WP243 ANHANG – HÄUFIG GESTELLTE FRAGEN

Mit diesem Anhang soll in einem vereinfachten und lesefreundlichen Format eine Reihe der wichtigsten Fragen beantwortet werden, die sich Einrichtungen in Bezug auf die neuen Anforderungen der DS-GVO in Bezug auf die Ernennung eines DSB möglicherweise stellen.

Benennung des DSB (Artikel 37)

1 Welche Einrichtungen sind zur Benennung eines DSB verpflichtet? (Artikel 37 Absatz 1)

In der DS-GVO ist die Benennung eines DSB in drei bestimmten Fällen zwingend vorgeschrieben:

- wenn die Verarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird (unabhängig von der Art der verarbeiteten Daten);
- wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Verarbeitungsvorgängen besteht, welche eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, und
- wenn die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten besteht.

Hierbei ist zu beachten, dass Rechtsvorschriften der Union oder der Mitgliedstaaten die Benennung eines DSB auch in anderen Fällen vorschreiben können. Schließlich können Einrichtungen es auch in Fällen, in denen die DS-GVO nicht ausdrücklich die Benennung eines DSB vorsieht, für sinnvoll erachten, einen solchen auf freiwilliger Basis zu ernennen. Die Artikel-29-Datenschutzgruppe („WP29“) befürwortet derartige freiwillige Anstrengungen.

Weitere Informationen finden sich in Abschnitt 2.1 der Leitlinien.

2 Wie ist der Begriff „Kerntätigkeiten“ zu verstehen? (Artikel 37 Absatz 1 Buchstaben b und c)

Als „Kerntätigkeiten“ sind die wichtigsten Vorgänge anzusehen, die zur Erreichung der vom Verantwortlichen oder Auftragsverarbeiter verfolgten Ziele erforderlich sind. Dies schließt auch alle Tätigkeiten ein, bei denen die Verarbeitung von Daten einen festen Bestandteil der Tätigkeit des Verantwortlichen oder Auftragsverarbeiters darstellt. Beispielsweise ist die Verarbeitung gesundheitsbezogener Daten, wie etwa Patientenakten als eine der Kerntätigkeiten eines Krankenhauses anzusehen, weshalb Krankenhäuser zur Benennung eines DSB verpflichtet sind.

Andererseits führen alle Einrichtungen bestimmte Unterstützungstätigkeiten aus, wie etwa die Entlohnung ihrer Mitarbeiter oder die Leistung von Standard-IT-Support. Hierbei handelt es sich um für die Kerntätigkeit oder das Kerngeschäft der Einrichtung notwendige Unterstützungsfunktionen. Trotz ihrer Notwendigkeit oder Unverzichtbarkeit werden solche Tätigkeiten gemeinhin eher als Nebenfunktionen denn als Kerntätigkeit angesehen.

Weitere Informationen finden sich in Abschnitt 2.1.2 der Leitlinien.

3 Wie ist der Begriff „umfangreich“ zu verstehen? (Artikel 37 Absatz 1 Buchstaben b und c)

In der DS-GVO ist nicht festgelegt, was der Begriff „umfangreich“ bedeutet. Die WP29 empfiehlt, bei der Klärung der Frage, ob eine umfangreiche Verarbeitung vorliegt, die folgenden Faktoren zu berücksichtigen:

- die Zahl der betroffenen Personen – entweder als spezifische Zahl oder als Anteil an der maßgeblichen Bevölkerung
- das Datenvolumen und/oder die Bandbreite der verarbeiteten Datenelemente
- die Dauer oder Permanenz der Datenverarbeitungstätigkeit
- die geografische Ausdehnung der Verarbeitungstätigkeit

Beispiele für eine umfangreiche Verarbeitung stellen dar:

- die Verarbeitung von Patientendaten im gewöhnlichen Geschäftsbetrieb eines Krankenhauses
- die Verarbeitung von Reisedaten natürlicher Personen, die ein Verkehrsmittel des kommunalen ÖPNV nutzen (z. B. Nachverfolgung über Netzkarten)
- die Verarbeitung von Geolokalisierungsdaten von Kunden einer internationalen Fast-food-Kette in Echtzeit zu statistischen Zwecken durch einen auf Tätigkeiten dieser Art spezialisierten Auftragsverarbeiter
- die Verarbeitung von Kundendaten im gewöhnlichen Geschäftsbetrieb eines Versicherungsunternehmens oder einer Bank
- die Verarbeitung personenbezogener Daten durch eine Suchmaschine zu Zwecken der verhaltensbasierten Werbung
- die Verarbeitung von Daten (Inhalte, Datenverkehrsaufkommen, Standort) durch Telefon- oder Internetdienstleister

Keine umfangreiche Verarbeitung stellen die folgenden Beispiele dar:

- die Verarbeitung von Patientendaten durch einen einzelnen Arzt
- die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten durch einen einzelnen Rechtsanwalt

Weitere Informationen finden sich in Abschnitt 2.1.3 der Leitlinien.

4 Wie ist der Begriff „regelmäßige und systematische Überwachung“ zu verstehen? (Artikel 37 Absatz 1 Buchstabe b)

Der Begriff „regelmäßige und systematische Überwachung“ ist in der DS-GVO zwar nicht definiert, beinhaltet jedoch jegliche Formen der Verfolgung und Profilerstellung im Internet, darunter auch zu Zwecken der verhaltensbasierten Werbung. Allerdings ist der Begriff „Überwachung“ nicht auf die Online-Umgebung beschränkt.

Die WP29 interpretiert den Begriff „regelmäßig“ als mindestens eine der folgenden Eigenschaften:

- fortlaufend oder in bestimmten Abständen während eines bestimmten Zeitraums vorkommend
- immer wieder oder wiederholt zu bestimmten Zeitpunkten auftretend
- ständig oder regelmäßig stattfindend

Die WP29 interpretiert den Begriff „systematisch“ als mindestens eine der folgenden Eigenschaften:

- systematisch vorkommend
- vereinbart, organisiert oder methodisch
- im Rahmen eines allgemeinen Datenerfassungsplans erfolgend
- im Rahmen einer Strategie erfolgend

Beispiele: Betrieb eines Telekommunikationsnetzes, Anbieten von Telekommunikationsdienstleistungen, verfolgende E-Mail-Werbung, Typisierung und Scoring zu Zwecken der Risikobewertung (zum Beispiel zu Zwecken der Kreditvergabe, der Festlegung von Versicherungsprämien, Maßnahmen zur Verhinderung von betrügerischen Handlungen, Ermittlung von Geldwäsche), Standortverfolgung (beispielsweise durch Mobilfunkanwendungen), Treueprogramme, verhaltensbasierte Werbung, Überwachung von Wellness-, Fitness- und gesundheitsbezogenen Daten über in Kleidung integrierte Geräte (Wearables), Überwachungskameras oder vernetzte Geräte (zum Beispiel intelligente Stromzähler, intelligente Autos, Haustechnik usw.)

Weitere Informationen finden sich in Abschnitt 2.1.4 der Leitlinien.

5 Können Einrichtungen gemeinsam einen DSB benennen? Falls ja, unter welchen Voraussetzungen? (Artikel 37 Absätze 2 und 3)

In der DS-GVO ist vorgesehen, dass eine Unternehmensgruppe einen gemeinsamen DSB ernennen kann, falls dieser „*von jeder Niederlassung aus […] leicht erreicht werden kann*“. Der Begriff „Erreichbarkeit“ bezieht sich auf die Aufgaben des DSB als Ansprechpartner für Betroffene, für die Aufsichtsbehörde und einrichtungsintern. Um die Erreichbarkeit des DSB sowohl intern als auch extern zu gewährleisten, ist dafür Sorge zu tragen, dass die Kontaktdaten im Einklang mit der DS-GVO zur Verfügung stehen. Der DSB muss in der Lage sein, mit dem Betroffenen wirksam zu kommunizieren und mit den zuständigen Aufsichtsbehörden effektiv zusammenzuarbeiten. Dies bedeutet, dass die Kommunikation in der bzw. den von den Aufsichtsbehörden und dem Betroffenen verwendeten Sprache(n) erfolgen muss. Damit die Betroffenen den DSB kontaktieren können, ist es unverzichtbar, dass dieser (entweder physisch auf dem gleichen Gelände wie die Beschäftigten oder über eine Hotline oder andere sichere Kommunikationskanäle) persönlich erreichbar ist.

Weitere Informationen finden sich in Abschnitt 2.3 der Leitlinien.

6 Besteht die Möglichkeit zur Ernennung eines externen DSB (Artikel 37 Absatz 6)?

Diese Möglichkeit ist gegeben. Nach Artikel 37 Absatz 6 kann der DSB Beschäftigter des Verantwortlichen oder des Auftragsverarbeiters sein (interner DSB) oder aber „seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen“. Dies bedeutet, dass der DSB durchaus eine externe Person sein kann; in einem solchen Falle kann seine Funktion auf Grundlage eines mit einer Einzelperson oder einer Einrichtung geschlossenen Dienstleistungsvertrags ausgeübt werden.

Die Bestimmungen der Artikel 37 bis 39 gelten auch für einen externen DSB. Wie in den Leitlinien dargelegt, kann in dem Fall, dass die Funktion des DSB von einem externen Dienstleister wahrgenommen wird, ein Team aus für diese Stelle tätigen Personen die Aufgaben eines DSB unter der Verantwortung eines ernannten primären Ansprechpartners und „Sachbearbeiters“ des Kunden in effizienter Weise ausführen. In einem solchen Falle ist es unverzichtbar, dass jeder Angehörige der externen Einrichtung, der die Funktionen eines DSB ausübt, alle einschlägigen Anforderungen der DS-GVO erfüllt.

Im Interesse der Rechtssicherheit und einer ordnungsgemäßen Organisation wird in den Leitlinien empfohlen, im Dienstleistungsvertrag eine klare Aufgabenverteilung innerhalb des externen DSB-Teams vorzusehen und eine einzelne Person als primären Ansprechpartner festzulegen, die zugleich für den jeweiligen Kunden „zuständig“ ist.

Weitere Informationen finden sich in den Abschnitten 2.3, 2.4 und 2.5 der Leitlinien.

7 Über welche berufliche Qualifikation sollte der DSB verfügen (Artikel 37 Absatz 5)?

Die DS-GVO sieht vor, dass der Datenschutzbeauftragte aufgrund seiner beruflichen Qualifikation und insbesondere des Fachwissens ernannt wird, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie aufgrund seiner Befähigung, die in Artikel 39 genannten Aufgaben zu erfüllen.

Das erforderliche Niveau des Fachwissens sollte sich insbesondere nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz der verarbeiteten personenbezogenen Daten richten. Wenn etwa eine Datenverarbeitungstätigkeit besonders komplex ist oder in großem Umfang sensible Informationen betrifft, bedarf der DSB unter Umständen eines höheren Maßes an Fachkompetenz und Unterstützung.

Zu den geforderten Fähigkeiten und Fachkenntnissen gehören:

- Fachkenntnisse auf dem Gebiet des einzelstaatlichen und des gemeinschaftlichen Datenschutzrechts und der diesbezüglichen Anwendungspraxis einschließlich eines fundierten Verständnisses der DS-GVO
- Verständnis der durchgeführten Datenverarbeitungsvorgänge
- Vertrautheit mit Informationstechnologien und Datensicherheit
- Kenntnis der Branche und der Einrichtung
- die Fähigkeit, die Verbreitung einer Datenschutzkultur innerhalb der Einrichtung zu fördern

Weitere Informationen finden sich in Abschnitt 2.4 der Leitlinien.

Stellung des DSB (Artikel 38)

8 Welche Ressourcen sollten dem DSB zur Wahrnehmung seiner Aufgaben zur Verfügung stehen?

Artikel 38 Absatz 2 der DS-GVO sieht vor, dass Einrichtungen ihrem DSB Unterstützung leisten, „*indem sie die für die Erfüllung [seiner] Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellen*“.

Je nach Art der Datenverarbeitungsvorgänge und des Tätigkeitsfelds und der Größe der Einrichtung sollten dem DSB die folgenden Ressourcen zur Verfügung stehen:

- aktive Unterstützung von Seiten des leitenden Managements bei der Erfüllung seiner Funktion
- genügend Zeit zur Erfüllung seiner Pflichten

- angemessene Unterstützung durch Finanzmittel, Infrastrukturen (Räumlichkeiten, Einrichtungen, Ausrüstung) und ggf. Personal
- offizielle Unterrichtung des gesamten Personals über die Ernennung des DSB
- Zugang zu anderen Dienststellen der Einrichtung, damit der DSB von diesen wesentliche Unterstützung, Anregungen und Informationen erhalten kann
- kontinuierliche Fortbildung

Weitere Informationen finden sich in Abschnitt 3.2 der Leitlinien.

9 Durch welche Vorkehrungen soll sichergestellt werden, dass der DSB seinen Aufgaben in unabhängiger Weise nachgehen kann (Artikel 38 Absatz 3)?

Es wurden eine Reihe von Vorkehrungen getroffen, damit der DSB in unabhängiger Weise agieren kann, wie dies in Erwägungsgrund 97 gefordert wird:

- keine Anleitung durch die Verantwortlichen oder die Auftragsverarbeiter im Hinblick auf die Ausübung der Aufgaben des DSB
- keine in der Erfüllung seiner Aufgaben begründete Abberufung oder Benachteiligung des DSB durch den Verantwortlichen
- keine Interessenkonflikte aufgrund möglicher anderer Aufgaben und Pflichten

Weitere Informationen finden sich in den Abschnitten 3.3. bis 3.5 der Leitlinien.

10 Welche „anderen Aufgaben und Pflichten“ (Artikel 38 Absatz 6) eines DSB können einen Interessenkonflikt zur Folge haben?

Der DSB darf innerhalb der Einrichtung insbesondere keine Position innehaben, welche es mit sich bringt, dass er die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt. Aufgrund der jeder Einrichtung eigenen strukturellen Unterschiede ist diese Frage fallweise zu betrachten.

Als Faustregel lassen sich zu den mit Interessenkonflikten einhergehenden Positionen solche des leitenden Managements (wie etwa Leiter des Unternehmens, Leiter des operativen Geschäftsbereichs, Finanzvorstand, leitender medizinischer Direktor, Leiter der Marketingabteilung, Leiter der Personalabteilung oder Leiter der IT-Abteilung) zählen, jedoch auch hierarchisch nachgeordnete Positionen, wenn die betreffenden Funktionen oder Aufgabenfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen.

Weitere Informationen finden sich in Abschnitt 3.5 der Leitlinien.

Aufgaben des DSB (Artikel 39)

11 Worauf erstreckt sich der Begriff „Überwachung der Einhaltung der DS-GVO“ (Artikel 39 Absatz 1 Buchstabe b)?

Im Rahmen ihrer diesbezüglichen Überwachungspflichten sind DSB insbesondere befugt,

- Informationen zur Ermittlung von Datenverarbeitungstätigkeiten zu sammeln,
- die Einhaltung der Vorgaben bei Datenverarbeitungstätigkeiten zu analysieren und zu kontrollieren sowie

- den Verantwortlichen oder den Auftragsverarbeiter zu unterrichten und zu beraten und ihm Empfehlungen zu unterbreiten.

Weitere Informationen finden sich in Abschnitt 4.1 der Leitlinien.

12 Kann der DSB für Verstöße gegen die DS-GVO persönlich zur Verantwortung gezogen werden?

Nein, DSB tragen im Falle der Nichteinhaltung der DS-GVO keine persönliche Verantwortung. Aus der DS-GVO geht klar hervor, dass es Sache des Verantwortlichen oder des Auftragsverarbeiters ist, sicherzustellen und nachweisen zu können, dass die Verarbeitung im Einklang mit dieser Verordnung erfolgt (Artikel 24 Absatz 1). Die Einhaltung der datenschutzrechtlichen Bestimmungen fällt in die Zuständigkeit des Verantwortlichen oder des Auftragsverarbeiters.

13 Welche Funktion kommt dem DSB in Bezug auf Datenschutz-Folgenabschätzungen (Artikel 37 Absatz 1 Buchstabe c) und die Führung eines Verzeichnisses aller Verarbeitungstätigkeiten (Artikel 30) zu?

In Bezug auf die Datenschutz-Folgenabschätzung sollte der Verantwortliche oder der Auftragsverarbeiter den DSB insbesondere dann zu Rate ziehen, wenn es um die Frage geht,

- ob eine DS-Folgenabschätzung durchgeführt werden sollte oder nicht,
- welche Methodik bei der Durchführung einer solchen DS-Folgenabschätzung angewandt werden sollte,
- ob diese DS-Folgenabschätzung intern oder extern erfolgen sollte,
- welche Sicherheitsvorkehrungen (einschließlich technischer und organisatorischer Maßnahmen) getroffen werden sollten, um bestehenden Bedrohungen der Rechte und Interessen der Betroffenen zu begegnen,
- ob eine solche Datenschutz-Folgenabschätzung ordnungsgemäß durchgeführt worden ist und ob die daraus gezogenen Schlussfolgerungen (bezüglich der Frage, ob die Datenverarbeitung fortgesetzt werden sollte oder nicht und welche Sicherheitsvorkehrungen gegebenenfalls getroffen werden sollten) im Einklang mit der DS-GVO stehen.

Weitere Informationen finden sich in Abschnitt 4.2 der Leitlinien.

Was die Aufzeichnung der Datenverarbeitungstätigkeiten anbelangt, so ist es Sache des Verantwortlichen oder des Auftragsverarbeiters - und nicht des DSB -, ein Verzeichnis der Verarbeitungsvorgänge zu führen. Allerdings hindert den Verantwortlichen oder den Auftragsverarbeiter nichts daran, dem DSB die Aufgabe zu übertragen, unter der Verantwortung des Verantwortlichen ein Verzeichnis der Verarbeitungsvorgänge zu führen. Ein solches Verzeichnis sollte als eines der Instrumente angesehen werden, die den DSB in die Lage versetzen, die ihm in Bezug auf die Überwachung der Vorschrifteneinhaltung und in Bezug auf die Unterrichtung und Beratung des Verantwortlichen bzw. des Auftragsverarbeiters obliegenden Aufgaben wahrzunehmen.

Weitere Informationen finden sich in Abschnitt 4.4 der Leitlinien.