47. Jahrgang
datenschutz-berater.de
DSB 05/2023

DATENSCHUTZ-BERATER

» Ihr zuverlässiger Partner für Datenschutz und Datensicherheit

Editorial

Stichwort des Monats

Datenschutz im Fokus

Aktuelles aus den Aufsichtsbehörden

Rechtsprechung

ISSN 0170-7256

dfv Mediengruppe

Anna Cardillo, Guido Hansch, Wolfgang Lehna und Heiko Markus Roth

Koordinierte Prüfung zu Stellung und Aufgaben von Datenschutzbeauftragten

Mit Pressemitteilung vom 15. März 2023 gab das BayLDA den Startschuss für die zweite EU-weite Prüfaktion der europäischen Datenschutz-Aufsichtsbehörden. Koordiniert durch den EDSA, widmet sich die Prüfaktion der Stellung und den Aufgaben von Datenschutzbeauftragten (DSBen). Die Autoren beleuchten in diesem Beitrag den Fragenkatalog, der an 36.000 Unternehmen versandt wurde.

Anlass und Rahmenbedingungen der Prüfung

Gestützt auf Artikel 29 der Geschäftsordnung des Europäischen Datenschutzausschusses (EDSA) verabschiedetet eben jenes Gremium aus Vertretern der einzelnen europäischen Datenschutz-Aufsichtsbehörden (ASBen) am 14. Februar 2023 ihr Arbeitsprogramm für 2023/24. Dort wurde für 2023 eine „CEF"-Prüfung zur Benennung und zur Position von DSBen angekündigt. Am 15. März 2023 wurde durch Pressemeldung des EDSA der Startschuss für diese Prüfung verkündet. Das CEF bildet den Rahmen für EU-weite, koordinierte Prüfungen der ASBen mit dem Ziel kohärenter Rechtsanwendung und Rechtsdurchsetzung, es leitet sich aus Art. 57 Abs. 1 lit. g DSGVO ab. Seine Ausgestaltung wird in einem am 20. Oktober 2020 verabschiedeten Dokument des EDSA näher beschrieben. Die teilnehmenden ASBen müssen sich bei der Umsetzung des Prüfauftrags, eventuell nachfolgender Untersuchungen und Maßnahmen an Artt. 57, 58 DSGVO messen lassen. Ein abschließender Prüfbericht wird erwartet. Die Behörde in Dänemark (Datatilsynet) veröffentlichte am 17. April 2023 als Erste den Fragebogen.

Gegenstand der Prüfung

An der CEF-Prüfung nehmen 26 ASBen und der Europäische Datenschutzbeauftragte teil. Soweit ersichtlich gehen einzelne ASBen bei der aktuellen CEF-Prüfung unterschiedlich vor. Beispiele: In Deutschland nimmt das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) teil, also jene Behörde, welche die Aufsicht in Bayern über die nicht-öffentlichen Stellen innehat (siehe die Pressemeldung vom 15. März 2023). Die Datatilsynet gab bekannt, dass sie die Prüfung auf DSBen der Kommunen beschränke, da diese DSBen benennen müssten und ihre Aufgabenerledigung mit der Verarbeitung einer großen Menge an Daten einhergehe (siehe die Pressemeldung vom 22. März 2023). Tschechien teilte mit, sich auf öffentliche Stellen zu konzentrieren (siehe die Pressemeldung vom 14. März 2023). Griechenland und Estland kontaktieren öffentliche und nicht-öffentliche Stellen (siehe die Pressemeldung vom 21. März 2023). Es bleibt zu hoffen, dass sich diese Unterschiede im Bericht niederschlagen werden.

Teilnehmende ASB in Deutschland

Wenige Tage nach der Veröffentlichung der Pressemeldung des BayLDA wurde ein Beitrag von Thomas Kranig, vormaliger Präsident eben jener Behörde, in der Online-Zeitschrift ZD-Aktuell (2023, 01121) veröffentlicht. In dem Beitrag wurde insbesondere das Bedauern ausgedrückt, dass in Deutschland nur das BayLDA an der Prüfung teilnehme. Gleichermaßen weist Thomas Kranig auf Art. 51 DSGVO hin, wonach sich weiterhin weitere ASBen an der Prüfung beteiligen können. Der Beitrag ist nachvollziehbar. In Deutschland gibt es auf Ebene der Bundesländer 17 ASBen. Mit Blick auf die begrenzten Ressourcen der öffentlichen Hand ist es zumindest fraglich, wie performant und effizient eine einzelne Behörde die Rückmeldung von bis zu 36.000 DSBen im Vergleich zu 17 ASBen erledigen kann, die ihrerseits je eine Teilmenge prüfen. Warum sich nur das BayLDA beteiligt, ist den Autoren nicht bekannt.

Bisherige Prüfungen von DSBen

Nach Art. 57 Abs. 1 DSGVO haben die ASBen insbesondere die Aufgabe, die Anwendung der DSGVO zu überwachen und durchzusetzen (lit. a) sowie Untersuchungen über die Anwendung der DSGVO durchzuführen (lit. h). Eine Handvoll separierter Prüfungen der ASBen in Deutschland, die auch den Datenschutzbeauftragten betreffen, sind bekannt. Namentlich haben solche Prüfungen durchgeführt: Nordrhein-Westfalen (zwei Mal), Thüringen (ein Mal), Saarland (ein Mal) und Niedersachsen (ein Mal). EU-weit einheitliche und systemische Prüfungen gab es nach Kenntnis der Autoren noch nicht.

„Datenschutzbeauftragte": Rechtsrahmen

In DE ist die Rolle von DSBen lange bekannt. Noch vor Art. 18 Abs. 2 Datenschutzrichtlinie 95/46 EG sah der Bundesgesetzgeber 1977 mit § 38 BDSG a. F. eine Bestellpflicht für bestimmte Organisationen vor. Heute sind die Anforderungen an die Benennung, die Stellung und die Aufgaben des Datenschutzbeauftragten in Artt. 37 bis 39 DSGVO verankert. Verstöße dagegen sind nach Art. 83 Abs. 4 lit. a DSGVO bußgeldbewährt. Das Bundesrecht reagiert mit §§ 5, 38 BDSG auf diese Vorgaben. Im Landesrecht finden sich Regelungen zur Rolle des Rundfunkbeauftragten für den Datenschutz und zu DSBen für öffentliche Stellen.

Flankiert werden diese Vorgaben durch exekutive Positionierungen, etwa des EDSA (WP 243 rev.01) und des gemeinsamen Gremiums deutsche ASBen (KP Nr. 12). Die Unabhängigkeit von DSBen im Rahmen der Beratungs- und Überwachungsaufgabenerfüllung, ihre organisatorische Integration im operativen und strategischen Datenschutz als auch ihre Qualifikation sind rollenprägend. Besonders die „erforderliche" Qualifikation und das damit verbundene Fachwissen sind „erfolgskritisch" und werden seit Jahren diskutiert. 2007 konstatierte die Bundesregierung in Deutschland deutlich: „Betriebliche Datenschutzbeauftragte, die den gesetzlichen Qualifikationserfordernissen nicht genügen oder ihre Aufgaben nicht ordnungsgemäß erfüllen, sind eine Gefahr für den Datenschutz" (BT-Drs. 16/4249, S. 2).

Pflicht der nicht-öffentlichen Stellen zur Beantwortung der Fragebogen

Nach wie vor besteht bei Empfängern von Fragebogen der ASBen Unsicherheit darüber, aufgrund welcher Befugnis die Behörde überhaupt tätig wird und ob ein solcher Fragebogen beantwortet werden muss.

Befugnis der ASBen

Art. 31 DSGVO bestimmt, dass Verantwortliche auf Anfrage mit ASBen bei der Erfüllung ihrer Aufgaben zur Kooperation und damit auch zur Bereitstellung von Informationen verpflichtet sind. Daneben ist die maßgebliche Vorschrift in Bezug auf die aufsichtsbehördlichen Befugnisse Art. 58 DSGVO. Die Untersuchungsbefugnisse des Art. 58 DSGVO dienen zuvorderst der Überwachung der Einhaltung der DSGVO und können auch anlasslos eingesetzt werden, wie es bei der Auswahl der Adressaten der Fragebogen ganz überwiegend der Fall sein dürfte.

Art. 58 Abs. 1 lit a DSGVO gestattet den ASBen, „den Verantwortlichen, den Auftragsverarbeiter und gegebenenfalls den Vertreter des Verantwortlichen oder des Auftragsverarbeiters anzuweisen, alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind".

Daneben dürfte auch Art. 58 Abs. 1 lit. e DSGVO anwendbar sein, der bestimmt, dass die ASBen die Befugnis haben, „von dem Verantwortlichen und dem Auftragsverarbeiter Zugang zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu erhalten".

Die Vorschrift regelt dabei nicht, in welcher Form die ASBen Informationen und Daten anfordern und auch nicht in welcher Form die Informationen bereitgestellt werden müssen. Sofern seitens der ASBen der Verhältnismäßigkeitsgrundsatz gewahrt wird, dürften die Behörden damit relativ frei agieren können, sodass der Versand eines Fragebogens und die Aufforderung zu dessen Beantwortung, ggf. auch durch zusätzliche Offenlegung interner Prozessabläufe etc., von der Vorschrift gedeckt sein werden. Der in Rede stehende Fragebogen lässt auch nicht erkennen, dass die anfragende Behörde ihren Ermessensspielraum überschritten hätte. Der Vollständigkeit halber muss darauf hingewiesen werden, dass der betriebliche Datenschutzbeauftragte trotz Art. 39 Abs. 1 lit. d und e DSGVO natürlich nicht selbst der unmittelbar zur Auskunftserteilung Verpflichtete ist.

Es ist daher als Zwischenergebnis festzuhalten, dass den ASBen im Rahmen ihrer überwachenden Tätigkeit gem. Art. 58 Abs. 1 lit. a und e i. V. m. Art 31 DSGVO ein Auskunftsanspruch zusteht, dessen Geltendmachung bei dem Unternehmen als datenschutzrechtlich Verantwortliche grundsätzlich eine Handlungspflicht auslöst. Die Verpflichtung von nicht-öffentlichen Stellen zur Auskunftserteilung gegenüber den ASBen der Länder ist in § 40 Abs. 2 BDSG geregelt.

Entscheidend für die Bejahung einer Pflicht zur Beantwortung eines Auskunftsersuchens einer Behörde ist, ob die konkrete Ausgestaltung der Prüfaktion als Verwaltungsakt im Sinne von § 35 Satz 1 VwVfG zu qualifizieren ist. Danach ist ein Verwaltungsakt jede Verfügung, Entscheidung oder andere hoheitliche Maßnahme, die eine Behörde zur Regelung eines Einzelfalls auf dem Gebiet des öffentlichen Rechts trifft und die auf unmittelbare Rechtswirkung nach außen gerichtet ist. Ein Anschreiben einer Aufsichtsbehörde mit beiliegendem Fragebogen kann eine unverbindliche Bitte um Teilnahme an einer Umfrage sein. Die ASBen können gemäß Art. 58 Abs. 1 lit. a DSGVO den Verantwortlichen oder den Auftragsverarbeiter aber auch „anweisen", alle Informationen bereitzustellen, die für die Erfüllung ihrer Aufgaben erforderlich sind. Es steht grundsätzlich im Ermessen der Behörde, die nach Art. 58 Abs. 1 lit. a DSGVO und § 40 Abs. 4 BDSG bestehende Handlungsverpflichtung (Auskunftserteilung) durch einen Verwaltungsakt zu konkretisieren (VG Mainz, Urt. v. 9.5.19 – 1 K 760/18.MZ). Ob dem Anschreiben die für einen Verwaltungsakt erforderliche Regelungswirkung („Ich verpflichte dich hiermit, die gewünschten Informationen zu erteilen!") zukommt, ist im Einzelfall zu prüfen (zum Erstankündigungsschreiben Zensus 2011 nebst Fragebogen: VG Berlin, Beschl. v. 22.8.11 – 6 L 1.11). Sind Rechtsbelehrungen über Auskunftsverweigerungsrechte (vgl. § 40 Abs. 4 Satz 2 und 3 BDSG), Rechtsbehelfsbelehrung, Zwangsgeldandrohungen im Falle von Zuwiderhandlungen beigefügt, wird ein Verwaltungsakt vorliegen. Fehlen diese, ist nicht zwangsläufig von einem unverbindlichen Anschreiben auszugehen, es können gleichwohl andere Indizien gegeben sein, die die Intention der Behörde zum Erlass einer verbindlichen Anordnung erkennen lassen.

Auskunftsverweigerungsrecht des Verantwortlichen

Die Beantwortung von Fragen der Behörde durch den Verantwortlichen kann ggf. Sachverhalte tangieren, die straf- oder ordnungswidrigkeitsrechtlich relevant sein können. In Anwendung des Grundsatzes „nemo tenetur" steht dem Auskunftspflichtigen nach § 40 Abs. 4 Satz 2 BDSG höchstpersönlich, d. h. nicht der juristischen Person, und ausschließlich für die vorgenannte Art von Fragen ein Auskunftsverweigerungsrecht zu, wenn er sich oder einen der in § 383 Abs. 1 Nr. 1 bis 3 ZPO aufgelisteten Angehörigen der Gefahr der Strafverfolgung oder eines Ordnungswidrigkeitenverfahrens aussetzen würde. Darauf ist der Auskunftspflichtige hinzuweisen. Erfolgt der Hinweis nicht, dürfen die erteilten Auskünfte nicht verwertet werden. Die bloße Gefahr, dass dem befragten Unternehmen an sich bei Offenlegung von datenschutzrechtlich nachteiligen Informationen ein Bußgeld gemäß Art. 83 DSGVO droht, dürfte regelmäßig nicht ausreichen, um ein Auskunftsverweigerungsrecht anzunehmen.

Folgen bei Nichtbeantwortung/verzögerter/unvollständiger Beantwortung

Liegt im Einzelfall ein verbindlicher Verwaltungsakt vor, so kann die Behörde diesen anschließend im Wege des Verwaltungszwangs durchzusetzen. Daraus folgt, dass die ASBen einer verzögerten Auskunftserteilung oder Nichtbeantwortung mit einem Zwangsgeld begegnen können. Zumindest ein Sachverhalt ist bekannt, bei dem eine Behörde in einem ähnlich gelagerten Sachverhalt zu diesem Mittel gegriffen hat (VG Mainz, Urt. v. 9.519 – 1 K760/18. MZ). Zugleich ist auch die Verhängung eines Bußgeldes nach Art. 83 Abs. 5 lit. e DSGVO denkbar.

Dokumente, die zur Beantwortung der Fragen herangezogen werden sollten

Neben dem beantworteten Fragebogen fordern die ASBen – sofern ein Datenschutzbeauftragter benannt ist – einerseits ein Organigramm der Organisation, aus welchem auch die Verortung des Datenschutzbeauftragten hervorgeht. Andererseits wird auch der aktuelle schriftlichen Bericht – alternativ die aktuelle vergleichbare Dokumentation – von DSBen über ihre Tätigkeit gefordert.

Das Organigramm

Die konkret formulierte Anforderung ein Organigramm zu erstellen, ergibt sich weder aus der DSGVO noch aus den korrespondierenden Vorschriften des BDSG. Die Anfrage zielt offensichtlich auf die Umsetzung der Vorgaben der Veröffentlichung der Kontaktdaten des Datenschutzbeauftragten aus Art. 37 Abs. 7 DSGVO und der unmittelbaren Berichtspflicht an die höchste Managementebene aus Art. 38 Abs. 3 Satz 3 DSGVO. Selbstverständlich lassen sich die Vorgaben auch durch andere Wege der Veröffentlichung, sei es für die Kontaktdaten über das Intranet für die Mitarbeiter oder die Website für externe Betroffene erfüllen. Ebenso lässt sich die unmittelbare Berichtslinie auch außerhalb eines Organigramms, zum Beispiel in einem Datenschutzhandbuch oder den internen Datenschutzrichtlinien darstellen. Auch die Artikel-29-Datenschutzgruppe (Art.-29-Gruppe) nennt in ihrem WP243 (rev.01, Kap. 2.6) bei den „bewährten Verfahren" zur Veröffentlichung neben dem Organigramm das Intranet oder das interne Telefonbuch als gleichwertig.

Sofern ein Organigramm existiert, wird es als Ausdruck der oben genannten Vorschriften auch die Einordnung des Datenschutzbeauftragten in die Organisation darstellen müssen. In der Praxis haben sich hier unterschiedliche Berichtsmodelle herausgebildet, die sich im Wesentlichen in zwei Varianten darstellen. Zum einen die sogenannte „dotted line" für die Fälle, in denen DSBen organisatorisch dem Fachbereich einer anderen Managementebene zugeordnet sind, jedoch formal auch eine Berichtslinie zur höchsten Managementebene haben. Häufig sieht man hier DSBen, die dem Leiter Recht oder dem Leiter der IT unterstellt sind. Zum anderen gibt es die unmittelbare Berichtslinie an die höchste Managementebene, zum Beispiel in Form einer Stabsstelle Datenschutz.

Die Berichtslinie als „dotted line" wird von den ASBen kritisch betrachtet. Ausweislich der Pressemitteilung des BayLDA zur koordinierten Prüfung zu Stellung und Aufgaben von DSBen vom 15. März 2023 wird bei der Prüfung ein besonderes Augenmerk auf die Berichtslinie gelegt und insbesondere bei „dotted lines" über mehrere Hierarchieebenen hinweg die Umsetzung der unmittelbaren Berichtspflicht hinterfragt.

Der Bericht von DSBen

Eine unmittelbare gesetzliche Pflicht von DSBen zur Erstellung eines Tätigkeitsberichtes ergibt sich ebenfalls weder aus der DSGVO noch aus dem BDSG. Art. 38 Abs. 3 DSGVO verlangt, dass der Datenschutzbeauftragte unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters berichtet. In welcher Art und Weise wird hierbei nicht vorgegeben. Die Art.-29-Gruppe führt den Jahresbericht über die Tätigkeit als „ein weiteres Beispiel für unmittelbare Berichterstattung" an (WP 243 rev.01, Kap. 3.3). Der Tätigkeitsbericht wird hier als eine von mehreren Möglichkeiten gesehen, der gesetzlich normierten Berichtspflicht nachzukommen. Hierfür spricht auch die Betrachtung im Rahmen des Trilogs. Zwar gab es im Rahmen des Trilog zur DSGVO seitens Kommission und Parlament die Bestrebung, den Datenschutzbeauftragten zu einer Dokumentation der im Rahmen seiner Tätigkeit erhaltenen Antworten zu verpflichten. Diese konnten sich aber mit ihrem Ansinnen nicht durchsetzen. Daher verlangen die ASBen bei Nichtvorliegen eines Jahresberichts die Vorlage der aktuellen vergleichbaren Dokumentation des Datenschutzbeauftragten. Welche Doku-

mente damit gemeint sind, bleibt offen. Die Formulierung weist aber auf DSBen als Verfasser hin. Andere Dokumente, zum Beispiel Auditberichte von Dritten, scheiden hier offensichtlich aus.

Auch wenn es keine direkte gesetzliche Verpflichtung für die Erstellung eines „Tätigkeitsberichts" gibt, ist die Erstellung eines solchen in vielen Unternehmen üblich und aus guten Gründen fester Bestandteil des Datenschutzmanagements geworden. Tätigkeitsberichte können Verantwortlichen ganzheitlich und kanalisiert Informationen über den „Zustand" der Datenschutzorganisation liefern und bilden bei regelhafter und einheitlicher Fortschreibung die Basis für Kennzahlen und die Ermittlung des Reifegrads eben jener Organisation. Dies ist mit Blick auf Artt. 24, 32 Abs. 1 Halbsatz 2 lit. d DSGVO auch empfehlenswert. Schließlich können solche Berichte auch Bestandteil des allgemeinen Risikomanagements der Organisation sein.

Interessant wird aus Sicht der Autoren sein, wie sich in der Praxis das unter Umständen existierende Spannungsfeld zwischen (1) der Herausgabe einer Dokumentation, die ihren Zweck nur erfüllen kann, wenn sie den sprichwörtlichen Finger in die Wunde legt, und (2) dem Grundsatz nemo tenetur auflösen wird.

Grundsätzlich ist die Erstellung eines Jahresberichts oder einer Dokumentation sinnvoll und kann die Umsetzung der Ziele des Datenschutzes innerhalb der Organisation fördern. Wird der Bericht gemäß dem gesetzlichen Leitbild der Aufgaben als Instrument nicht nur der Beratung, sondern auch der Überwachung verfasst, liegt es durchaus im Rahmen der Möglichkeiten, dass im Bericht Themen angesprochen werden, die das Unternehmen ungern nach außen geben möchte. Realistisch gesehen ist auch bei einem hohen Umsetzungsgrad beim Datenschutz kein Unternehmen vor Datenschutzverletzungen gefeit. Idealerweise sind eventuelle Vorfälle dokumentiert und die Ursachen ausgeräumt und Maßnahmen ergriffen worden, um Wiederholungen zu vermeiden. Bei einem Vorfall sollten gem. Artt. 33 oder 34 DSGVO die Notwendigkeit der Unterrichtung der ASBen und der Betroffenen und die Gründe für das Ausbleiben der Unterrichtung sorgfältig abgewogen werden und dokumentiert sein. In Abhängigkeit des Zeitablaufs seit Erstellung des letzten Berichts kann es sinnvoll sein, die Wirksamkeit der getroffenen Maßnahmen in einer ergänzenden Aktualisierung zu beleuchten.

Fazit und Empfehlungen für die Praxis

Die EU-weit einheitliche und systemische Prüfung der ASBen zu Stellung und Aufgaben von DSBen, ist aus Sicht der Autoren dem Grunde sehr zu begrüßen. Es gibt weder aktuelle noch in dieser Größenordnung initiierte Prüfungen, die sich den im Fragebogen aufgeworfenen Fragen widmen. Es bleibt zu hoffen, dass der EDSA in seinem Prüfbericht nicht nur über einzelne Auffälligkeiten berichten, sondern grundlegend Aussagen zu „Dauerbrennern" in der Praxis treffen wird. Ggf. finden die Befunde auch Niederschlag in einer zweiten Revision des in die Jahre gekommenen WP243 (rev.01 aus 2017). Es wurde in diesem Beitrag auf die Fallstricke bei der Frage der Pflicht zur Beantwortung des Fragebogens hingewiesen. In einem Folgebeitrag werden die Autoren auf die einzelnen Fragen eingehen. Wie noch gezeigt wird, steckt auch hier der „Teufel im Detail". Ein wachsames, kritisches Auge wird empfohlen.

Autoren:

Anna Cardillo ist Rechtsanwältin bei Spirit Legal und zudem als Datenschutz-Auditorin sowie externe DSB tätig.

Guido Hansch, LL. M. und CIPP/E, ist Legal Counsel und Group Data Protection Officer bei der codecentric AG in Solingen

Dipl.-Jur. Wolfgang Lehna, CIPP/E, CIPM, FIP (IAPP) ist Konzern-DSB bei der SAMSON GROUP

Heiko Markus Roth, LL. M., ist interner DSB im Konzernumfeld.

Der Beitrag spiegelt die private Meinung der Autoren wider.