



Leitlinien in Bezug auf Datenschutzbeauftragte („DSB“)

angenommen am 13. Dezember 2016

zuletzt überarbeitet und angenommen am 5. April 2017

Die Datenschutzgruppe wurde nach Artikel 29 der Richtlinie 95/46/EG eingesetzt. Sie ist ein unabhängiges Beratungsgremium der EU zum Themenkreis Datenschutz und Schutz der Privatsphäre. Ihr Aufgabenbereich geht aus Artikel 30 der Richtlinie 95/46/EG und Artikel 15 der Richtlinie 2002/58/EG hervor.

Die Sekretariatsaufgaben werden von der Direktion C (Grundrechte und Rechtsstaatlichkeit) der Europäischen Kommission, Generaldirektion Justiz und Verbraucher, 1049 Brüssel, Belgien, Büro MO59 05/35 wahrgenommen.

Website: http://ec.europa.eu/justice/data-protection/index_en.htm (in englischer Sprache)

DIE ARBEITSGRUPPE FÜR DIE WAHRUNG DER RECHTE VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN –

eingesetzt nach der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf die Artikel 29 und 30 dieser Richtlinie

gestützt auf ihre Geschäftsordnung –

HAT DIE FOLGENDEN LEITLINIEN ANGENOMMEN:

Inhaltsverzeichnis

| | | |
|-----------|---|-----------|
| 1 | EINFÜHRUNG | 4 |
| 2 | BENENNUNG EINES DSB | 5 |
| | 2.1. OBLIGATORISCHE BENENNUNG | 5 |
| | 2.1.1 „Behörden oder öffentliche Stellen“ | 6 |
| | 2.1.2 „Kerntätigkeit“ | 8 |
| | 2.1.3 „Umfangreiche Verarbeitung“ | 9 |
| | 2.1.4 „Regelmäßige und systematische Überwachung“ | 10 |
| | 2.1.5 Besondere Kategorien von Daten und Daten über strafrechtliche Verurteilungen und Straftaten . | 11 |
| | 2.2. DSB DES AUFTRAGSVERARBEITERS | 11 |
| | 2.3. BENENNUNG EINES GEMEINSAMEN DSB FÜR MEHRERE ORGANISATIONEN | 12 |
| | 2.4. ERREICHBARKEIT UND STANDORT DES DSB | 13 |
| | 2.5. FÄHIGKEITEN UND FACHKENNTNISSE DES DSB | 13 |
| | 2.6. VERÖFFENTLICHUNG UND MITTEILUNG DER KONTAKTDATEN DES DSB | 15 |
| 3 | STELLUNG DES DSB | 16 |
| | 3.1. EINBINDUNG DES DSB IN ALLE MIT DEM SCHUTZ PERSONENBEZOGENER DATEN IN ZUSAMMENHANG STEHENDE ANGELEGENHEITEN | 16 |
| | 3.2. ERFORDERLICHE RESSOURCEN | 16 |
| | 3.3. ANWEISUNGEN UND „AUSÜBUNG DER PFLICHTEN UND AUFGABEN IN VOLLSTÄNDIGER UNABHÄNGIGKEIT“ | 17 |
| | 3.4. ABBERUFUNG ODER BENACHTEILIGUNG DES DSB WEGEN DER ERFÜLLUNG SEINER AUFGABEN | 18 |
| | 3.5. INTERESSENKONFLIKTE | 19 |
| 4 | AUFGABEN DES DSB | 20 |
| | 4.1. ÜBERWACHUNG DER EINHALTUNG DER DS-GVO..... | 20 |
| | 4.2. DIE FUNKTION DES DSB BEI EINER DATENSCHUTZ-FOLGENABSCHÄTZUNG..... | 20 |
| | 4.3. ZUSAMMENARBEIT MIT DER AUFSICHTSBEHÖRDE UND TÄTIGKEIT ALS ANLAUFSTELLE | 21 |
| | 4.4. RISIKOBASIERTER ANSATZ | 22 |
| | 4.5. DIE FUNKTION DES DSB BEI DER FÜHRUNG VON VERZEICHNISSSEN | 22 |
| 5 | ANHANG ZU DEN DSB-LEITLINIEN: WAS SIE WISSEN MÜSSEN | 24 |
| | BENENNUNG DES DSB | 24 |
| 1 | WELCHE EINRICHTUNGEN SIND ZUR BENENNUNG EINES DSB VERPFLICHTET? | 24 |
| 2 | WAS BEDEUTET „KERNTÄTIGKEIT“? | 24 |
| 3 | WAS BEDEUTET „UMFANGREICHE BEARBEITUNG“? | 25 |
| 4 | WAS BEDEUTET „REGELMÄßIGE UND SYSTEMATISCHE ÜBERWACHUNG“? | 25 |
| 5 | KÖNNEN EINRICHTUNGEN EINEN GEMEINSAMEN DSB BENENNEN? WENN JA, UNTER WELCHEN VORAUSSETZUNGEN? | 26 |
| 6 | WO SOLLTE DER DSB LOKALISIERT SEIN? | 26 |
| 7 | KANN EIN EXTERNER DSB BESTELLT WERDEN? | 27 |
| 8 | ÜBER WELCHE BERUFLICHEN QUALIFIKATIONEN SOLLTE DER DSB VERFÜGEN? | 27 |
| | STELLUNG DES DSB | 28 |
| 9 | WELCHE RESSOURCEN SOLLTEN VERANTWORTLICHE ODER AUFTRAGSVERARBEITER DEM DSB ZUR VERFÜGUNG STELLEN? | 28 |
| 10 | WIE WIRD DIE AUSÜBUNG DER PFLICHTEN UND AUFGABEN DES DSB IN VOLLSTÄNDIGER UNABHÄNGIGKEIT GEWÄHRLEISTET? WAS BEDEUTET „INTERESSENKONFLIKT“? | 28 |
| | AUFGABEN DES DSB | 29 |
| 11 | WAS BEDEUTET „EINHALTUNG DER VORGABEN IN BEZUG AUF DIE ÜBERWACHUNG“ | 29 |
| 12 | IST DER DSB IM FALL DER NICHTEINHALTUNG DER DATENSCHUTZANFORDERUNGEN PERSÖNLICH VERANTWORTLICH? | 29 |
| 13 | WELCHE FUNKTION KOMMEN DEM DSB BEI EINER DATENSCHUTZ-FOLGENABSCHÄTZUNG UND BEIM FÜHREN VON VERZEICHNISSSEN ZU VERARBEITUNGSVORGÄNGEN ZU? | 29 |

1 Einführung

Die Datenschutz-Grundverordnung (DS-GVO)¹, die am 25. Mai 2018 in Kraft treten soll, wird einen modernisierten, auf dem Prinzip der Rechenschaftspflicht beruhenden Handlungsrahmen für die Überprüfung der Einhaltung der Datenschutzvorschriften in Europa bieten. Den Kern dieser neuen Rechtsgrundlage werden für viele Einrichtungen Datenschutzbeauftragte (DSB) bilden, die die Einhaltung der Bestimmungen der DS-GVO erleichtern.

Nach der DS-GVO sind Verantwortliche und Auftragsverarbeiter unter bestimmten Voraussetzungen verpflichtet, einen DSB² zu ernennen. Diese Pflicht besteht für alle Behörden und öffentlichen Stellen (unabhängig von der Art der verarbeiteten Daten) wie auch für sonstige Einrichtungen, die – als Kerntätigkeit – systematisch und in großem Umfang Einzelpersonen überwachen oder in großem Umfang besondere Kategorien von personenbezogenen Daten verarbeiten.

In Fällen, in denen die DS-GVO die Bestellung eines DSB nicht ausdrücklich vorschreibt, können Einrichtungen es mitunter für zweckmäßig erachten, einen solchen auf freiwilliger Basis zu ernennen. Die Artikel-29-Datenschutzgruppe („WP29“)³ fördert derartige freiwillige Anstrengungen.

Das dem DSB zugrundeliegende Konzept ist nicht neu. Wenngleich nach der Richtlinie 95/46/EG³ keine Einrichtung zur Ernennung eines DSB verpflichtet ist, hat sich die Praxis der Ernennung eines DSB in zahlreichen Mitgliedstaaten im Laufe der Jahre immer mehr verbreitet.

Vor dem Erlass der DS-GVO argumentierte die WP29, dass der DSB ein wichtiger Akteur im Bereich der Rechenschaftspflicht sei und dass die Ernennung eines DSB die Einhaltung der Vorschriften erleichtere und überdies Unternehmen als Wettbewerbsinstrument diene.⁴ DSB erleichtern nicht nur die Einhaltung der Bestimmungen, indem sie etwa Instrumente zur Anwendung bringen, die der Einhaltung der Rechenschaftspflicht dienen (wie etwa die Erleichterung oder Durchführung von Datenschutz-Folgenabschätzungen und -Überprüfungen), sondern fungieren darüber hinaus auch als Mittler zwischen den maßgeblichen Interessenträgern (z. B. Aufsichtsbehörden, betroffene Personen und für die Geschäftsführung zuständige Stellen einer Einrichtung).

¹Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung) (ABl. L 119 vom 4.5.2016). Die DS-GVO ist mit Bedeutung für den EWR und wird nach ihrer Aufnahme in das EWR-Abkommen angewendet.

² Auch bei den zuständigen Behörden ist die Ernennung eines DSB zwingend vorgeschrieben nach Artikel 32 der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (ABl. L 119 vom 4.5.2016, S. 89) und nach den nationalen Durchführungsbestimmungen. Diese Leitlinien stellen zwar vorrangig auf DSB im Rahmen der DS-GVO ab, sind jedoch auch für DSB im Rahmen der Richtlinie 2016/680 im Hinblick auf die darin enthaltenen ähnlichen Bestimmungen relevant.

³ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).

⁴ Vgl. http://ec.europa.eu/justice/data-protection/article-29/documentation/other-document/files/2015/20150617_appendix_core_issues_plenary_de.pdf

DSB sind im Falle der Nichteinhaltung der DS-GVO nicht persönlich verantwortlich. Aus der DS-GVO geht klar hervor, dass es Aufgabe des Verantwortlichen oder des Auftragsverarbeiters ist, sicherzustellen und nachweisen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt (Artikel 24 Absatz 1). Für die Einhaltung der datenschutzrechtlichen Bestimmungen ist der Verantwortliche oder der Auftragsverarbeiter verantwortlich.

Dem Verantwortlichen oder dem Auftragsverarbeiter kommt zugleich eine wichtige Rolle dabei zu, die Voraussetzung dafür zu schaffen, dass der DSB seinen Aufgaben wirksam nachgehen kann. Die Ernennung eines DSB stellt hierbei nur einen ersten Schritt dar: Um ihren Aufgaben wirksam nachgehen zu können, müssen DSB auch über hinreichende Eigenständigkeit und genügend Ressourcen verfügen.

In der DS-GVO werden die Bedeutung des DSB als Schlüsselfigur im neuen Data-Governance-System anerkannt und die Bedingungen für seine Ernennung, Stellung und Aufgaben dargelegt. Ziel dieser Leitlinien ist es, die einschlägigen Bestimmungen der DS-GVO klarzustellen, um die Verantwortlichen und Auftragsverarbeiter bei der Erfüllung der gesetzlichen Vorgaben zu unterstützen und den DSB bei ihrer Tätigkeit Hilfestellung zu leisten. Die Leitlinien enthalten zugleich Empfehlungen für bewährte Verfahren, denen die in verschiedenen EU-Mitgliedstaaten gesammelten Erfahrungen zugrunde liegen. Die WP29 wird die Umsetzung dieser Leitlinien beaufsichtigen und erforderlichenfalls im Detail ergänzen.

2 Benennung eines DSB

2.1. Obligatorische Benennung

Nach Artikel 37 Absatz 1 der DS-GVO ist die Benennung eines DSB in drei bestimmten Fällen⁵ vorgeschrieben:

- a) falls die Datenverarbeitung durch Behörden oder öffentliche Stellen erfolgt⁶,
- b) falls die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in Datenverarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang erfordern, oder
- c) falls die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten⁷ oder⁸ von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten⁹ besteht.

⁵ Hierbei ist zu beachten, dass nach Artikel 37 Absatz 4 Gemeinschafts- oder einzelstaatliche Rechtsvorschriften die Benennung eines DSB auch in anderen Fällen zwingend erforderlich machen können.

⁶ mit Ausnahme von Gerichten, die in ihrer justiziellen Eigenschaft agieren. Siehe Artikel 32 der Richtlinie (EU) 2016/680.

⁷ Nach Artikel 9 zählen hierzu personenbezogene Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen, sowie die Verarbeitung von genetischen Daten, biometrischen Daten zur eindeutigen Identifizierung einer natürlichen Person, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung einer natürlichen Person.

⁸ In Artikel 37 Absatz 1 Buchstabe c wird das Wort „und“ verwendet. Erläuterungen zur Verwendung von „oder“ anstelle von „und“ finden sich nachfolgend in Abschnitt 2.1.5.

⁹ Artikel 10.

In den nachfolgenden Unterabschnitten stellt die WP29 Anleitungen in Bezug auf die in Artikel 37 Absatz 1 zugrunde gelegten Kriterien und die darin enthaltene Terminologie bereit.

Sofern eine Einrichtung offenkundig nicht verpflichtet ist, einen DSB zu benennen, empfiehlt die WP29, dass die Verantwortlichen und Auftragsverarbeiter die durchgeführte interne Analyse zur Klärung der Frage, ob ein DSB benannt werden muss, dokumentieren, um nachweisen zu können, dass die maßgeblichen Faktoren ordnungsgemäß berücksichtigt wurden.¹⁰ Diese Analyse ist Teil der Dokumentation nach dem Prinzip der Rechenschaftspflicht. Sie kann von der Aufsichtsbehörde angefordert werden und ist gegebenenfalls zu aktualisieren, z. B. wenn die Verantwortlichen oder die Auftragsverarbeiter neue Tätigkeiten durchführen oder neue Leistungen erbringen, die unter Artikel 37 Absatz 1 fallen können.

Wenn eine Einrichtung einen DSB auf freiwilliger Basis ernennt, so unterliegen dessen Benennung Artikel 37 bis 39, Stellung und Aufgabenbereich den Anforderungen wie bei einer obligatorischen Benennung.

Einer Einrichtung, die zur Benennung eines DSB nicht gesetzlich verpflichtet ist und die nicht gewillt ist, einen solchen auf freiwilliger Basis zu benennen, steht es frei, Mitarbeiter oder externe Berater/Beraterinnen mit Aufgaben zu betrauen, die mit dem Schutz personenbezogener Daten in Zusammenhang stehen. In einem solchen Fall gilt es jegliche Unklarheit hinsichtlich ihrer Funktionsbezeichnung, ihres Status, ihrer Stellung und ihres Aufgabenfelds zu vermeiden. Daher sollte aus allen Mitteilungen innerhalb des Unternehmens und gegenüber Datenschutzbehörden, betroffenen Personen und der breiten Öffentlichkeit klar hervorgehen, dass die Funktionsbezeichnung der natürlichen Person bzw. des Beraters/der Beraterin nicht die eines Datenschutzbeauftragten (DSB) ist.¹¹

Der DSB wird für alle vom Verantwortlichen oder Auftragsverarbeiter durchgeführten Verarbeitungsvorgänge ernannt, unabhängig davon, ob die Ernennung obligatorisch ist oder auf freiwilliger Basis erfolgt.

2.1.1 „BEHÖRDEN ODER ÖFFENTLICHE STELLEN“

Die DS-GVO enthält keine Definition von „Behörden oder öffentliche Stellen“. Die WP29 ist der Ansicht, dass dieser Begriff nach Maßgabe des einzelstaatlichen Rechts zu bestimmen ist. Der Begriff „Behörden und öffentliche Stellen“ schließt landesweite, regionale und lokale Behörden ein, beinhaltet jedoch nach geltendem einzelstaatlichem Recht außerdem üblicherweise noch eine Reihe weiterer dem öffentlichen Recht unterliegender Stellen.¹² In solchen Fällen ist die Benennung eines DSB obligatorisch.

Eine öffentliche Aufgabe und öffentliche Gewalt kann nicht nur von öffentlichen Einrichtungen und Stellen wahrgenommen bzw. ausgeübt werden¹³, sondern auch von jeglicher natürlichen oder juristischen Person, die – je nach den einzelstaatlichen Bestimmungen des betreffenden Mitgliedstaates – in Bereichen wie etwa dem öffentlichem Transportwesen, der Wasser- und

¹⁰ Vgl. Artikel 24 Absatz 1.

¹¹ Dies betrifft auch leitende Datenschutzbeauftragte (engl. Chief Privacy Officers, CPO) und sonstige in bestimmten Firmen im Datenschutzbereich tätige Personen, die möglicherweise nicht immer die Kriterien der DS-GVO (beispielsweise in Bezug auf die verfügbaren Ressourcen oder ihre garantierte Unabhängigkeit) erfüllen und in einem solchen Fall nicht als DSB betrachtet oder bezeichnet werden dürfen.

Energieversorgung, der Verkehrsinfrastruktur, dem öffentlich-rechtlichen Rundfunk, dem sozialen Wohnungsbau oder den Disziplinarcommissionen für reglementierte Berufe öffentlichem oder privatem Recht unterliegt.

In diesen Fällen können sich Betroffene in einer sehr ähnlichen Situation befinden, wie wenn ihre Daten von einer Behörde oder öffentlichen Stelle verarbeitet würden. Insbesondere können Daten zu ähnlichen Zwecken verarbeitet werden, wobei natürliche Personen oftmals nur wenig bis gar keine Einflussmöglichkeit darauf haben, wie ihre Daten verarbeitet werden, und von daher möglicherweise jenes zusätzlichen Schutzes bedürfen, den die Benennung eines DSB ermöglichen kann.

Wenn auch in solchen Fällen keine Verpflichtung besteht, empfiehlt die WP29 gleichwohl als bewährtes Verfahren, dass private Einrichtungen, die öffentliche Aufgaben wahrnehmen oder Staatsgewalt ausüben, einen DSB benennen. Die Tätigkeit eines solchen DSB erfasst zugleich sämtliche durchgeführten Datenverarbeitungsvorgänge, einschließlich solcher, die nicht mit der Wahrnehmung einer öffentlichen Aufgabe oder Ausübung einer öffentlichen Pflicht im Zusammenhang stehen (z. B. das Führen einer Personaldatenbank).

¹² Vgl. hierzu z. B. die Definition von „*öffentliche Stelle*“ und „*Einrichtung des öffentlichen Rechts*“ in Artikel 2 Absatz 1 und Absatz 2 der Richtlinie 2003/98/EG des Europäischen Parlaments und des Rates vom 17. November 2003 über die Weiterverwendung von Informationen des öffentlichen Sektors (ABl. L 345 vom 31.12.2003, S. 90).

¹³ Artikel 6 Absatz 1 Buchstabe e.

2.1.2 „KERNTÄTIGKEIT“

Artikel 37 Absatz 1 Buchstabe b und Buchstabe c der DS-GVO bezieht sich auf die „*Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters*“. In Erwägungsgrund 97 ist dargelegt, dass sich die Kerntätigkeit eines Verantwortlichen auf „*seine Haupttätigkeiten und nicht auf die Verarbeitung personenbezogener Daten als Nebentätigkeit*“ bezieht. Als „Kerntätigkeit“ lassen sich die wichtigsten Arbeitsabläufe betrachten, die zur Erreichung der Ziele des Verantwortlichen oder des Auftragsverarbeiters erforderlich sind.

Gleichwohl sollte der Begriff „Kerntätigkeit“ nicht dahingehend interpretiert werden, dass sich dieser nicht auch auf Tätigkeiten erstreckte, bei denen die Verarbeitung von Daten einen untrennbaren Bestandteil der Tätigkeit des Verantwortlichen oder Auftragsverarbeiters darstellt. So besteht beispielsweise die Kerntätigkeit eines Krankenhauses darin, medizinische Versorgung zu leisten. Ohne dabei gesundheitsbezogenen Daten wie etwa Krankenakten von Patienten zu verarbeiten, wäre ein Krankenhaus nicht in der Lage, dies in sicherer und wirksamer Form zu tun. Daher ist die Verarbeitung solcher Daten als Kerntätigkeit eines jeden Krankenhauses anzusehen, weshalb selbige zur Benennung eines DSB verpflichtet sind.

Als weiteres Beispiel sei ein privates Sicherheitsunternehmen angeführt, das private Einkaufszentren und öffentliche Plätze überwacht. Überwachung stellt die Kerntätigkeit des Unternehmens dar, die wiederum untrennbar mit der Verarbeitung personenbezogener Daten einhergeht. Daher ist auch ein solches Unternehmen verpflichtet, einen DSB zu benennen.

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

2.1.3 „UMFANGREICHE VERARBEITUNG“

Artikel 37 Absatz 1 Buchstabe b und Buchstabe c sieht vor, dass das Erfordernis der Benennung eines DSB nur dann besteht, wenn eine umfangreiche Verarbeitung personenbezogener Daten erfolgt. In der DS-GVO ist nicht näher quantifiziert, was unter „umfangreich“ zu verstehen ist. Gleichwohl liefert Erwägungsgrund 91 diesbezüglich einen gewissen Anhaltspunkt.¹⁴

Es ist nicht möglich, eine genaue, auf jeden Einzelfall anwendbare Zahlenangabe bezüglich der Menge an verarbeiteten Daten oder der Zahl an betroffenen natürlichen Personen zu machen. Dies schließt indes nicht aus, dass sich im Laufe der Zeit eine Standard-Praxis dafür entwickeln wird, wie sich der Begriff „umfangreiche Verarbeitung“ in Bezug auf bestimmte Formen gängiger Datenverarbeitungsvorgänge spezifischer und quantitativer definieren lässt. Die WP29 plant, durch Weitergabe und Veröffentlichung von Beispielen für maßgebliche Schwellenwerte für die Bestimmung eines DSB zu dieser Entwicklung beizutragen.

Auf alle Fälle empfiehlt die WP29, bei der Klärung der Frage, ob sich von einer umfangreichen Verarbeitung sprechen lässt, die folgenden Faktoren zu berücksichtigen:

- die Zahl der betroffenen Personen – entweder als bestimmte Zahl oder als Anteil an der maßgeblichen Bevölkerung
- das Datenvolumen und/oder das Spektrum an in Bearbeitung befindlichen Daten
- 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 Dienstleistungen 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

¹⁴ Diesem Erwägungsgrund zufolge bezieht sich dieser Begriff besonders auf „umfangreiche Verarbeitungsvorgänge [...], die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene zu verarbeiten, eine große Zahl von Personen betreffen könnten und - beispielsweise aufgrund ihrer Sensibilität - wahrscheinlich ein hohes Risiko mit sich bringen“. Andererseits ist im Erwägungsgrund ausdrücklich vorgesehen: „Die Verarbeitung personenbezogener Daten sollte nicht als umfangreich gelten, wenn die Verarbeitung personenbezogener Daten von Patienten oder von Mandanten betrifft und durch einen einzelnen Arzt, sonstigen Angehörigen eines Gesundheitsberufes oder Rechtsanwalt erfolgt.“ In diesem Zusammenhang gilt es zu berücksichtigen, dass in diesem Erwägungsgrund Extrembeispiele (die Verarbeitung durch einen einzelnen Arzt gegenüber der Verarbeitung von landes- oder gar europaweiten Daten) angeführt werden und zwischen diesen Extremen eine große Grauzone besteht. Auch ist zu beachten, dass sich dieser Erwägungsgrund auf Datenschutz-Folgeabschätzungen bezieht. Dies bringt es mit sich, dass manche dieser Elemente möglicherweise kontextspezifisch sind und nicht unbedingt in der genau gleichen Weise für die Bestimmung eines DSB gelten.

- 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

2.1.4 „REGELMÄßIGE UND SYSTEMATISCHE ÜBERWACHUNG“

Der Begriff der regelmäßigen und systematischen Überwachung ist in der DS-GVO zwar nicht definiert, doch das Konzept einer „*Beobachtung des Verhaltens von betroffenen Personen*“ wird in Erwägungsgrund 24¹⁵ erwähnt und erstreckt sich demnach eindeutig auf jede Form der Verfolgung und Profilerstellung im Internet, darunter auch zu Zwecken der verhaltensbasierten Werbung.

Gleichwohl beschränkt sich der Begriff der Überwachung nicht auf die Online-Umgebung, weshalb die Online-Verfolgung nur als ein Beispiel für die Überwachung des Verhaltens von betroffenen Personen angesehen werden sollte.¹⁶

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

Folgende Tätigkeiten können eine regelmäßige und systematische Überwachung von betroffenen Personen darstellen: Betrieb eines Telekommunikationsnetzes, Anbieten von Telekommunikationsdienstleistungen, verfolgende E-Mail-Werbung, datengesteuerte Marketingaktivitäten, Typisierung und Scoring zu Zwecken der Risikobewertung (zum Beispiel zu

¹⁵ □□ „Ob eine Verarbeitungstätigkeit der Beobachtung des Verhaltens von betroffenen Personen gilt, sollte daran festgemacht werden, ob ihre Internetaktivitäten nachvollzogen werden, einschließlich der möglichen nachfolgenden Verwendung von Techniken zur Verarbeitung personenbezogener Daten, durch die von einer natürlichen Person ein Profil erstellt wird, das insbesondere die Grundlage für sie betreffende Entscheidungen bildet oder anhand dessen ihre persönlichen Vorlieben, Verhaltensweisen oder Gepflogenheiten analysiert oder vorausgesagt werden sollen.“

¹⁶ Zu beachten ist, dass Erwägungsgrund 24 sich auf die extraterritoriale Anwendung der DS-GVO konzentriert. Überdies besteht ein Unterschied zwischen den Formulierungen „das Verhalten betroffener Personen zu beobachten“ (Artikel 3 Absatz 2 Buchstabe b) und „regelmäßige und systematische Überwachung von betroffenen Personen“ (Artikel 37 Absatz 1 Buchstabe b), so dass diese als unterschiedliche Begrifflichkeiten interpretiert werden können.

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.)

2.1.5 BESONDERE KATEGORIEN VON DATEN UND DATEN ÜBER STRAFRECHTLICHE VERURTEILUNGEN UND STRAFTATEN

Artikel 37 Absatz 1 Buchstabe c behandelt die Verarbeitung besonderer Kategorien von Daten nach Artikel 9 sowie personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten nach Artikel 10. Wenn auch in der Bestimmung das Wort „und“ verwendet wird, besteht kein politischer Grund dafür, dass die beiden Kriterien gleichzeitig angewandt werden müssten. Der Wortlaut sollte daher im Sinne eines „oder“ verstanden werden.

2.2. DSB des Auftragsverarbeiters

Artikel 37 gilt im Hinblick auf die Benennung eines DSB gleichermaßen für Verantwortliche¹⁷ und Auftragsverarbeiter¹⁸. Je nachdem, wer die Kriterien für eine zwingend vorgeschriebene Benennung erfüllt, sind in manchen Fällen lediglich der Verantwortliche oder der Auftragsverarbeiter, in anderen wiederum beide zur Benennung eines DSB verpflichtet (und sollten in solchen Fällen zusammenarbeiten).

Dabei gilt es hervorzuheben, dass selbst dann, wenn der Verantwortliche die Kriterien für eine obligatorische Benennung eines DSB erfüllt, dies nicht zwangsläufig auch für dessen Auftragsverarbeiter gilt. Dies kann indes ein bewährtes Verfahren darstellen.

Beispiele:

- Ein im Vertrieb von Haushaltswaren in einer einzelnen Stadt tätiges kleines Familienunternehmen nimmt die Dienste eines Auftragsverarbeiters in Anspruch, dessen Kerntätigkeit in der Bereitstellung von Website-Analysediensten und der Unterstützung bei zielgruppenorientierten Werbe- und Marketingmaßnahmen besteht. Bei den Tätigkeiten des Familienunternehmens und seiner Kunden fällt in Anbetracht der geringen Kundenzahl und der vergleichsweise beschränkten Tätigkeiten keine „umfangreiche Verarbeitung“ von Daten an. Die Tätigkeiten des Auftragsverarbeiters hingegen, der über eine große Zahl an Kunden wie diesem Kleinunternehmen verfügt, ergeben zusammen eine durchaus als umfangreich einzustufende Verarbeitung. Der Auftragsverarbeiter ist daher zur Benennung eines DSB nach Artikel 37 Absatz 1 Buchstabe b verpflichtet. Für das Familienunternehmen hingegen besteht eine solche Pflicht nicht.

¹⁷ Der Verantwortliche ist nach Artikel 4 Absatz 7 als natürliche oder juristische Person definiert, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet.

¹⁸ Der Auftragsverarbeiter ist nach Artikel 4 Absatz 8 als natürliche oder juristische Person definiert, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- Ein mittelgroßer Fliesenhersteller beauftragt einen externen Auftragsverarbeiter, der über eine Vielzahl ähnlicher Kunden verfügt, mit der Erbringung seiner arbeitsmedizinischen Dienste. Sofern dabei eine Verarbeitung von Daten in großem Umfang erfolgt, ist der Auftragsverarbeiter nach Artikel 37 Absatz 1 Buchstabe c zur Benennung eines DSB verpflichtet. Gleiches gilt nicht zwangsläufig auch für den Fliesenhersteller.

Der von einem Auftragsverarbeiter benannte DSB beaufsichtigt auch die von der Einrichtung des Auftragsverarbeiters durchgeführten Tätigkeiten, wenn diese als für die Verarbeitung eigenständiger Verantwortlicher auftritt (z. B. Personal-, IT- oder Logistikabteilungen).

2.3. Benennung eines gemeinsamen DSB für mehrere Organisationen

Artikel 37 Absatz 2 gestattet einer Unternehmensgruppe die Benennung eines gemeinsamen DSB, sofern dieser „von jeder Niederlassung aus [...] leicht erreicht werden kann“. Der Begriff der Erreichbarkeit bezieht sich auf die Aufgaben des DSB als Ansprechpartner für Betroffene¹⁹ und für die Aufsichtsbehörde²⁰, gilt jedoch auch für dessen Aufgaben als einrichtungsinterner Ansprechpartner, denn eine der Aufgaben des DSB ist ja die „*Unterrichtung und Beratung des Verantwortlichen oder des Auftragsverarbeiters und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach dieser Verordnung*“.²¹

Um die Erreichbarkeit des DSB sowohl intern als auch extern zu gewährleisten, ist dafür Sorge zu tragen, dass die Kontaktdaten im Einklang mit den Vorgaben der DS-GVO zur Verfügung stehen²².

Der DSB muss – gegebenenfalls mithilfe eines Teams – in der Lage sein, mit Betroffenen wirksam zu kommunizieren²³ und mit den zuständigen Aufsichtsbehörden effektiv zusammenzuarbeiten²⁴. 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.

Nach Artikel 37 Absatz 3 kann von mehreren öffentlichen Einrichtungen und Stellen in Anbetracht ihrer Organisationsstruktur und Größe ein gemeinsamer DSB benannt werden. Gleiches gilt für die erforderlichen Ressourcen und die Kommunikation: Da der DSB eine Vielzahl von Aufgaben

¹⁹ Artikel 38 Absatz 4: „*Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäß dieser Verordnung im Zusammenhang stehenden Fragen zu Rate ziehen.*“

²⁰ Artikel 39 Absatz 1 Buchstabe e: „*Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen.*“

²¹ Artikel 39 Absatz 1 Buchstabe a.

²² Vgl. auch Abschnitt 2.6.

²³ Artikel 12 Absatz 1 besagt diesbezüglich: „*Der Verantwortliche trifft geeignete Maßnahmen, um der betroffenen Person alle Informationen gemäß den Artikeln 13 und 14 und alle Mitteilungen gemäß den Artikeln 15 bis 22 und Artikel 34, die sich auf die Verarbeitung beziehen, in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu übermitteln; dies gilt insbesondere für Informationen, die sich speziell an Kinder richten.*“

²⁴ Artikel 39 Absatz 1 Buchstabe d sieht eine „*Zusammenarbeit mit der Aufsichtsbehörde*“ vor.

wahrzunehmen hat, ist es Sache des Verantwortlichen oder des Auftragsverarbeiters, dafür Sorge zu tragen, dass einzelne DSB trotz der Zuständigkeit für mehrere öffentliche Einrichtungen und Stellen in der Lage sind, diesen – gegebenenfalls mithilfe eines Teams – wirksam nachzugehen.

2.4. Erreichbarkeit und Standort des DSB

Nach Abschnitt 4 der DS-GVO bedarf es der effektiven Erreichbarkeit des DSB.

Die WP29 empfiehlt, die effektive Erreichbarkeit des DSB durch die Ernennung eines DSB mit Sitz in der Europäischen Union zu gewährleisten, unabhängig davon, ob der Verantwortliche oder der Auftragsverarbeiter in der Union niedergelassen ist.

Jedoch ist nicht ausgeschlossen, dass in Situationen, in denen der Verantwortliche oder der Auftragsverarbeiter nicht in der Europäischen Union niedergelassen ist²⁵, ein außerhalb der EU niedergelassener DSB seine Aufgaben effektiver ausüben kann.

2.5. Fähigkeiten und Fachkenntnisse des DSB

Nach Artikel 37 Absatz 5 wird der Datenschutzbeauftragte *„auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens benannt, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage seiner Fähigkeit zur Erfüllung der in Artikel 39 genannten Aufgaben“*. Nach Erwägungsgrund 97 sollte sich das erforderliche Niveau des Fachwissens nach den durchgeführten Datenverarbeitungsvorgängen und dem erforderlichen Schutz der vom Verantwortlichen oder vom Auftragsverarbeiter verarbeiteten personenbezogenen Daten richten.

- **Fachwissen**

Das verlangte Fachwissen ist nicht genau umrissen, muss jedoch mit der Sensibilität, der Komplexität und der Menge der Daten, die eine Einrichtung verarbeitet, im Einklang stehen. 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. Ebenso macht es einen Unterschied aus, ob die Einrichtung personenbezogene Daten systematisch an Orte außerhalb der Europäischen Union übermittelt oder dies nur gelegentlich geschieht. Die Wahl des DSB sollte daher mit Bedacht erfolgen; sich innerhalb der Einrichtung stellenden Datenschutzfragen ist dabei in angemessener Weise Rechnung zu tragen.

- **Berufliche Qualifikation**

Auch wenn Artikel 37 Absatz 5 keine Angaben bezüglich der beruflichen Qualifikation enthält, die es bei der Bestimmung eines DSB zu berücksichtigen gilt, gilt diesbezüglich die maßgebliche Überlegung, dass ein DSB über Erfahrung sowohl im einzelstaatlichen als auch im europäischen Datenschutzrecht und in der diesbezüglichen Praxis sowie über ein umfassendes Verständnis der DS-

²⁵ Siehe Artikel 3 DS-GVO zum räumlichen Anwendungsbereich.

GVO verfügen muss. Von Vorteil ist es auch, wenn die Aufsichtsbehörden angemessene und regelmäßige Schulungen für DSB fördern.

Branchenkenntnis und Vertrautheit mit der Organisationsstruktur des Auftragsverarbeiters sind von ebenfalls Nutzen. Auch sollte der DSB über ein gutes Verständnis der durchgeführten Datenverarbeitungsvorgänge, der betreffenden Informationssysteme sowie der Datensicherheits- und Datenschutzerfordernisse des Auftragsverarbeiters verfügen.

Im Fall von Behörden oder öffentlichen Stellen sollte der DSB zudem über fundierte Kenntnis ihrer Verwaltungsvorschriften und -verfahren verfügen.

- **Fähigkeit zur Erfüllung seiner Aufgaben**

Der Begriff der Fähigkeit zur Erfüllung der dem DSB obliegenden Aufgaben ist im Sinne sowohl seiner persönlichen Eigenschaften und Kenntnisse als auch seiner Position innerhalb der Einrichtung zu verstehen. Zu den persönlichen Eigenschaften sollten beispielsweise Integrität und ein ausgeprägtes Berufsethos zählen; vorrangiges Anliegen des DSB sollte die Schaffung der Voraussetzungen für die Einhaltung der Vorgaben der DS-GVO sein. Dem DSB kommt eine zentrale Rolle dabei zu, die Verbreitung einer Datenschutzkultur innerhalb der Einrichtung zu fördern und zur Umsetzung wesentlicher Bestandteile der DS-GVO beizutragen, darunter die Grundsätze der Datenverarbeitung²⁶, die Rechte der betroffenen Personen²⁷, Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen²⁸, die Aufzeichnung von Verarbeitungstätigkeiten²⁹, die Sicherheit der Verarbeitung³⁰ sowie die Meldung und Mitteilung von Verstößen gegen den Schutz personenbezogener Daten³¹.

- **Im Rahmen eines Dienstleistungsvertrags beschäftigte DSB**

Die Funktion eines DSB kann auch auf Grundlage eines Dienstleistungsvertrags ausgeübt werden, der mit einer natürlichen oder juristischen Person geschlossen wird, die nicht der Einrichtung des Verantwortlichen oder Auftragsverarbeiters angehört. In letzterem Falle ist es unverzichtbar, dass jedes Mitglied der Einrichtung, das die Funktionen eines DSB wahrnimmt, sämtliche in Abschnitt 4 der DS-GVO genannten Anforderungen erfüllt (sodass Interessenkonflikte ausgeschlossen werden können). Ebenso wichtig ist es, dass jedes Mitglied durch die Bestimmungen der DS-GVO geschützt ist (keine ungerechtfertigte Kündigung von Dienstleistungsverträgen in Bezug auf Tätigkeiten als DSB und keine ungerechtfertigte Entlassung einer der Einrichtung angehörigen natürlichen Person, welche die Aufgaben eines DSB wahrnimmt). Zugleich lassen sich individuelle Qualifikationen und Stärken so miteinander kombinieren, dass Einzelpersonen durch die Zusammenarbeit im Team ihren Mandanten noch wirksamere Dienste leisten können.

Im Interesse der Rechtssicherheit und einer ordnungsgemäßen Organisation, aber auch, um Interessenkonflikte der Teammitglieder zu vermeiden, wird empfohlen, eine klare Aufgabenverteilung innerhalb des DSB-Teams vorzusehen und eine einzelne Person als primären Ansprechpartner

²⁶ Kapitel II.

²⁷ Kapitel III.

²⁸ Artikel 25.

²⁹ Artikel 30.

³⁰ Artikel 32.

³¹ Artikel 33 und 34.

festzulegen, der zugleich für den jeweiligen Kunden „zuständig“ ist. Es ist generell von Nutzen, diese Punkte im Dienstleistungsvertrag festzuhalten.

2.6. Veröffentlichung und Mitteilung der Kontaktdaten des DSB

Artikel 37 Absatz 7 der DS-GVO sieht vor, dass der Verantwortliche bzw. Auftragsverarbeiter

- die Kontaktdaten des DSB veröffentlicht und
- diese Daten den zuständigen Aufsichtsbehörden mitteilt.

Durch diese Anforderung soll sichergestellt werden, dass sich Betroffene (sowohl innerhalb als auch außerhalb der Einrichtung) und die Aufsichtsbehörden ohne Weiteres auf direktem Wege an den DSB wenden können, ohne mit einem anderen Teil der Einrichtung in Kontakt treten zu müssen. Ein weiterer wichtiger Gesichtspunkt ist Vertraulichkeit: So könnten z. B. Arbeitnehmer zögern, eine Beschwerde an den DSB zu richten, wenn die Vertraulichkeit ihrer Kommunikation nicht gewährleistet ist.

Der DSB ist nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden (Artikel 38 Absatz 5).

Die Kontaktdaten des DSB sollten Angaben enthalten, die Betroffene ebenso wie die Aufsichtsbehörde in die Lage versetzen, den DSB auf einfachem Wege (postalisch, über eine persönliche Telefonnummer und/oder über eine persönliche E-Mail-Adresse) zu erreichen. Wo dies angezeigt ist, können zum Zwecke der Kommunikation mit der Öffentlichkeit weitere Kommunikationsmöglichkeiten (z.B. eine persönliche Hotline oder ein an den DSB persönlich adressiertes Kontaktformular auf der Website der Einrichtung) angeboten werden.

Artikel 37 Absatz 1 schreibt nicht vor, dass in den veröffentlichten Kontaktdaten auch der Name des DSB aufzuführen ist. Auch wenn es sich hierbei um ein bewährtes Verfahren handeln mag, liegt die Entscheidung, ob dies unter den gegebenen Umständen erforderlich oder hilfreich ist, im Ermessen des Verantwortlichen oder Auftragsverarbeiters und des DSB³².

Die Mitteilung des Namens des DSB an die Aufsichtsbehörde ist jedenfalls erforderlich angesichts der Tätigkeit des DSB als Anlaufstelle der Einrichtung für die Aufsichtsbehörde (Artikel 39 Absatz 1 Buchstabe e).

Darüber hinaus empfiehlt die WP29 als bewährtes Verfahren, dass jede Einrichtung ihren Mitarbeitern den Namen und die Kontaktdaten des DSB zur Kenntnis bringen sollte. Beispielsweise könnten der Name und die Kontaktdaten des DSB im Intranet der betreffenden Einrichtung sowie in ihrem internen Telefonverzeichnis und in ihren Organigrammen veröffentlicht werden.

³² Artikel 33 Absatz 3 Buchstabe b, in dem die Angaben aufgeführt sind, die der Aufsichtsbehörde und den Betroffenen im Falle einer Verletzung datenschutzrechtlicher Bestimmungen übermittelt werden müssen, sieht im Unterschied zu Artikel 37 Absatz 7 ausdrücklich vor, dass auch der Name (und nicht nur die Kontaktdaten) des DSB mitzuteilen sind.

3 Stellung des DSB

3.1. Einbindung des DSB in alle mit dem Schutz personenbezogener Daten in Zusammenhang stehende Angelegenheiten

Nach Artikel 38 der DS-GVO haben der Verantwortliche und der Auftragsverarbeiter dafür Sorge zu tragen, dass der Datenschutzbeauftragte *„ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden“* wird.

Es ist von größter Bedeutung, dass der DSB oder sein Team vom frühestmöglichen Zeitpunkt an in alle im Zusammenhang mit dem Datenschutz stehenden Angelegenheiten eingebunden wird. In Bezug auf Datenschutz-Folgenabschätzungen sieht die DS-GVO ausdrücklich die frühzeitige Einbindung des DSB vor und besagt, dass der Verantwortliche bei der Durchführung solcher Folgenabschätzungen den DSB zu Rate zu ziehen hat.³³ Die systematische Unterrichtung und Konsultation des DSB von Anfang an vereinfacht die Einhaltung der DS-GVO und dient der Praxis eines „eingebauten Datenschutzes“ und sollte daher ein Standardverfahren der Führung von Einrichtungen darstellen. Überdies ist wichtig, dass der DSB innerhalb der Einrichtung als Gesprächspartner angesehen wird und dass er den maßgeblichen Arbeitsgruppen angehört, die mit Datenverarbeitungstätigkeiten innerhalb der Einrichtung befasst sind.

Dementsprechend sollte die Einrichtung beispielsweise dafür Sorge tragen, dass

- der DSB zur regelmäßigen Teilnahme an Treffen des leitenden und des mittleren Managements eingeladen wird.
- Seine Anwesenheit empfiehlt sich bei der Fällung von Entscheidungen, welche Fragen des Datenschutzes tangieren. Jegliche maßgeblichen Informationen sind dem DSB zeitnah zu übermitteln, damit dieser in adäquater Weise als Ratgeber fungieren kann.
- Der Meinung des DSB ist stets die gebührende Beachtung zu schenken. Im Falle einer abweichenden Meinung empfiehlt die WP29 als bewährtes Verfahren, die Gründe, aus denen dem Rat des DSB nicht gefolgt wird, zu dokumentieren.
- Bei einer Verletzung datenschutzrechtlicher Bestimmungen oder einem sonstigen Vorfall ist der DSB unverzüglich hinzuzuziehen.

Gegebenenfalls sollte der Verantwortliche oder der Auftragsverarbeiter Datenschutzrichtlinien oder -programme ausarbeiten, in denen festgelegt ist, wann der DSB zu Rate zu ziehen ist.

3.2. Erforderliche Ressourcen

Artikel 38 Absatz 2 der DS-GVO sieht vor, dass alle 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“*. Dies beinhaltet insbesondere

- eine aktive Unterstützung der Funktion des DSB durch das leitende Management (beispielsweise auf Vorstandsebene)

³³ Artikel 35 Absatz 2.

- die Gewährung von genügend Zeit für die Erfüllung seiner Pflichten. Besonders wichtig ist dies in Fällen, in denen ein interner DSB seiner Arbeit in Teilzeit nachgeht oder ein externer DSB seine Datenschutzstätigkeit neben anderen Pflichten wahrnimmt. Andernfalls besteht die Gefahr einer Vernachlässigung der DSB-eigenen Pflichten infolge einander zuwiderlaufender Prioritäten. Über genügend Zeit für die Erledigung der dem DSB obliegenden Aufgaben zu verfügen, ist von größter Wichtigkeit. In Fällen, in denen die DSB-Funktion nicht in Vollzeit geleistet wird, empfiehlt es sich, hierfür einen festen Prozentsatz der Arbeitszeit vorzusehen. Ebenso empfiehlt es sich, die zur Wahrnehmung der Funktion benötigte Zeit sowie die Priorität, die DSB-eigenen Pflichten beizumessen ist, zu ermitteln und von Seiten des DSB (oder der Einrichtung) ein Arbeitsprogramm zu erstellen;
- angemessene Unterstützung durch Finanzmittel, Infrastrukturen (Räumlichkeiten, Einrichtungen, Ausrüstung) sowie gegebenenfalls Personal;
- die offizielle Unterrichtung aller Beschäftigten über die Benennung eines DSB, damit dessen Existenz und Funktion einrichtungsweit bekannt sind;
- den nötigen Zugang zu anderen Dienststellen wie Personal-, Rechts-, IT-, Sicherheitsabteilung usw., damit DSB unverzichtbare Unterstützung, Anregungen und Informationen von diesen erhalten können;
- kontinuierliche Fortbildung: Dem DSB sollte Gelegenheit gegeben werden, sich in Bezug auf Entwicklungen im Bereich des Datenschutzes auf dem aktuellen Stand zu halten. Ziel sollte dabei sein, die Fachkompetenz der DSB kontinuierlich zu erhöhen, und DSB sollten ermuntert werden, an Fortbildungsveranstaltungen über Datenschutz und an sonstigen Formen der beruflichen Weiterbildung (Datenschutzforen, Workshops usw.) teilzunehmen;
- Je nach Größe und Aufbau der Einrichtung kann es erforderlich sein, ein DSB-Team (bestehend aus einem DSB und dessen Mitarbeitern) einzurichten. In solchen Fällen sollten die Zusammensetzung des Teams sowie die Aufteilung der Aufgaben und Zuständigkeiten unter den Mitgliedern klar festgelegt werden. Falls die Funktion des DSB von einem externen Dienstleister wahrgenommen wird, kann ein Team aus für diese Stelle tätigen Personen die Aufgaben eines DSB unter der Verantwortung eines ernannten primären Ansprechpartners für den Kunden in effizienter und entsprechender Weise ausführen. Allgemein gilt:

Je komplexer und/oder sensibler die Datenverarbeitungsvorgänge sind, desto mehr Ressourcen müssen dem DSB zur Verfügung gestellt werden. Der Unternehmensbereich Datenschutz muss effektiv arbeiten können und über eine ausreichende Mittelausstattung für die durchgeführte Datenverarbeitung verfügen.

3.3. Anweisungen und „Ausübung der Pflichten und Aufgaben in vollständiger Unabhängigkeit“

In Artikel 38 Absatz 3 sind grundlegende Garantien festgelegt, die dazu beitragen sollen, dass DSB ihren Aufgaben mit hinreichender Eigenständigkeit innerhalb ihrer Einrichtung nachgehen können. Insbesondere sind Verantwortliche/Auftragsverarbeiter verpflichtet, dafür Sorge zu tragen, dass der DSB *„keine Anweisungen bezüglich der Ausübung [seiner] Aufgaben erhält“*. Erwägungsgrund 97 fügt hinzu: *„Derartige Datenschutzbeauftragte sollten unabhängig davon, ob es sich bei ihnen um Beschäftigte des Verantwortlichen handelt oder nicht, ihre Pflichten und Aufgaben in vollständiger Unabhängigkeit ausüben können.“*

Dies bedeutet, dass DSB bei der Erfüllung ihrer Aufgaben nach Artikel 39 keine Anweisungen erteilt werden dürfen, wie sie bei einem gegebenen Sachverhalt zu verfahren haben, also beispielsweise,

welches Ergebnis erzielt werden soll, wie einer Beschwerde nachzugehen ist oder ob die Aufsichtsbehörde zurate gezogen werden soll oder nicht. Des Weiteren dürfen sie nicht angewiesen werden, in einer datenschutzrechtlichen Frage einen bestimmten Standpunkt (beispielsweise in Bezug auf die Auslegung eines Gesetzes) zu vertreten.

Die Eigenständigkeit der DSB schließt jedoch keine über ihr Aufgabenfeld nach Artikel 39 hinausgehende Entscheidungsbefugnis ein.

Der Verantwortliche bzw. der Auftragsverarbeiter trägt stets die Verantwortung für die Einhaltung der datenschutzrechtlichen Bestimmungen und muss diese Einhaltung nachweisen können.³⁴ Trifft der Verantwortliche bzw. der Auftragsverarbeiter Entscheidungen, die der DS-GVO und den Empfehlungen des DSB zuwiderlaufen, sollte der DSB die Möglichkeit haben, seine abweichende Meinung der höchsten Managementebene und den Entscheidungsträgern deutlich zur Kenntnis zu bringen. Nach Artikel 38 Absatz 3 berichtet der DSB „*unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters*“. Dadurch soll sichergestellt werden, dass das leitende Management (beispielsweise auf Vorstandsebene) von den Anregungen und Empfehlungen des DSB im Rahmen seiner Aufgabe, den Verantwortlichen oder den Auftragsverarbeiter zu unterrichten und zu beraten, Kenntnis erlangt. Ein weiteres Beispiel für unmittelbare Berichterstattung ist die Erstellung eines Jahresberichts über die Tätigkeit des DSB, der der höchsten Managementebene vorgelegt wird.

3.4. Abberufung oder Benachteiligung des DSB wegen der Erfüllung seiner Aufgaben

Gemäß Artikel 38 Absatz 3 dürfen DSB „*von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden*“.

Diese Anforderung stärkt die Eigenständigkeit der DSB und trägt dazu bei, dass diese unabhängig agieren können und bei der Ausführung ihrer datenschutzbezogenen Aufgaben hinreichenden Schutz genießen.

Strafen sind nach der DS-GVO nur dann unzulässig, wenn sie gegen den DSB allein deshalb verhängt werden, weil dieser seinen Pflichten als DSB nachgekommen ist. Beispielsweise kann es vorkommen, dass ein DSB zu der Einschätzung gelangt, dass eine bestimmte Form der Datenverarbeitung ein hohes Risiko in sich birgt, und er dem Verantwortlichen bzw. dem Auftragsverarbeiter eine Datenschutz-Folgenabschätzung empfiehlt, der Verantwortliche bzw. der Auftragsverarbeiter diese Einschätzung des DSB jedoch nicht teilt. In einem solchen Fall ist es nicht zulässig, den DSB wegen seiner diesbezüglichen Empfehlung abberufen zu lassen.

Strafen können verschiedenerlei Formen annehmen und unmittelbarer oder mittelbarer Natur sein. Denkbar sind beispielsweise eine ausbleibende oder verspätet erfolgende Beförderung, die Verwehrung einer beruflichen Fortentwicklung oder der Ausschluss von Leistungen, die anderen Beschäftigten gewährt werden. Dabei ist es nicht erforderlich, dass solche Strafen tatsächlich verhängt werden: Ihr bloße Androhung reicht aus, solange diese dazu dient, den DSB aus im Zusammenhang mit seiner Tätigkeit stehenden Gründen zu bestrafen.

³⁴ Artikel 5 Absatz 2.

Als normale Management-Regel und wie dies bei jedem anderen Beschäftigten oder Fremdmitarbeiter nach geltendem nationalem Vertrags-, Arbeits- oder Strafrecht der Fall wäre, kann ein DSB jederzeit von Rechts wegen aus Gründen abberufen werden, die nicht im Zusammenhang mit der Erfüllung seiner Pflichten als DSB stehen (beispielsweise wegen Diebstahls, physischer, psychischer oder sexueller Belästigung oder einem vergleichbarem groben Fehlverhalten).

In diesem Zusammenhang ist anzumerken, dass die DS-GVO keine Angaben dazu enthält, wie und wann ein DSB abberufen oder durch eine andere Person ersetzt werden darf. Je stabiler allerdings der Vertrag eines DSB ist und je mehr Garantien gegen eine ungerechtfertigte Abberufung bestehen, desto wahrscheinlicher ist es, dass er in unabhängiger Weise agieren kann. Daher würde es die WP29 begrüßen, wenn von Seiten der Einrichtungen hierauf zielende Anstrengungen unternommen würden.

3.5. Interessenkonflikte

Nach Artikel 38 Absatz 6 können DSB *„andere Aufgaben und Pflichten wahrnehmen“*. Die betreffende Einrichtung hat allerdings dafür Sorge zu tragen, dass *„derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen“*.

Die Abwesenheit eines Interessenkonflikts ist eng mit dem Erfordernis einer unabhängigen Tätigkeit verknüpft. DSB dürfen zwar auch andere Funktionen wahrnehmen, aber nur mit Aufgaben und Pflichten betraut werden, die zu keinen Interessenkonflikten mit ihrer Tätigkeit als DSB führen. Diese Vorgabe bringt insbesondere mit sich, dass der DSB innerhalb einer Einrichtung keine Position innehaben kann, 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 innerhalb der Einrichtung solche des leitenden Managements zählen (wie etwa Leiter des Unternehmens, Leiter des operativen Geschäftsbereichs, Finanzvorstand, leitender medizinischer Direktor, Leiter der Marketingabteilung, Leiter der Personalabteilung oder Leiter der IT-Abteilung), jedoch auch hierarchisch nachgeordnete Positionen, wenn die betreffenden Funktionen oder Aufgabenfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen. Auch können Interessenkonflikte auftreten, wenn z. B. ein externer DSB aufgefordert wird, den Verantwortlichen oder den Auftragsverarbeiter in datenschutzrelevanten Rechtssachen vor Gericht zu vertreten.

Je nach Tätigkeiten, Größe und Struktur der Einrichtung kann es für Verantwortliche bzw. Auftragsverarbeiter ratsam sein,

- die Positionen zu benennen, die mit der Funktion eines DSB unvereinbar sind,
- zur Vermeidung von Interessenkonflikten diesbezügliche interne Richtlinien aufzustellen
- eine allgemeine Erläuterung potenzieller Interessenkonflikte vorzunehmen
- zu erklären, dass sich der DSB in Bezug auf seine Funktion in keinem Interessenkonflikt befindet und auf diese Weise das Bewusstsein für diese Anforderung zu schärfen
- in die internen Richtlinien der Einrichtung Sicherungsvorkehrungen aufzunehmen und dafür Sorge zu tragen, dass die Stellenausschreibung für die Position eines DSB bzw. der betreffende Dienstleistungsvertrag zwecks Vermeidung von Interessenkonflikten hinreichend genau und präzise formuliert wird. In diesem Zusammenhang ist zu beachten, dass

Interessenkonflikte je nachdem, ob der DSB intern oder extern rekrutiert wird, unterschiedliche Formen annehmen können.

4 Aufgaben des DSB

4.1. Überwachung der Einhaltung der DS-GVO

Artikel 39 Absatz 1 Buchstabe b überträgt dem DSB unter anderem die Pflicht zur Überwachung der Einhaltung der DS-GVO. Erwägungsgrund 97 besagt ferner, dass *„der Verantwortliche oder der Auftragsverarbeiter bei der Überwachung der internen Einhaltung der Bestimmungen dieser Verordnung von einer weiteren Person unterstützt werden“* sollte.

Im Rahmen dieser Überwachungspflicht sind DSB insbesondere befugt,

- Informationen zur Ermittlung von Datenverarbeitungstätigkeiten zu sammeln,
- die Einhaltung der Vorgaben bei Datenverarbeitungstätigkeiten zu analysieren und zu kontrollieren,
- den Verantwortlichen oder den Auftragsverarbeiter zu unterrichten und zu beraten und ihm Empfehlungen zu unterbreiten.

Überwachung der Einhaltung bedeutet nicht, dass der DSB im Fall der Nichteinhaltung persönlich zur Verantwortung gezogen werden kann. Aus der DS-GVO geht klar hervor, dass es Sache des Verantwortlichen – und nicht des DSB – ist, *„geeignete technische und organisatorische Maßnahmen [umzusetzen], um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt“* (Artikel 24 Absatz 1). Die Einhaltung der datenschutzrechtlichen Bestimmungen fällt somit in den Aufgabenbereich des Verantwortlichen und nicht in den des DSB.

4.2. Die Funktion des DSB bei einer Datenschutz-Folgenabschätzung

Gemäß Artikel 35 Absatz 1 ist es Sache des Verantwortlichen - und nicht des DSB -, erforderlichenfalls eine Datenschutz-Folgenabschätzung („DS-Folgenabschätzung“) durchzuführen. Allerdings kann der DSB eine überaus wichtige und nützliche Rolle spielen, indem er dem Verantwortlichen Hilfestellung leistet. Dem Grundsatz eines „eingebauten Datenschutzes“ folgend sieht Artikel 35 Absatz 2 ausdrücklich vor, dass der Verantwortliche bei der Durchführung einer Datenschutz-Folgenabschätzung (im Folgenden „DS-Folgenabschätzung“) den Rat des DSB einholt. Artikel 39 Absatz 1 Buchstabe c wiederum überträgt den DSB die Pflicht, *„Beratung – auf Anfrage – im Zusammenhang mit der [DS-Folgenabschätzung] und Überwachung ihrer Durchführung gemäß Artikel 35“* zu leisten.

Die WP29 empfiehlt, dass der Verantwortliche den DSB insbesondere³⁵ dann zurate zieht, wenn es um die Frage geht,

- ob eine DS-Folgenabschätzung durchgeführt werden sollte oder nicht

³⁵ In Artikel 39 Absatz 1 sind die Aufgaben der DSB aufgeführt, demnach haben sie *„zumindest“* die im Folgenden genannten Aufgaben wahrzunehmen. Daher hindert den Verantwortlichen nichts daran, dem DSB Aufgaben zu übertragen, die über die in Artikel 39 Absatz 1 ausdrücklich erwähnten Aufgaben hinausgehen, oder solche Aufgaben zu präzisieren.

- 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

Falls der Verantwortliche der Empfehlung des DSB nicht zustimmt, ist in der Dokumentation zu der DS-Folgenabschätzung ausdrücklich schriftlich zu begründen, warum der Empfehlung nicht Folge geleistet wurde³⁶.

Die WP29 empfiehlt ferner, dass der Verantwortliche – beispielsweise im Vertrag des DSB und auch in an die Beschäftigten, die Unternehmensleitung und etwaige sonstige Interessenträger gerichteten Mitteilungen – die Aufgaben, die der DSB in Bezug auf die Durchführung der DS-Folgenabschätzung zu erfüllen hat, und deren Umfang genau darlegt.

4.3. Zusammenarbeit mit der Aufsichtsbehörde und Tätigkeit als Anlaufstelle

Nach Artikel 39 Absatz 1 Buchstaben d und e obliegt dem DSB die *„Zusammenarbeit mit der Aufsichtsbehörde“* und die *„Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschließlich der vorherigen Konsultation gemäß Artikel 36, und gegebenenfalls Beratung zu allen sonstigen Fragen“*.

Diese Aufgaben zeugen von der in der Einführung zu diesen Leitlinien erwähnten Funktion des DSB als „Mittler“. Der DSB handelt als Anlaufstelle, um den Zugang der Aufsichtsbehörden zu Dokumenten und Informationen zur Erfüllung der Aufgaben nach Artikel 57 und die Ausübung ihrer Untersuchungs-, Abhilfe-, Genehmigungs- und beratenden Befugnisse nach Artikel 58 zu erleichtern. Wie bereits erwähnt, ist der DSB nach dem Recht der Union oder der Mitgliedstaaten bei der Erfüllung seiner Aufgaben an die Wahrung der Geheimhaltung oder der Vertraulichkeit gebunden (Artikel 38 Absatz 5). Allerdings verbietet die Wahrung der Geheimhaltung oder der Vertraulichkeit es dem DSB nicht, die Aufsichtsbehörden zu Rate zu ziehen. Laut Artikel 39 Absatz 1 Buchstabe e kann der DSB die Aufsichtsbehörde gegebenenfalls zu allen sonstigen Fragen konsultieren.

³⁶ Artikel 24 Absatz 1 besagt: *„Der Verantwortliche setzt unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der Risiken für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen um, um sicherzustellen **und den Nachweis dafür erbringen zu können**, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Diese Maßnahmen werden erforderlichenfalls überprüft und aktualisiert“*.

4.4. Risikobasierter Ansatz

Artikel 39 Absatz 2 sieht vor, *dass der DSB „dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung [trägt], wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt“.*

Dieser Artikel bezieht sich auf einen allgemeinen, auf dem gesunden Menschenverstand basierenden Grundsatz, der für viele Aspekte der Alltagstätigkeit eines DSB von Belang sein kann. Im Wesentlichen verpflichtet er den DSB, seine Tätigkeiten nach Priorität zu ordnen und seine Anstrengungen auf Fragen zu konzentrieren, von denen größere Bedrohungen für den Datenschutz ausgehen. Dies bedeutet keineswegs, dass er die Überwachung der Vorschrifteneinhaltung bei vergleichsweise weniger risikobehafteten Datenverarbeitungsvorgängen vernachlässigen sollte, sondern besagt, dass er sich in erster Linie auf die Bereiche konzentrieren sollte, von denen ein höheres Risiko ausgeht.

Dieser selektive, pragmatische Ansatz soll DSB dabei helfen, Verantwortliche darüber zu beraten, nach welcher Methodik bei einer DS-Folgenabschätzung vorgegangen werden sollte, welche Bereiche einer internen oder externen Datenschutzprüfung unterzogen werden sollten, welche internen Schulungsmaßnahmen für leitende oder sonstige mit Datenverarbeitungstätigkeiten befasste Mitarbeiter durchgeführt werden sollten und welchen Datenverarbeitungsvorgängen mehr Zeit und Ressourcen gewidmet werden sollten.

4.5. Die Funktion des DSB bei der Führung von Verzeichnissen

Nach Artikel 30 Absatz 1 und Absatz 2 ist es Sache der Verantwortlichen oder der Auftragsverarbeiter - und nicht der DSB -, *„ein Verzeichnis aller Verarbeitungstätigkeiten [zu führen], die ihrer Zuständigkeit unterliegen“* bzw. *„ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung [zu führen]“.*

In der Praxis erstellen DSB oftmals Inventarlisten und führen Register der Verarbeitungsvorgänge auf der Grundlage der Informationen, die ihnen von den verschiedenen für die Verarbeitung personenbezogener Daten zuständigen Bereichen ihrer Einrichtung vorgelegt werden. Dieses Vorgehen ist in zahlreichen aktuellen einzelstaatlichen Rechtsvorschriften und in den geltenden Datenschutzbestimmungen der EU-Organe und -Einrichtungen³⁷ festgeschrieben worden.

Artikel 39 Absatz 1 sieht eine Liste von Aufgaben vor, die der DSB als Mindestanforderung wahrzunehmen hat. Den Verantwortlichen bzw. den Auftragsverarbeiter hindert somit nichts daran, den DSB die Aufgabe zu übertragen, unter der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters 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.

In jedem Falle sollte das nach Artikel 30 zu führende Verzeichnis auch als ein Instrument angesehen werden, das den Verantwortlichen und die Aufsichtsbehörde in die Lage versetzt, sich bei Bedarf einen Überblick über sämtliche in einer Einrichtung erfolgenden Tätigkeiten der Verarbeitung

³⁷ Artikel 24 Absatz 1 Buchstabe d der Verordnung (EG) 45/2001.

personenbezogener Daten zu verschaffen. Es stellt von daher eine unverzichtbare Voraussetzung für die Vorschrifteneinhaltung und somit eine wirksame Maßnahme zur Rechenschaftslegung dar.

5 ANHANG ZU DEN DSB-LEITLINIEN: WAS SIE WISSEN MÜSSEN

Ziel dieses Anhangs ist es, in vereinfachter und leicht verständlicher Form Antworten auf die wichtigsten Fragen zu geben, die sich bei einer Einrichtung in Bezug auf die neuen Anforderungen der Datenschutz-Grundverordnung (DS-GVO) für die Benennung eines DSB stellen können.

Benennung des DSB

1 Welche Einrichtungen sind zur Benennung eines DSB verpflichtet?

Die Benennung eines DSB ist obligatorisch, wenn

- die Datenverarbeitung von einer Behörde oder öffentlichen Stelle durchgeführt wird (unabhängig von der Art der verarbeiteten Daten),
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in Datenverarbeitungsvorgängen besteht, die eine regelmäßige und systematische Überwachung von betroffenen Personen in großem Umfang erfordern,
- 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 zwingend erforderlich machen können. Schließlich kann es auch in Fällen, in denen die Benennung eines DSB nicht obligatorisch ist, für eine Einrichtung zweckmäßig erscheinen, einen DSB auf freiwilliger Basis zu benennen. Die Artikel-29-Datenschutzgruppe („WP29“) fördert derartige freiwillige Anstrengungen. Wenn eine Einrichtung auf freiwilliger Basis einen DSB ernennt, so unterliegen dessen Benennung, Stellung und Aufgabenbereich den gleichen Anforderungen wie bei einer obligatorischen Benennung.

Quelle: Artikel 37 Absatz 1 DS-GVO

2 Was bedeutet „Kerntätigkeit“?

Als „Kerntätigkeit“ lassen sich die wichtigsten Arbeitsabläufe betrachten, die zur Erreichung der Ziele des Verantwortlichen oder des Auftragsverarbeiters erforderlich sind. Dazu gehören auch sämtliche Tätigkeiten, bei denen die Verarbeitung von Daten einen untrennbaren Bestandteil der Tätigkeit des Verantwortlichen oder Auftragsverarbeiters darstellt. So ist beispielsweise die Verarbeitung von gesundheitsbezogenen Daten, wie etwa Krankenakten von Patienten, als Kerntätigkeit eines jeden Krankenhauses anzusehen, weshalb Krankenhäuser zur Benennung eines DSB verpflichtet sind.

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

Quelle: Artikel 37 Absatz 1 Buchstabe b und c DS-GVO

3 Was bedeutet „umfangreiche Bearbeitung“?

In der DS-GVO ist nicht definiert, was unter „umfangreicher Verarbeitung“ zu verstehen ist. Die WP29 empfiehlt, bei der Klärung der Frage, ob sich von einer umfangreichen Verarbeitung sprechen lässt, die folgenden Faktoren zu berücksichtigen:

- die Zahl der betroffenen Personen – entweder als bestimmte Zahl oder als Anteil an der maßgeblichen Bevölkerung
- das Datenvolumen und/oder das Spektrum an in Bearbeitung befindlichen Daten
- 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 Dienstleistungen 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

Quelle: Artikel 37 Absatz 1 Buchstabe b und c DS-GVO

4 Was bedeutet „regelmäßige und systematische Überwachung“?

Der Begriff der regelmäßigen und systematischen Überwachung ist in der DS-GVO zwar nicht definiert, erstreckt sich jedoch eindeutig auf jede Form der Verfolgung und Profilerstellung im Internet (auch zu Zwecken der verhaltensbasierten Werbung). Gleichwohl beschränkt sich der Begriff der Überwachung nicht auf die Online-Umgebung.

Folgende Tätigkeiten können eine regelmäßige und systematische Überwachung von betroffenen Personen darstellen: Betrieb eines Telekommunikationsnetzes, Anbieten von Telekommunikationsdienstleistungen, verfolgende E-Mail-Werbung, datengesteuerte Marketingtätigkeiten, Typisierung und Scoring zu Zwecken der Risikobewertung (zum Beispiel zu Zwecken der Kreditvergabe, zur Festlegung von Versicherungsprämien, zur Verhinderung von betrügerischen Handlungen oder zur Aufdeckung 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.)

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

Quelle: Artikel 37 Absatz 1 Buchstabe b DS-GVO

5 Können Einrichtungen einen gemeinsamen DSB benennen? Wenn ja, unter welchen Voraussetzungen?

Die Antwort ist ja. Artikel 37 Absatz 2 gestattet einer Unternehmensgruppe die Benennung eines gemeinsamen DSB, sofern dieser „von jeder Niederlassung aus [...] leicht erreicht werden kann“. Der Begriff der Erreichbarkeit bezieht sich auf die Aufgabe des DSB als Ansprechpartner für Betroffene und für die Aufsichtsbehörde, aber auch als einrichtungsinterne Ansprechpartner. Um die Erreichbarkeit des DSB sowohl intern als auch extern zu gewährleisten, ist dafür Sorge zu tragen, dass seine Kontaktdaten zur Verfügung stehen. Der DSB muss – gegebenenfalls mithilfe eines Teams – in der Lage sein, mit 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.

Mehrere öffentliche Einrichtungen und Stellen können in Anbetracht ihrer Organisationsstruktur und Größe einen gemeinsamen DSB benennen. Gleiches gilt für die erforderlichen Ressourcen und die Kommunikation: Da ein DSB eine Vielzahl von Aufgaben wahrzunehmen hat, ist es Sache des Verantwortlichen oder des Auftragsverarbeiters, dafür Sorge zu tragen, dass ein einzelner DSB trotz der Zuständigkeit für mehrere öffentliche Einrichtungen und Stellen in der Lage ist, diesen – gegebenenfalls mithilfe eines Teams – wirksam nachzugehen.

Quelle: Artikel 37 Absatz 2 und 3 DS-GVO

6 Wo sollte der DSB lokalisiert sein?

Die WP29 empfiehlt, die effektive Erreichbarkeit des DSB durch die Ernennung eines DSB mit Sitz in der Europäischen Union zu gewährleisten, unabhängig davon, ob der Verantwortliche oder der Auftragsverarbeiter in der Union niedergelassen ist. Jedoch ist nicht ausgeschlossen, dass in Situationen, in denen der Verantwortliche oder der Auftragsverarbeiter nicht in der Europäischen

Union niedergelassen ist, ein außerhalb der EU niedergelassener DSB seine Aufgaben effektiver ausüben kann.

7 Kann ein externer DSB bestellt werden?

Die Antwort ist ja. Der DSB kann ein Mitarbeiter des Verantwortlichen oder des Auftragsverarbeiters (interner DSB) sein oder seine Aufgaben im Rahmen eines Dienstleistungsvertrags erfüllen. Das bedeutet, dass ein externer DSB benannt werden kann, der seine Funktion auf Grundlage eines mit einer natürlichen oder juristischen Person geschlossenen Dienstleistungsvertrags ausübt.

Falls die Funktion des DSB von einem externen Dienstleister wahrgenommen wird, kann ein Team aus für diesen Dienstleister tätigen Personen die Aufgaben des DSB unter der Verantwortung eines ernannten primären und für den Kunden „zuständigen“ Ansprechpartners in effizienter Weise ausführen. In diesem Fall ist es unverzichtbar, dass jedes Mitglied der externen Einrichtung, das die Funktionen eines DSB wahrnimmt, sämtliche in der DS-GVO genannten Anforderungen erfüllt.

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

Quelle: Artikel 37 Absatz 6 DS-GVO

8 Über welche beruflichen Qualifikationen sollte der DSB verfügen?

Der DSB ist auf der Grundlage seiner beruflichen Qualifikation und insbesondere des Fachwissens zu benennen, das er auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzt, sowie auf der Grundlage der Fähigkeit zur Erfüllung seiner Aufgaben.

Das erforderliche Niveau des Fachwissens sollte sich 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.

Die entsprechende Sachkunde und Erfahrung umfasst:

- Fachkompetenz auf dem Gebiet des nationalen und europäischen Datenschutzrechts und der Datenschutzpraxis, einschließlich eines umfassenden Verständnisses der DS-GVO
- Verständnis der jeweils durchgeführten Verarbeitungsvorgänge
- Kenntnisse in den Bereichen IT und Datensicherheit
- Kenntnis der jeweiligen Branche und Einrichtung
- die Fähigkeit, eine Datenschutzkultur innerhalb der Einrichtung zu fördern.

Quelle: Artikel 37 Absatz 5 DS-GVO

9 Welche Ressourcen sollten Verantwortliche oder Auftragsverarbeiter dem DSB zur Verfügung stellen?

Der DSB muss über die für die Erfüllung seiner Aufgaben erforderlichen Ressourcen verfügen.

Dies beinhaltet, je nach Art der Verarbeitungsvorgänge und der Tätigkeit und Größe der Einrichtung:

- eine aktive Unterstützung der Funktion des DSB durch das leitende Management
- die Gewährung von genügend Zeit für die Erfüllung der Pflichten der DSB
- angemessene Unterstützung durch Finanzmittel, Infrastrukturen (Räumlichkeiten, Einrichtungen, Ausrüstung) sowie gegebenenfalls Personal
- die offizielle Unterrichtung aller Beschäftigten über die Benennung eines DSB
- den Zugang zu anderen Dienststellen der jeweiligen Einrichtung, damit der DSB unverzichtbare Unterstützung, Anregungen und Informationen von diesen erhalten kann
- kontinuierliche Fortbildung

Quelle: Artikel 38 Absatz 2 DS-GVO

10 Wie wird die Ausübung der Pflichten und Aufgaben des DSB in vollständiger Unabhängigkeit gewährleistet? Was bedeutet „Interessenkonflikt“?

Es gibt eine Reihe von Garantien, die dazu beitragen sollen, dass der DSB seine Tätigkeit in vollständiger Unabhängigkeit ausübt:

- dem DSB dürfen bei der Erfüllung seiner Aufgaben keine Anweisungen durch den Verantwortlichen oder den Auftragsverarbeiter erteilt werden
- der DSB darf wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden
- es darf kein Interessenkonflikt im Hinblick auf sonstige Aufgaben und Pflichten bestehen

Die Wahrnehmung sonstiger Aufgaben und Pflichten durch einen DSB führt aber nicht zwangsweise zu einem Interessenkonflikt. Das bedeutet einerseits, dass der DSB innerhalb einer Einrichtung keine Position innehaben kann, 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 innerhalb der Einrichtung solche des leitenden Managements zählen (wie etwa Leiter des Unternehmens, Leiter des operativen Geschäftsbereichs, Finanzvorstand, leitender medizinischer Direktor, Leiter der Marketingabteilung, Leiter der Personalabteilung oder Leiter der IT-Abteilung), jedoch auch hierarchisch nachgeordnete Positionen, wenn die betreffenden Funktionen oder Aufgabenfelder die Festlegung von Zwecken und Mitteln der Datenverarbeitung mit sich bringen. Auch können Interessenkonflikte auftreten, wenn z. B. ein externer DSB aufgefordert wird, den Verantwortlichen oder den Auftragsverarbeiter in datenschutzrelevanten Rechtssachen vor Gericht zu vertreten.

Quelle: Artikel 38 Absätze 3 und 6 DS-GVO

Aufgaben des DSB

11 Was bedeutet „Einhaltung der Vorgaben in Bezug auf die Überwachung“

Im Rahmen dieser Überwachungspflicht sind DSB insbesondere befugt,

- Informationen zur Ermittlung von Datenverarbeitungstätigkeiten zu sammeln,
- die Einhaltung der Vorgaben bei Datenverarbeitungstätigkeiten zu analysieren und zu kontrollieren,
- den Verantwortlichen oder den Auftragsverarbeiter zu unterrichten und zu beraten und ihm Empfehlungen zu unterbreiten.

Quelle: Artikel 39 Absatz 1 Buchstabe b DS-GVO

12 Ist der DSB im Fall der Nichteinhaltung der Datenschutzanforderungen persönlich verantwortlich?

Die Antwort ist nein. Der DSB ist im Fall der Nichteinhaltung der Datenschutzanforderungen nicht persönlich verantwortlich. Es ist Aufgabe des Verantwortlichen oder des Auftragsverarbeiters, sicherzustellen und nachweisen zu können, dass die Verarbeitung gemäß dieser Verordnung erfolgt. Für die Einhaltung der datenschutzrechtlichen Bestimmungen ist der Verantwortliche oder der Auftragsverarbeiter verantwortlich.

13 Welche Funktion kommt dem DSB bei einer Datenschutz-Folgenabschätzung und beim Führen von Verzeichnissen zu Verarbeitungsvorgängen zu?

In Sachen Datenschutz-Folgenabschätzung lässt sich der Verantwortliche bzw. der Auftragsverarbeiter vom DSB beraten,

- 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 die 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 den Datenschutzanforderungen stehen

In Bezug auf die Verzeichnung von Verarbeitungsvorgängen liegt es in der Verantwortung des Verantwortlichen oder des Auftragsverarbeiters und nicht des DSB, ein Verzeichnis der Verarbeitungsvorgänge zu führen. Den Verantwortlichen bzw. den Auftragsverarbeiter hindert jedoch 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.

Quelle: Artikel 39 Absatz 1 Buchstabe c und Artikel 30 DS-GVO

Brüssel, den 13. Dezember 2016

Für die Arbeitsgruppe

Die Vorsitzende

Isabelle FALQUE-PIERROTIN

Am 5. April 2017 angenommene überarbeitete
Fassung

Für die Arbeitsgruppe

Die Vorsitzende

Isabelle FALQUE-PIERROTIN