eines Dienstleistungsvertrages bestellt werden durften. So sahen noch Landesdatenschutzgesetze in Bayern, Nordrhein-Westfalen und anderen Bundesländern vor, dass öffentliche Stellen, auch wenn sie mit anderen privaten Stellen im Wettbewerb stehen, nur Beschäftigte (der jeweiligen Stelle) zum Datenschutzbeauftragten bestellen können. Art. 37 Abs. 6 DSGVO stellt es den betroffenen verantwortlichen Stellen nun jedoch frei, ob Beschäftigte oder Externe auf der Grundlage eines Dienstleistungsvertrages die Aufgaben des Datenschutzbeauftragten erfüllen. Diese Freiheit umfasst mangels anderweitiger Einschränkung auch den vorstehenden Abs. 1 lit. a des Art. 37, wonach Behörden oder öffentliche Stellen in jedem Fall einen Datenschutzbeauftragten bestellen müssen. Anderweitige Regelungen in den o.g. Landesdatenschutzgesetzen werden danach von dieser europäischen Regelung überstimmt mit dem Ergebnis, dass unabhängig von der Eigenschaft als öffentlicher oder privater Stelle grundsätzlich auch Externe die Aufgaben des Datenschutzbeauftragten wahrnehmen können.

Bestellpflicht aufgrund Art, Umfang und Zweck der Verarbeitungsvorgänge

14 So weit, so (zumindest partiell) bekannt. Neu, und zwar in jeder Hinsicht, ist nun die Regelung, dass ein Datenschutzbeauftragter gemäß Art. 37 Abs. 1 lit. b zu bestellen ist, wenn

> „die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche regelmäßige und systematische Beobachtung von Personen erforderlich machen."

15 Der Verordnungsgeber hat den Anwendern zwar in über 130 Erwägungsgründen Auslegungshilfen für einen Großteil der Vorschriften mit auf den Weg gegeben, für diese neue Klausel (nachfolgend zwecks einfacherer Zitierweise nur „Personen-Beobachtung" genannt) hingegen fehlt (fast) jegliche Art von Information, welche Anwendungsfälle hiervon eigentlich umfasst sein sollen. Lediglich der Begriff Kerntätigkeit wird in Erwägungsgrund 97 dahingehend umschrieben, dass es sich bei der fraglichen Datenverarbeitung um die Haupttätigkeit der verantwortlichen Stelle handeln muss, nicht um eine Nebentätigkeit.

16 Es verbleiben damit im Ergebnis die klassischen juristischen Auslegungsmöglichkeiten, mit denen nachfolgend, soweit anwendbar, versucht wird, die Anwendungsfälle einzugrenzen.

17 In systematischer und auch teleologischer Hinsicht, also mit Blick auf den Regelungszusammenhang und den Sinn und Zweck der Regelung, soll die „Personen-Beobachtung" eine Art hochriskante (Ausnahme-)Verarbeitung darstellen, deren Risiken sich nicht mehr mit der Datenschutz-Folgenabschätzung (Art. 35) und

einer ggf. hierzu ergänzend herangezogenen vorherigen Konsultation der Aufsichtsbehörde (Art. 33) beherrschen lassen. Dies ist insoweit nachvollziehbar, als die Datenschutz-Folgenabschätzung eine eher schlaglichtartige (Einmal-)Bewertung darstellt, die Kontrolle eines Datenschutzbeauftragten aber eine kontinuierliche ist – und diese Kontroll-Kontinuität bei der regelmäßigen Beobachtung von Personen sinnvoll und erforderlich ist. Voraussetzung ist also, dass die fragliche Verarbeitung mindestens den Risikograd des Art. 35 aufweist, also aufgrund der Art, des Umfangs und der Umstände ein hohes Risiko für die persönlichen Rechte und Freiheiten beinhaltet – und zusätzlich regelmäßig und systematisch stattfindet. Wenn man nun ergänzend die grammatische Auslegung hinzuzieht, verbleibt die Frage, welche das Kerngeschäft des Unternehmens bildende Tätigkeit die umfangreiche, regelmäßige und systematische Beobachtung von Personen erfordert.

18 Ohne gedankliche Klimmzüge kann man hierunter **Auskunfteien** subsumieren, jedenfalls diejenigen, die Verbraucherbewertungen vornehmen: Unternehmen, die geschäftsmäßig (vermögens- oder verhältnisrelevante) personenbezogene Daten zum Zweck der Übermittlung erheben, speichern oder verändern, erfordern genau diese Art der Datenverarbeitung: Eine umfangreiche, regelmäßige und systematische Beobachtung von Personen. Vom Wortsinn her kann dies (aufgrund der fraglos ungewöhnlichen Formulierung „Beobachtung von Personen") zwar in ähnlicher Weise partiell auch für **Detekteien** gelten – allerdings bedarf es hier aufgrund der verschiedenen Tätigkeitsfelder dieser Branche einer genauen Analyse, ob solche Beobachtungen auch die „Kerntätigkeit" bilden und tatsächlich auch systematisch und regelmäßig stattfinden bzw. den erforderlichen Umfang einnehmen.

19 Im Übrigen darf der Anwendungsbereich der Bestellpflicht nicht zu eng auf Unternehmen beschränkt werden, die nach allgemeinem Verständnis der Kategorie Auskunfteien unterfallen – auch ohne Auskunftei zu sein, können ähnliche Dienstleistungen erbracht werden, die eine regelmäßige und systematische Personen-Beobachtung zum Geschäftszweck haben.

20 Soweit **Warndienste**, also geschäftsmäßig organisierte Datenbank-Betreiber, die Kunden gegen Gebühr bestimmte selektive Informationen von Betroffenen bereitstellen (z.B. sog. Mieterwarndienste) ähnliche Tätigkeiten wie Auskunfteien wahrnehmen, können diese bei Vorliegen der sonstigen quantitativen Voraussetzungen ebenfalls dem Tatbestand unterfallen.

21 Erfasst werden dürften von der neuen Regelung auch ähnliche Dienstleister, wie z.B. Betreiber von **Bewertungsportalen** im Internet, wenn mit diesen Personen (z.B. Ärzte, Lehrer) bewertet werden. Geschäftszweck solcher Portale ist es, ein Interesse der Nutzer an den Bewertungen von Personen zu erzeugen und damit hohe Zugriffszahlen auf die entsprechenden Seiten zu generieren, um dann über Werbeanzeigen bzw. deren -erlöse Umsatz zu erzeugen.

22 Auch **soziale Netzwerke** dürften den Tatbestand ausfüllen: Der Geschäftszweck dieser Anbieter besteht, ähnlich (aber in größerem Stil als Bewertungsportale) darin, Nutzer und deren von sich aus übermittelte bzw. dort veröffentlichte Daten möglichst umfassend zu beobachten, um dann Werbekunden passgenaue – in der

Regel pseudonyme – Profile bzw. Profilgruppen als werberelevante Zielgruppe zu verkaufen. Dass der Werbetreibende hier seine potenziellen Kunden zunächst nicht identifizieren, sondern nur seine Zielgruppe über Merkmale (z.B. weiblich, unter 40 Jahre alt, Single, Mutter etc.) bestimmen kann, ändert nichts daran, dass der Betreiber der Plattform sämtliche Daten personenbezogen verarbeitet und die Personen so auch, im Wortsinne des Tatbestands, systematisch und regelmäßig beobachtet.

23 Die vorgenannte Aufzählung soll und kann in keiner Weise abschließend sein. Die genannten Beispiele sollen daher eher nur die Richtung vorgeben, in die eine Interpretation dieser speziellen Bestellpflicht tendieren kann. Wie so oft, bleibt es der Prüfung dem konkreten Einzelfall überlassen, ob eine Bestellpflicht vorliegt – und später der Auslegung der Aufsichtsbehörden (und Gerichte).

Bestellpflicht wegen der Verarbeitung besonders sensibler Daten

24 Soweit die vorhergehende Voraussetzung hinsichtlich der Bestimmung ihrer Kriterien in der Praxis vermutlich erhebliche Schwierigkeiten bereiten dürfte, sollte die Voraussetzung des Art. 37 Abs. 1 lit. c weniger Probleme aufwerfen. Hiernach ist ein Datenschutzbeauftragter zu bestellen, wenn

> „die Kerntätigkeit des für die Verarbeitung Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten gem. Art. 9 oder von Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 besteht."

25 Praktikern, die bisher mit dem BDSG gearbeitet haben, kommt diese (Art der) Regelung fraglos vertrauter vor – denn der Gesetzgeber verweist die Anwender hier nicht nur auf eigene Definitionen – hier in Art. 9 und 10 mit den entsprechenden Definitionen in Art. 4, sondern regelt die Bestellungsvoraussetzung auch deutlich konkreter und somit praxisnäher als in Art. 37 Abs. 1 lit. b.

26 Art. 9 der DSGVO sieht die Verarbeitung der besonders sensiblen Daten nur im Rahmen eines – quasi geschachtelten – Verbots mit Erlaubnisvorbehalt vor. Bereits aus dieser Gesetzessystematik, die die Verarbeitung dieser Daten nur in sehr eng begrenzten Ausnahmefällen überhaupt zulässt, ist zu entnehmen, dass diese Verarbeitung zwangsläufig von einem Datenschutzbeauftragten begleitet werden muss. Allerdings gilt die Voraussetzung nicht per se, wenn besondere Kategorien von Daten verarbeitet werden, sondern nur, wenn diese Verarbeitung umfangreich erfolgt. Aufgrund des Regelungszusammenhangs darf davon ausgegangen werden, dass der Gesetzgeber diesem Kriterium dasselbe Verständnis zugrunde legen wollte wie im Abschnitt zuvor bei der Bestimmung der „umfangreichen Beobachtung (…) von Personen". Insoweit kann zur Vermeidung von Wiederholungen hierzu auf die obigen Ausführungen[2] verwiesen werden.

27 Um das Kriterium zu erfüllen, muss der für die Verarbeitung Verantwortliche die Verarbeitung dieser Daten als Kerntätigkeit vornehmen. Auch diese Anforderung

2 Vgl. oben Rn. 17 ff.

wurde bereits zuvor im Kontext von Art. 35 Abs. 1 lit. b erläutert[3]. Beispiele hierfür sind Medizinische (Gen-)Datenbanken, die von privaten Unternehmen (mit) betrieben werden, Parteien, Gewerkschaften, Softwareunternehmen, die biometrische Daten zur Authentisierung verwenden (soweit sie tatsächlich Zugriff auf diese Daten haben), Krankenhäuser in privater Trägerschaft, Arztpraxen.

28 Aufgrund der sehr speziellen Art von Daten über strafrechtliche Verurteilungen und Straftaten gem. Art. 10 und auch aufgrund der Tatsache, dass diese Daten im Wesentlichen von Behörden und Gerichten verarbeitet wird, wird diese Fallgruppe wenig praxisrelevant sein. Vorstellbare Adressaten sind hier z.B. Dienstleister, die für Behörden entsprechende Daten im Auftrag verarbeiten oder private Vereinigungen von Opfern von Straftaten.

1.1.3. Gemeinsame Bestellung eines Datenschutzbeauftragten durch eine Unternehmensgruppe

29 Ein weiterer Baustein im neuen, kleinen Konzernprivileg der DSGVO[4] bildet Art. 37 Abs. 2: Hiernach ist es Konzernen nunmehr erlaubt, einen Datenschutzbeauftragten für die gesamte Unternehmensgruppe zu bestellen, wenn dieser von jeder Niederlassung aus leicht erreicht werden kann. Diese Regelung, ebenso wie ein wirkliches Konzernprivileg, war auch vor dem Hintergrund einer etwaigen neuen nationalen Regelung überfällig. Dass es für die Bestellung des Datenschutzbeauftragten in einem Unternehmensgeflecht jeweils auf die einzelne juristische Person ankam, war zwar gesetzestechnisch logisch, in der Praxis aber nur schwer vermittelbar bzw. hat letztlich unnötigen Papieraufwand verursacht, wenn für jedes Konzernunternehmen eine Bestellungsurkunde auszufertigen war.

30 Die neue Regelung hat Vor- und Nachteile. Vorteile bestehen fraglos darin, dass die Neigung von Konzernen, einen Datenschutzbeauftragten einheitlich zu bestellen, sicherlich größer sein dürfte, als wenn dies für diverse Unternehmen separat erfolgen müsste. Damit einhergehend können, wenn sich das Know-how über Unternehmensprozesse und deren datenschutzrechtliche Bewertung in einer Person konzentriert, durchaus Synergieeffekte einstellen. Allerdings muss hierbei berücksichtigt werden, dass die Vorschrift nur die Bestellung eines Datenschutzbeauftragten ermöglicht – was nicht damit gleichzusetzen ist, dass die Datenschutzbelange einer Unternehmensgruppe nur durch einen Datenschutzbeauftragten wahrgenommen werden können. Gerade in multinationalen Konzernen ist vielmehr die Einrichtung einer Datenschutzorganisation gefragt, denen zwar ein Datenschutzbeauftragter als Leitung vorsteht, die aber vom Umfang her je nach Aufgabenspektrum die Größe einer internen Organisationseinheit mit z.T. sogar mehreren Hierarchien einnehmen kann.

3 Vgl. oben Rn. 15.
4 Vgl. hierzu auch Kapitel B 9.

Unternehmensgruppe

31 Unternehmensgruppe wird in Art. 4 Nr. 19 legal definiert, hierbei handelt es sich um eine Gruppe, die aus einem herrschenden Unternehmen und von diesen abhängigen Unternehmen besteht. Interessant ist hierbei, dass die DSGVO nicht auf den Begriff der verbundenen Unternehmen im Sinne des § 15 AktG abstellt, sondern auf den der abhängigen bzw. herrschenden Unternehmen des § 17 AktG. Warum allerdings nicht generell auf verbundene Unternehmen abgestellt wird, lässt sich auch aus dem betreffenden Erwägungsgrund 28 nicht herleiten[5].

Sofern von jeder Niederlassung aus ... leicht erreicht werden kann.

32 Die Anforderung soll lediglich sicherstellen, dass der Datenschutzbeauftrage die bei Unternehmensgruppen im Zweifel häufig fehlende Lokalität durch eine Erreichbarkeit per E-Mail oder Telefon sicherstellen kann. Das Gesetz spricht dabei bewusst nicht von „leicht verfügbar" im Sinne eines vor-Ort-Seins, sondern nur von „erreichbar". Dieses Kriterium dürfte allerdings in Zeiten einer täglich wachsenden Vernetzung kein besonderes Gewicht haben.

Formvorschriften

33 Wie sieht eine Bestellung eines Datenschutzbeauftragten in der Praxis aus? Hierfür sah weder das vorherige BDSG noch sieht die jetzige DSGVO (bzw. das BDSG-neu) eine besondere Förmlichkeit vor[6]. Voraussetzung für eine (insbesondere auch arbeitsrechtlich) wirksame und nachweisbare Bestellung ist, dass diese schriftlich erfolgt und der bzw. die bestellte Person namentlich benannt, so dass eine Verwechselung ausgeschlossen ist. Auf Seiten des bzw. der Unternehmen sollte jedes Unternehmen vollständig im Rubrum bezeichnet werden, für das der Datenschutzbeauftragte bestellt wird.

34 Weiterhin muss das Datum, ab dem die Bestellung wirksam sein soll, angegeben werden. In der Regel wird hier kein Ende-Datum angegeben, denn die Bestellung erfolgt in der Regel unbefristet. Interessant ist in diesem Zusammenhang, dass die DSGVO keinerlei Regelungen zur Abberufung trifft – außer der, dass der Datenschutzbeauftragte wegen seiner Aufgabenwahrnehmung nicht abberufen oder benachteiligt werden kann, (Art. 38 Abs. 3 S. 2, vgl. hierzu Kapitel B 1.7). Nicht ausgeschlossen ist allerdings, dass dies in besonderen Fällen – z.B. um eine festgelegte Übergangszeit zu überbrücken – dennoch geschieht. Falls dies der Fall sein sollte, bedarf es dann nach Ablauf des benannten Zeitraums keiner Abberufung.

---

5 Hier heißt es lediglich, dass „das herrschende Unternehmen dasjenige sein sollte, dass zum Beispiel aufgrund der Eigentumsverhältnisse, der finanziellen Beteiligung oder der für das Unternehmen geltenden Vorschriften oder der Befugnis, Datenschutzvorschriften umsetzen zu lassen, einen beherrschenden Einfluss auf die übrigen Unternehmen ausüben kann".

6 Für interne Datenschutzbeauftragte können in einer analogen Anwendung von § 2 NachwG („Gesetz über den Nachweis der für ein Arbeitsverhältnis geltenden wesentlichen Bedingungen" vom 20.07.1995, BGBl. S. 946) zumindest einige schriftlich zu regelnde Punkte bestimmt werden.

Schließlich, wenig überraschend, muss das Dokument das Datum der Zeichnung sowie die Unterschriften des bzw. der Datenschutzbeauftragten sowie des Vertretungsberechtigten des betreffenden Unternehmens beinhalten. Für eine Unternehmensgruppe muss hier der Vertretungsberechtigte zeichnen, dessen Vertretungsbefugnis diejenigen der anderen Unternehmen aufgrund der Beteiligungs- bzw. Beherrschungsstruktur umfasst. *35*

1.1.4. Die Bestellpflicht nach nationalem Recht – § 38 BDSG-neu

Soweit also nach den vorstehenden Regelungen auf jeden Fall ein Datenschutzbeauftragter zu bestellen ist, stellt Abs. 4 klar, dass in anderen als in den benannten Fällen Verantwortliche, Auftragsverarbeiter oder auch Verbände und Vereinigungen einen Datenschutzbeauftragten bestellen können (wer sollte sie daran hindern?). Welchen Regelungsgehalt dieser Satzteil haben soll, bleibt allerdings unklar und hätte nur in dem Fall einen eigenen Aussagegehalt, wenn in bestimmten, gesetzlich bezeichneten Fällen ein Datenschutzbeauftragter tatsächlich nicht benannt werden dürfte. Da dies aber nicht der Fall ist, bleibt nur der zweite Teil des Absatzes relevant, nachdem auch dann ein Datenschutzbeauftragter bestellt werden muss, wenn zwar die Voraussetzungen der DSGVO nicht vorliegen, dafür aber der betreffende Mitgliedsstaat eine Bestellpflicht vorsieht. Der deutsche Gesetzgeber hat, wie anfangs bereits kurz erwähnt, hiervon Gebrauch gemacht und mit § 38 BDSG-neu die bisherigen Regelungen zur Bestellung eines Datenschutzbeauftragten nahezu wortgleich beibehalten. *36*

Dies bedeutet in der Praxis, dass für die Frage nach der Bestellpflicht entgegen der gesetzlichen Normenhierarchie zunächst der Blick in § 38 BDSG-neu erforderlich ist. Liegen die dortigen Voraussetzungen vor, *37*

- in der Regel ständig mindestens 10 Personen mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt oder
- der Betrieb von Verarbeitungen, die einer Datenschutzfolgenabschätzung unterliegen, oder
- geschäftsmäßige Verarbeitung zum Zweck der Übermittlung, oder
- Verarbeitung zum Zweck der Markt- und Meinungsforschung

ist auch dann ein Datenschutzbeauftragter zu bestellen, wenn die Anforderungen des Art. 37 DSGVO nicht erfüllt sind[7].

1.2. Mitteilungspflicht gegenüber der Aufsichtsbehörde

Neu und bisher ohne nationales Vorbild ist nun die Mitteilungspflicht des Art. 37 Abs. 7 DSGVO. Danach müssen die Kontaktdaten des Datenschutzbeauftragten veröffentlicht und auch der Aufsichtsbehörde gemeldet werden. Zur Umsetzung der Veröffentlichungspflicht bieten sich natürlich die entsprechenden Webseiten *38*

7 Zu den Bestellpflichten z.B. Simitis, in Simitis, Bundesdatenschutzgesetz, 8. Auflage 2014, § 4f Rn. 12ff.; Scheja, in: Taeger/Gabel, Bundesdatenschutzgesetz, 2. Auflage 2013, § 4f Rn. 18; Gola/Schomerus, Bundesdatenschutzgesetz, 12. Auflage 2015, § 4f Rn. 7.

Ab dem 25. Mai 2018 finden die Regelungen der Datenschutz-Grundverordnung (DSGVO) und des neuen BDSG Anwendung. Unternehmen sind dann zum Beispiel verpflichtet, transparent und ausführlich zu beschreiben, welche Daten sie für welche Zwecke verarbeiten und wie lange die Daten gespeichert werden. Anders als heute können Verstöße mit empfindlichen Bußgeldern geahndet werden. Dieser Aspekt führt in der Praxis dazu, dass sich viele Unternehmen – zum Teil erstmalig – intensiv mit den datenschutzrechtlichen Vorschriften und ihrer Umsetzung im Unternehmen befassen.

Dieses Handbuch hilft Ihnen bei der Umsetzung der mitunter komplizierten Regelungen der DSGVO und des neuen BDSG. Es zeigt Ihnen praxisorientierte Lösungen für Fragen auf, die sich in den Unternehmen stellen. Weiterhin wird der Themenbereich der Informationssicherheit ausführlich behandelt, der in der Praxis stets zusammen mit dem Datenschutz gedacht werden sollte.

Sämtliche Autoren dieses Handbuchs sind erfahrene Beraterinnen und Berater, die seit Jahren in den Bereichen Datenschutz und Informationssicherheit tätig sind. In diesem Handbuch stellen sie Best Practice-Ansätze vor, wie den neuen gesetzlichen Vorgaben am besten entsprochen werden kann.

Leseprobe, mehr zum Werk unter www.ESV.info/17727

9 783503 177271

www.ESV.info