Kurzpapier Nr. 12
Datenschutzbeauftragte bei Verantwortlichen und Auftragsverarbeitern

Dieses Kurzpapier der unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz – DSK) dient als erste Orientierung insbesondere für den nicht-öffentlichen Bereich, wie nach Auffassung der DSK die Datenschutz-Grundverordnung (DS-GVO) im praktischen Vollzug angewendet werden sollte. Diese Auffassung steht unter dem Vorbehalt einer zukünftigen - möglicherweise abweichenden - Auslegung des Europäischen Datenschutzausschusses.

Die nachfolgenden Erläuterungen zum Datenschutzbeauftragten (DSB) gelten sowohl für Verantwortliche als auch für Auftragsverarbeiter.

Benennung des DSB

Eine Pflicht zur Benennung eines DSB kann sich sowohl aus der DS-GVO als auch aus dem nationalen Recht ergeben. Eine Benennungspflicht kann für den Verantwortlichen, für den Auftragsverarbeiter oder für beide bestehen, je nachdem wer durch seine Tätigkeit selbst die Voraussetzungen für diese Pflicht erfüllt. Wer bisher einen DSB bestellen musste, muss in der Regel auch weiterhin einen DSB benennen.

Benennung des DSB nach Art. 37 DS-GVO

Nach Art. 37 Abs. 1 lit. a – c DS-GVO ist auf jeden Fall ein DSB zu benennen, wenn eine der folgenden Voraussetzungen gegeben ist:

- Behörde oder öffentliche Stelle (mit Ausnahme von Gerichten, die im Rahmen ihrer justiziellen Tätigkeit handeln),
- Kerntätigkeit mit umfangreicher oder systematischer Überwachung von Personen oder
- Kerntätigkeit mit umfangreicher Verarbeitung besonders sensibler Daten (Artikel 9, 10 DS-GVO).

„Kerntätigkeit" ist die Haupttätigkeit eines Unternehmens, die es untrennbar prägt, und nicht die Verarbeitung personenbezogener Daten als Nebentätigkeit (ErwGr. 97 der DS-GVO). Zu den Kerntätigkeiten gehören danach auch alle Vorgänge, die einen festen Bestandteil der Haupttätigkeit des Verantwortlichen darstellen. Hierzu gehören nicht die das Kerngeschäft unterstützenden Tätigkeiten wie z. B. die Verarbeitung der Beschäftigtendaten der eigenen Mitarbeiter.

Für die Definition des Begriffs "umfangreich" können aus ErwGr 91 der DS-GVO folgende Faktoren herangezogen werden:

- Menge der verarbeiteten personenbezogenen Daten (Volumen),
- Verarbeitung auf regionaler, nationaler oder supranationaler Ebene (geografischer Aspekt),
- Anzahl der betroffenen Personen (absolute Zahl oder in Prozent zur relevanten Bezugsgröße) und
- Dauer der Verarbeitung (zeitlicher Aspekt).

Sind mehrere Faktoren hoch, so kann dies für eine "umfangreiche" Überwachung bzw. Verarbeitung sprechen.

Erfolgt eine Verarbeitung von Patienten- oder Mandantendaten durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufs oder Rechtsanwalt, handelt es sich regelmäßig nicht um eine die Benennungspflicht auslösende umfangreiche Datenverarbeitung (siehe ErwGr. 91). Unter Berücksichtigung der Umstände des Einzelfalls und der konkreten Elemente einer umfangreichen Verarbeitung im Sinne des ErwGr. 91 – beispielsweise bei einer Anzahl von Betroffenen, die erheblich über

den Betroffenenkreis eines durchschnittlichen, durch ErwGr. 91 Satz 4 privilegierten Einzelarztes hinaus geht – kann eine umfangreiche Verarbeitung gegeben sein, sodass ein DSB zu benennen ist. Ungeachtet dessen ist die Benennung generell zu empfehlen, um die Einhaltung der datenschutzrechtlichen Bestimmungen zu erleichtern und damit gegebenenfalls aufsichtsbehördliche Maßnahmen zu vermeiden.

Die Regelung des Art. 37 Abs. 4 S. 1 DS-GVO sieht vor, dass DSBe auch auf freiwilliger Basis benannt werden können. Soweit keine Pflicht zur Benennung eines DSB vorliegt, kann eine freiwillige Benennung eines DSB empfehlenswert sein.

Benennung des DSB bei weiteren Verantwortlichen und Auftragsverarbeitern nach § 38 BDSG-neu

Die EU-Mitgliedsstaaten haben die Möglichkeit, die Pflicht zur Benennung eines DSB in ihren nationalen Ausführungsgesetzen auf weitere Stellen auszudehnen (Art. 37 Abs. 4 S. 1 DS-GVO). Der Bundesgesetzgeber hat diesen Regelungsspielraum genutzt, um die Pflicht zur Benennung von betrieblichen DSBen dem in Deutschland bestehenden „Status quo“ anzupassen (vgl. § 4f BDSG-alt sowie § 38 BDSG-neu).

Demnach ist eine Benennung eines DSB auch in folgenden Fällen erforderlich:

- es werden in der Regel mindestens zehn Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt oder
- es werden Verarbeitungen vorgenommen, die einer Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO unterliegen oder es werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeitet;
- dann muss unabhängig von der Anzahl der mit der Verarbeitung beschäftigten Personen ein DSB benannt werden.

Gemeinsamer DSB

Eine Unternehmensgruppe darf einen gemeinsamen DSB benennen (vgl. Art. 37 Abs. 2 DS-GVO). Voraussetzung hierfür ist, dass der DSB von jeder Niederlassung aus leicht erreicht werden kann. Hiervon ist auch der Fall erfasst, dass nach deutschem Recht eine Pflicht zur Benennung eines DSB besteht und dieser DSB außerhalb Deutschlands für deutsche Niederlassungen benannt wird. In diesem Zusammenhang wird jedoch empfohlen, den DSB in der Europäischen Union anzusiedeln, um die Aufgabenerfüllung in Bezug auf die DS-GVO zu erleichtern.

Behörden oder öffentliche Stellen haben die Möglichkeit, für mehrere Behörden oder Stellen unter Berücksichtigung ihrer Organisationsstruktur und ihrer Größe einen gemeinsamen DSB zu benennen (Art. 37 Abs. 3 DS-GVO). Der Bezug auf Organisationsstruktur und Größe bedeutet auch, dass der Verantwortliche sicherstellen muss, dass der gemeinsame DSB in der Lage ist, die Aufgaben zu erfüllen, welche ihm in Bezug auf sämtliche Behörden oder öffentliche Stellen übertragen wurden.

Leichte Erreichbarkeit des DSB

Es sind Vorkehrungen zu treffen, die es den betroffenen Personen oder anderen Stellen ermöglichen, den DSB leicht zu erreichen (z. B. Einrichtung einer Hotline oder eines Kontaktformulars auf der Homepage). Dem DSB muss eine Kommunikation in der Sprache möglich sein, welche für die Korrespondenz mit Aufsichtsbehörden und betroffenen Personen notwendig ist.

Berufliche Qualifikation und Fachwissen

Der DSB wird aufgrund seiner beruflichen Qualifikation und insbesondere seines Fachwissens auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis sowie seiner Fähigkeit, die Aufgaben gemäß Artikel 39 DS-GVO zu erfüllen, benannt.

Interner und externer DSB

Der DSB kann Beschäftigter des Unternehmens oder der Behörde sein (interner DSB) oder seine Aufgaben aufgrund eines Dienstleistungsvertrages erfüllen (externer DSB, Art. 37 Abs. 6 DS-GVO).

Form der Benennung

Da die DS-GVO lediglich von einer Benennung des DSB spricht, ist eine Schriftform – im Gegensatz zum § 4f Abs. 1 S. 1 BDSG-alt – nicht mehr vorgeschrieben. Aus Beweisgründen im Hinblick auf die Nachweispflichten gemäß Art. 24 Abs. 1 DS-GVO und Art. 5 Abs. 2 DS-GVO und zur Rechtssicherheit ist es jedoch empfehlenswert, die Benennung eines DSB in geeigneter Form zu dokumentieren. Die bereits vor Geltung der DS-GVO und dem BDSG-neu unterzeichneten Bestellungsurkunden gelten vor diesem Hintergrund fort. Die Urkunde und etwaige darin enthaltenen Zusatzvereinbarungen und Aufgabenzuweisungen sollten auf ihre Vereinbarkeit mit den neuen Regelungen der DS-GVO überprüft und ggf. angepasst werden.

Stellung des DSB und Pflichten des Verantwortlichen oder des Auftragsverarbeiters

Der Verantwortliche oder der Auftragsverarbeiter muss die Weisungsfreiheit des DSB bei der Erfüllung seiner Aufgaben sicherstellen. Der DSB darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden. Der besondere Abberufungs- und Kündigungsschutz für DSB gemäß § 4f Abs. 3 S. 4 – 6 BDSG-alt ist im BDSG-neu beibehalten worden (§ 6 Abs. 4 i. V. m. § 38 Abs. 2 BDSG-neu). Der DSB berichtet unmittelbar der höchsten Leitungsebene (Art. 38 Abs. 3 S. 3 DS-GVO).

Es muss nach Art. 38 DS-GVO sichergestellt werden, dass der DSB ordnungsgemäß und frühzeitig in alle Datenschutzfragen eingebunden wird. Der DSB muss bei der Erfüllung seiner Aufgaben unterstützt werden, indem ihm Folgendes zur Verfügung gestellt wird:

- die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen (einschließlich Personals),
- der Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie
- die zur Erhaltung seines Fachwissens erforderlichen Ressourcen.

Der DSB ist bei der Erfüllung seiner Aufgaben zur Wahrung der Geheimhaltung oder Vertraulichkeit verpflichtet. Das BDSG-neu regelt für DSB ergänzend die Pflicht zur Verschwiegenheit über die Identität der betroffenen Person, die den DSB zu Rate zieht, sowie über die Umstände, die Rückschlüsse auf die betroffene Person zulassen. Darüber hinaus erstreckt § 6 Abs. 6 i. V. m. § 38 Abs. 2 BDSG-neu die Pflicht zur Wahrung der Geheimhaltung und Vertraulichkeit auf das Zeugnisverweigerungsrecht.

Der Verantwortliche kann dem DSB noch weitere Aufgaben übertragen, wobei er sicherstellen muss, dass keine Interessenkonflikte auftreten. Dies ist insbesondere anzunehmen, wenn gleichzeitig Positionen des leitenden Managements wahrgenommen werden oder die Tätigkeitsfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen.

Aufgaben des DSB

Der DSB hat nach Art. 39 DS-GVO folgende Aufgaben:

- Unterrichtung und Beratung des Verantwortlichen und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Datenschutz-Pflichten (lit. a);
- Überwachung der Einhaltung der Datenschutzvorschriften sowie der Strategien des Verantwortlichen für den Schutz personenbezogener Daten einschließlich der Zuweisung von Zuständigkeiten, der Sensibilisierung und Schulung der an den Verarbeitungsvorgängen beteiligten Mitarbeiter und der diesbezüglichen Überprüfungen (lit. b);

- Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung nach Art. 35 DS-GVO und Überwachung ihrer Durchführung (lit. c);
- Zusammenarbeit mit der Aufsichtsbehörde (lit. d) und Tätigkeit als Anlaufstelle für die Aufsichtsbehörde (lit. e).

Hinzu kommt die Beratung der betroffenen Personen zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß der DS-GVO im Zusammenhang stehenden Fragen (Art. 38 Abs. 4 DS-GVO).

Risikoorientierte Aufgabenerfüllung durch den DSB

Der DSB nimmt seine Aufgaben nach Art. 39 Abs. 2 DS-GVO risikoorientiert wahr. Er trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

Verantwortung für die Einhaltung der DS-GVO

Die DS-GVO stellt in Art. 24 Abs. 1 DS-GVO ausdrücklich klar, dass es die Pflicht des Verantwortlichen bzw. des Auftragsverarbeiters – und nicht die des DSB – bleibt, sicherzustellen und nachzuweisen, dass die Datenverarbeitungen im Einklang mit den Regelungen der DS-GVO stehen. Gleichwohl sollte der DSB seine Tätigkeiten in angemessener Weise dokumentieren, um ggf. nachweisen zu können, dass er seinen Aufgaben (insbesondere Unterrichtung und Beratung) ordnungsgemäß nachgekommen ist.

Veröffentlichungs- und Mitteilungspflichten der Kontaktdaten des DSB

Die Kontaktdaten des DSB sind nach Art. 37 Abs. 7 DS-GVO zu veröffentlichen und der Aufsichtsbehörde mitzuteilen. Die Aufsichtsbehörden werden den mitteilungspflichtigen Stellen ein Formular zur Mitteilung der Kontaktdaten des DSB zur Verfügung stellen.

Rechtsfolgen bei Verstoß

Verletzungen der Vorschriften zum DSB aus Art. 37 bis 39 DS-GVO (z. B. Nicht-Benennung oder unzureichende Unterstützung des DSB) sind nach Art. 83 Abs. 4 lit. a DS-GVO mit Geldbuße bedroht.

Hinweis

Die Artikel-29-Datenschutzgruppe hat zur näheren Erläuterung der Art. 37 bis 39 DS-GVO inzwischen *„Leitlinien in Bezug auf Datenschutzbeauftragte“* (Working Paper 243) erstellt.