Das berufliche Leitbild der Datenschutzbeauftragten

Code of Practice for Data Protection Officers

4. Ausgabe 2018 | *Edition 4/2018*

Publikation des Berufsverbandes der Datenschutzbeauftragten Deutschlands (BvD) e.V.

Publication of the Association of Data Protection Officers of Germany (BvD) e.V.

BvD e.V.
DATENSCHUTZ GESTALTEN

INHALT | CONTENT

HINWEIS ZUR AKTUELLEN AUSGABE | NOTE ON THE CURRENT EDITION 4
VORWORT | PREFACE 8
BEGRIFFE | TERMS 12
ZUSAMMENFASSUNG | SUMMARY 14

1 Die persönlichen und fachlichen Voraussetzungen 18
Personal and professional requirements
1.1 Voraussetzung für die Berufsausübung 18
Professional practice requirements
1.2 Fachwissen 18
Expertise
1.3 Weitere persönliche Voraussetzungen 22
Other personal requirements

2 Datenschutzmanagementsystem 26
Data protection management system
2.1 Ziele und Aufgaben im Datenschutzmanagementsystem 26
Objectives and tasks of the data protection management system
2.2 Grundsätze und Prozesse 26
Basic principles and processes

3 Aufgaben und Leistungen des Datenschutzbeauftragten 30
Tasks and services of the Data Protection Officer
3.1 Übersicht der Aufgaben der Datenschutzbeauftragten 30
Overview of tasks of the Data Protection Officer
3.2 Managementaufgaben 32
Management tasks
3.3 Beraten 32
Advising
3.4 Überwachen 36
Monitoring
3.5 Berichten und Informieren 42
Reporting and informing
3.6 Schulungs- und Sensibilisierungsaufgaben 44
Training and awareness-raising tasks

4 Anforderungen an die Berufsausübung 46
Professional practice requirements
4.1 Haltung zur Berufsausübung 46
Attitude towards professional practice
4.2 Ansprechbarkeit 46
Responsiveness
4.3 Überprüfbarkeit 48
Verifiability
4.4 Verschwiegenheit und Vertraulichkeit 48
Discretion and confidentiality
4.5 Qualitätssicherung der Aufgabenerfüllung 50
Quality assurance regarding the task completion
4.6 Benennung zum Datenschutzbeauftragten 50
Designation as data protection officer
4.7 Haftung und Versicherungspflicht 54
Liability and obligation to take out insurance
Revision / Unter Berücksichtigung der … 58
Revision / Taking into account …

HINWEIS ZUR AKTUELLEN AUSGABE

Die Fortschreibung des Beruflichen Leitbilds der Datenschutzbeauftragten befindet sich – vor dem Hintergrund der Auslegung, Einführung und Umsetzung der Bestimmungen der EU-Datenschutzgrundverordnung (DS-GVO) – in einem laufenden Prozess. Dies betrifft vor allem die genaue Interpretation der konkreten Pflichten und Aufgaben eines Datenschutzbeauftragten in diesem neuen Rechtsrahmen. Des Weiteren gibt es Aufgaben des Verantwortlichen, bei denen die Datenschutzbeauftragten eingebunden werden können um den Verantwortlichen zu unterstützen. Insbesondere zur Abgrenzung in diesem Bereich finden momentan noch Diskussionen auf Experten- und Aufsichtsebene statt.

Der Datenschutzbeauftragte im öffentlichen Bereich findet in dieser Version des Beruflichen Leitbildes noch keine Berücksichtigung. Die DS-GVO gibt vor, dass nun stets ein Datenschutzbeauftragter im öffentlichen Bereich zu benennen ist. Die Ausgestaltung der Tätigkeit erfolgt momentan durch die Überarbeitung und Anpassung der Landesdatenschutzgesetze, die zu diesem Zeitpunkt nur teilweise vorliegen. Unabhängig davon gelten die grundsätzlichen Aussagen zum Datenschutzbeauftragten (nach DS-GVO) aus dem Beruflichen Leitbild auch für die Datenschutzbeauftragten im öffentlichen Bereich.

Damit konzentriert sich diese Version des Beruflichen Leitbildes zunächst auf den nicht-öffentlichen Bereich. Durch das neue Bundesdatenschutzgesetz (BDSG-neu) wurde die Konkretisierungsvorgabe der DS-GVO zu den Datenschutzbeauftragten dahingehend konkretisiert, das Unternehmen, die mindestens 10 Personen mit der Verarbeitung personenbezogener Daten beschäftigen, zur Benennung von Datenschutzbeauftragten verpflichtet sind. Diese Regelung schreibt also die in Deutschland bewährte Bestellpflicht der Datenschutzbeauftragten fort. Ferner müssen Verantwortliche und Auftragsverarbeiter Datenschutzbeauftragte bestellen, wenn

NOTE ON THE CURRENT EDITION

With respect to the ongoing interpretation, introduction and implementation of the provisions of the EU General Data Protection Regulation (GDPR), the professional Code of Practice for Data Protection Officers is being updated on an ongoing basis. This concerns the exact interpretation of the specific duties and tasks of a data protection officer in this new legislative framework in particular. There are, moreover, tasks of the controller where the data protection officers can be integrated, in order to assist the controller. In particular with regard to the delimitation in this area, discussions are currently taking place among experts and at supervisory level.

The data protection officer in the public sector has not yet been taken into consideration in this version of the professional Code of Practice. The EU General Data Protection Regulation specifies that a data protection officer in the public sector is now always to be appointed. The activity is currently being shaped by the revision and adaptation of the data protection laws in the german federal states, which only partially exist to date. Notwithstanding the latter, the fundamental statements on the Data Protection Officer (in accordance with the GDPR) from the professional Code of Practice also apply to Data Protection Officers in the public sector.

Thus, this version of the professional Code of Practice initially focuses on the non-public sector. The new Federal Data Protection Act (BDSG-new) concretises the GDPR final requirements for Data Protection Officers, mandating that companies that engage 10 persons or more for the processing of personal data must appoint Data Protection Officers. This regulation therefore continues the existing obligation in Germany to appoint data protection officers. Controllers and processors must furthermore appoint Data Protection Officers if they are obligated to carry out data

diese zur Durchführung Datenschutz-Folgenabschätzung nach Artikel 35 der Verordnung (EU) 2016/679 verpflichtet sind oder wenn sie personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung, der anonymisierten Übermittlung oder für Zwecke der Markt- oder Meinungsforschung verarbeiten.

Auf Basis der vorhandenen Vorgaben der DS-GVO, des BDSG-neu und des WP 243 und aktueller Dokumente der Aufsichtsbehörden und Fachkreise wurden hier entsprechende Aufgaben und Pflichten zusammengetragen und das berufliche Leitbild an die (DS-GVO) angepasst. Die im WP 243 diskutierten DPO-Teams finden in dieser Version des Beruflichen Leitbildes noch keine gesonderte Berücksichtigung, da auch hierzu noch Klärungsbedarf besteht.

Die weitere Entwicklung in der Gesetzgebung, Rechtsprechung und Diskussion wird vom Ausschuss Berufsbild des BvD intensiv beobachtet, konstruktiv mitgestaltet und im beruflichen Leitbild fortlaufend ergänzt.

protection impact assessments as per Article 35 of Regulation (EU) 2016/679 or if they are commercially they commercially process personal data for the purpose of transfer, of anonymized transfer or for purposes of market or opinion research.

Based on the existing requirements of the EU General Data Protection Regulation, the new version of the Federal Data Protection Act (BDSG) and the WP 243 and current documents issued by the supervisory authorities and specialist circles, corresponding tasks and duties have been compiled in this context, and the professional Code of Practice adapted to the EU General Data Protection Regulation. The DPO teams discussed in the WP 243 have not yet separately been taken into account in this version of the professional Code of Practice, as, also in this respect, there is a requirement for clarification.

The further development in the legislation, case law and expert discussion is being observed intensively by the Occupational Profile Committee of the Association of Data Protection Officers (BvD), constructively co-designed, and supplemented in the professional Code of Practice on an ongoing basis.

VORWORT

**Daten sind der zentrale Faktor in modernen Wertschöpfungsketten.
Sie verdienen unsere Professionalität.**

Im Rahmen der Digitalisierung rückt die Verarbeitung von Daten – insbesondere von personenbezogenen Daten – immer mehr ins Zentrum der Wertschöpfungskette. Daher steigen die Anforderungen an die Rechtmäßigkeit der Datenverarbeitung und die Sicherheit der Verarbeitungsprozesse stark an. Nicht nur Prozess-Know-how auch die Datenquantität und insbesondere -qualität entscheiden über den Geschäftserfolg und sind daher als elementarer Erfolgsfaktor und Unternehmenswert zu behandeln.

Unternehmensleitung wie auch Kunden und Mitarbeiter müssen sich im hochkomplexen und schnell verändernden Umfeld der Digitalisierung darauf verlassen können, dass sie durch qualifizierte Experten mit umfassendem Know-how begleitet und im Kontext der Sicherheit und Compliance unterstützt werden.

Die Datenschutzbeauftragten nehmen sich genau dieser Aufgaben seit Jahrzehnten an. Sie begleiten die Unternehmen auf dem Weg der Digitalisierung und haben dabei einerseits die Betroffenenrechte – insbesondere die Persönlichkeitsrechte von Kunden und Beschäftigten – und andererseits die Bedürfnisse und den Erfolg der Unternehmen im Blick. Datenschutzbeauftragte ermöglichen innovative Lösungen und schützen Unternehmenswerte wie das Unternehmensimage und den Wert der Marke, indem sie Kundenvertrauen aufbauen und erhalten. Sicherer und zulässiger Umgang mit Daten ist zunehmend Gegenstand von Kundenentscheidungen und damit ein wichtiger Wettbewerbsfaktor. In dieser Rolle helfen Datenschutzbeauftragte nicht nur, die geltenden Gesetze einzuhalten, sie tragen mit ihrem Know-how dazu bei, dass der beste Prozess mit einer sicheren Lösung zum Erfolg für alle wird.

PREFACE

**Data are a central factor in modern value-added chains.
They deserve our professionalism.**

In the context of digitalisation, the processing of data, particularly of personal data, is increasingly moving into the centre of the value-added chain. Therefore, the requirements concerning the lawfulness of the data processing and the security of the processing procedures are increasing significantly. Not only process expertise but also the quantity and, in particular, the quality of data are decisive for business success and should therefore be treated as a fundamental success factor and corporate value.

In a highly complex and rapidly changing digitalisation environment, corporate management as well as customers and staff must be able to rely on support from qualified experts offering comprehensive expertise and assistance where security and compliance are concerned.

Data protection officers have been adopting these tasks for many decades. They support companies on the path towards digitalisation and therefore focus on the one hand on the rights of the individuals affected, particularly the personal rights of customers and persons employed, and on the other hand the success of the company. Data protection officers facilitate innovative solutions and protect corporate values such as the corporate image and the value of the brand by building up and maintaining customer confidence. Secure and admissible handling of data is increasingly the subject of customer decisions, and thus an important competitive factor. In this role, data protection officers not only help to keep existing laws but also contribute with their expertise to ensuring that the best process, combined with a secure solution, becomes a success for everyone concerned.

Um all diese Herausforderungen stemmen zu können, ist eine solide und umfassende Qualifikation des Datenschutzbeauftragten unabdingbar. Insbesondere ist Know-how in den folgenden Bereichen erforderlich:

- Prozesse und Organisation
- IT Systeme und Applikationen
- Datenschutzrecht

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. hat bereits 2004 damit begonnen, die Anforderungen an die Tätigkeit und das Know-how des Datenschutzbeauftragten zu beschreiben. 2009 entstand daraus das erste „Berufliche Leitbild des Datenschutzbeauftragten" in Europa, auf das sich Mitglieder schriftlich verpflichten müssen, um durch den BvD als entsprechend qualifiziert ausgezeichnet zu werden.

Durch diesen Prozess und die Auszeichnung „Selbstverpflichtung auf das berufliche Leitbild des Datenschutzbeauftragten" können Unternehmen und Institutionen nachweisen, dass qualifizierte Datenschutzbeauftragte benannt wurden.

Die vorliegende vierte Auflage des Leitbilds greift die Änderungen durch die DS-GVO und das BDSG-neu auf und stellt die neuen Aufgaben und Anforderungen ins Verhältnis zur erforderlichen Qualifikation der Datenschutzbeauftragten.

Berlin, März 2018
Thomas Spaeing
Vorstandsvorsitzender

A solid and comprehensive qualification of the Data Protection Officer is indispensable to be able to overcome such challenges. Expertise is particularly necessary in the following areas:

- Processes and organisation
- IT systems and applications
- Data protection law

The Association of Data Protection Officers of Germany began as early as 2004 to define the requirements for this field of activity and the expertise needed by Data Protection Officers. In 2009, the first "Code of practice for data protection officers" in Europe was created which members were required to commit themselves to in writing in order to be accredited by the BvD as being qualified in this respect.

Through this process and the "voluntary commitment to the code of practice for data protection officers" accreditation, companies and institutions can verify that qualified data protection officers have been designated.

This fourth issue of the professional Code of Practice incorporates the amendments made by the GDPR and the new version of the Federal Data Protection Act (BDSG), putting the new tasks and requirements in perspective in relation to the qualification required by data protection officers.

Berlin, March 2018
Thomas Spaeing
Chairman of the Board

BEGRIFFE

Aus Gründen der besseren Lesbarkeit werden im nachfolgenden Dokument Begriffe und Abkürzung auf Basis folgender Definition verwenden:

- **DS-GVO:** Europäische Datenschutz-Grundverordnung
  im internationalen Kontext: **GDPR** – General Data Protection Regulation

- **Auftragsverarbeiter:** Der Begriff des Auftragsverarbeiters wird in Art. 4 Nr. 8 DS-GVO definiert: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.

- **Verantwortlicher:** Der Begriff des für die Verarbeitung Verantwortlichen wird in Art. 4 Nr. 7 DSGVO definiert: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden.
  Im nachfolgenden Dokument wird bei der Verwendung des Begriffs des für die Verarbeitung Verantwortlichen eine erweiterte Auslegung der Definition verwendet, die den Auftragsverarbeiter inkludiert, da dieser aus Sicht der DSGVO Kapitel IV im Bereich des Datenschutz-Managements äquivalente Aufgaben hat und das Dokument so in seiner Lesbarkeit gewinnt.

- **Leitung (des Verantwortlichen):** Geschäftsleitung, Vorstand, Behördenleitung oder entsprechende Personenkreise.

TERMS

To make it more readable, the following document uses terms and abbreviations based on the following definitions:

- **GDPR:** European General Data Protection Regulation
  In an international context: GDPR - General Data Protection Regulation

- **Processors:** The term 'processor' is defined in Article 4(8) GDPR: a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

- **Controller:** The term 'controller' is defined in Article 4(7) GDPR: the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its appointment may be provided for by Union or Member State law;
  In the document which follows, the use of the term 'controller' makes use of an extended interpretation of the definition which includes the processor, since in the view of the GDPR Chapter IV on data protection management the former has equivalent tasks, and the document becomes more readable as a result.

- **Management (of controller):** Management, board of directors, public authority management or respective individuals.

ZUSAMMENFASSUNG

Ausgangssituation

Die DS-GVO stellt insbesondere im Kapitel IV hohe Anforderungen an die Pflichten des Verantwortlichen. Um diese Compliance Anforderungen insbesondere auch die daraus erwachsenden Nachweispflichten erfüllen zu können und ein betriebliches Organisationsverschulden des Verantwortlichen zu vermeiden, ist der Betrieb eines Managementsystems für den Bereich Datenschutz unabdingbar.

Bewährte Beispiele von Managementsystemen sind bereits im folgenden Kontext gängige Praxis:

- Qualitätsmanagements (DIN EN ISO 9001)
- Umweltmanagements (DIN EN ISO 14001)
- Arbeits- und Gesundheitsschutzes (OHSAS 18001, zukünftig DIN EN ISO 45001)
- Informationssicherheit (DIN ISO/IEC 27001)

Der Unterschied besteht allerdings darin, dass die Vorgaben vom europäischen Gesetzgeber kommen und nicht aus einer DIN EN/ISO/IEC Norm.

Umsetzung mit Unterstützung qualifizierter Datenschutzbeauftragter

Die Umsetzung des Datenschutzmanagements obliegt der Leitung des Verantwortlichen – also der Geschäftsleitung, dem Vorstand, der Behördenleitung oder entsprechenden Personenkreisen. Um dieser Pflicht nachzukommen, ist die Unterstützung durch qualifizierte Datenschutzbeauftragte unabdingbar. Die nachfolgenden Kapitel zeigen auf, welche persönlichen und fachlichen Voraussetzungen qualifizierte Datenschutzbeauftragte mitbringen müssen, welche Aufgaben und Leistungen sie erfüllen und welche Anforderungen an die Berufsausübung gestellt werden, um die

SUMMARY

Initial situation

The GDPR, particularly in Chapter IV, makes high demands on the obligations of the controller. In order to meet these compliance requirements, particularly including the ensuing burden of proof, and to avoid corporate organisational culpability by the controller, it is essential to operate a management system for the field of data protection.

Proven examples of management systems are already common practice in the following contexts:

- Quality management (DIN EN ISO 9001)
- Environmental management (DIN EN ISO 14001)
- Occupational health and safety (OHSAS 18001, in future DIN EN ISO 45001)
- Information security (DIN ISO/IEC 27001)

The difference, however, lies in the fact that the requirements come from the European legislator and not from a DIN EN/ISO/IEC standard.

Implementation with support of qualified data protection officers

The implementation of data protection management is the responsibility of the controller i.e. the management, the board of directors, the public authority management or respective individuals. Support through qualified data protection officers is essential in order to meet this obligation. The following chapters identify the personal and professional requirements that qualified data protection officers are required to have, the tasks and services that they need to fulfil and the professional practice demands that are made to enable the challenges of data

Herausforderungen des Datenschutzes in einer zunehmend digitalisierten Welt und im Kontext der DS-GVO erfüllen zu können:

- Die persönlichen und fachlichen Voraussetzungen (Kapitel 1)
- Aufgaben und Leistungen des Datenschutzbeauftragten (Kapitel 2)
- Anforderungen an die Berufsausübung (Kapitel 3)

Durch den Prozess der „Selbstverpflichtung auf das berufliche Leitbild des Datenschutzbeauftragten“, das in den anschließenden Kapiteln detailliert wird, kann die Leitung des Verantwortlichen nachweisen, dass qualifizierte Datenschutzbeauftragte benannt wurden.

protection to be met in an increasingly digitalised world and in the context of the GDPR:

- The personal and professional requirements (Chapter 1)
- Tasks and services of a data protection officer (Chapter 2)
- Professional practice requirements (Chapter 3)

Through the process of “voluntary commitment to the code of practice for the data protection officer”, which is detailed in the following chapter, the controller management can verify that qualified data protection officers have been designated.

1 DIE PERSÖNLICHEN UND FACHLICHEN VORAUSSETZUNGEN[1]

1.1 Voraussetzung für die Berufsausübung

Die Ausübung des Berufs „Datenschutzbeauftragter" setzt voraus, dass derjenige in der Regel

- über eine angemessene berufliche Qualifikation in zumindest einer der Kategorien Organisation und Prozesse, Informations- und Kommunikationstechnologie (IuK) oder Recht besitzt und solides Fachwissen in den beiden anderen Kategorien erworben hat,
- über eine mindestens 2-jährige Berufserfahrung in den genannten Bereichen verfügt und
- eine anerkannte Qualifikation zum Datenschutzbeauftragten erlangt hat.

1.2 Fachwissen

Datenschutzbeauftragte verfügen unabhängig von Branche und Größe des Unternehmens bzw. der Behörde über ein Mindestmaß an Fachwissen und deren praktischen Anwendungen. Darüber hinaus kann je nach konkreter Aufgabenstellung in dem Unternehmen bzw. der Behörde weiteres individuelles Fachwissen nötig werden.

1.2.1 Datenschutzrechtliches Fachwissen

Datenschutzbeauftragte verfügen über Wissen im Datenschutzrecht. Sie kennen sich in den datenschutzrelevanten Vorschriften ihres Fachbereiches/ihrer Branche aus. Datenschutzbeauftragte sind in der Lage, die für das Aufgabengebiet geltenden Rechtsvorschriften anzuwenden oder sich diese zu erschließen. Das Fachwissen umfasst die folgenden Bereiche:

- Allgemeines Persönlichkeitsrecht und Grundrechtecharta der EU mit Datenschutzbezug,
- Grundlagen des europäischen und jeweiligen nationalen Datenschutzrechts und dessen Prinzipien,
- Rechtsgrundlagen der Verarbeitung personenbezogener Daten,
- datenschutzrechtliche Anforderungen beim Einsatz der IuK.

[1] Konkretisierung der Anforderungen aus Art. 37 Abs. 5 DS-GVO

1 PERSONAL AND PROFESSIONAL REQUIREMENTS[1]

1.1 Professional practice requirements

As a rule, the ability to practise the occupation of "data protection officer" is conditional upon having

- an appropriate professional qualification in at least one of the categories of organisation and processes, information and communication technology (ICT) or law, and has gained sound expertise in the two other categories,
- at least two years' professional experience in the fields indicated and
- gained a recognised qualification as a data protection officer.

1.2 Expertise

Irrespective of the business sector and size of the company or public authority, data protection officers shall have a minimum amount of expertise and its practical applications. In addition, depending on the specific tasks in the company or public authority, further individual expertise may become necessary.

1.2.1 Expertise in the field of data protection law

Data protection officers shall have knowledge in data protection law. They will be familiar with the regulations of their professional field or business sector pertaining to data protection. Data protection officers are able to bring applicable legal provisions to bear on the task area or to acquire these. The expertise will include the following fields:

- General personal rights and EU charter of fundamental rights with reference to data protection,
- Basic principles of European and relevant national data protection law and its principles,
- Legal basis of processing personal data,
- Data protection-related requirements when using ITC.

[1] Specification of requirements of Article 37(5) GDPR

1.2.2 IuK-Fachwissen

Datenschutzbeauftragte müssen über technisches Verständnis verfügen und Sachverhalte der Informationstechnologien verstehen:

- Organisation der IuK
- Strukturen von IT-Systemen, IT-Applikationen und IT-Prozessen
- Informationssicherheitsmanagement, basierend auf den Schutzzielen der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit
- Erkennen von Risiken für betroffene Personen, die aus IT-Systemen, IT-Applikationen und IT-Prozessen resultieren

Darüber hinaus können Datenschutzbeauftragte grundlegende Risiken für Rechte und Freiheit der betroffenen Personen durch die Verarbeitung personenbezogener Daten erkennen und beurteilen. Datenschutzbeauftragte sind in der Lage, grundlegende Verbesserungen unter Anwendung datenschutzfreundlicher Technologien[2] vorzuschlagen und Normen zur Informationssicherheit zu berücksichtigen.

1.2.3 Betriebswirtschaftliches und organisatorisches Fachwissen

Datenschutzbeauftragte müssen über folgendes betriebswirtschaftliches und organisatorisches Wissen verfügen, um Sachverhalte im Unternehmens- bzw. Behördenkontext beurteilen zu können:

- Unternehmens- bzw. Behördenprozesse
- Managementsysteme
- Verwaltungsvorschriften und -verfahren[3]
- Methoden zur Risikoanalyse
- Audit- und Prüfverfahren.

[2] Art. 25 DS-GVO, [3] WP 243, 2.4., berufliche Qualifikation bei Behörden und öffentlichen Stellen

1.2.2 ITC expertise

Data protection officers must have technical understanding and comprehend issues concerning information technologies:

- Organisation of ITC
- Structures of IT systems, IT applications and IT processes
- Information security management, based on the protective objectives of confidentiality, integrity, availability and resilience
- Identification of risks for data subjects which result from IT systems, IT applications and IT processes

Furthermore, data protection officers can identify and evaluate basic risks to the rights and freedom of data subjects through the processing of personal data. Data protection officers are in a position to propose fundamental improvements using privacy enhancing technologies[2] and take into account information security standards.

1.2.3 Business administration and organisational expertise

Data protection officers must have the following business administration and organisational knowledge to enable them to evaluate issues in a company and/or public authority context:

- processes in companies and/or public bodies
- Management systems
- Administrative regulations and procedures[3]
- Methods of risk assessment
- Audit and monitoring procedures.

[2] Article 25 GDPR, [3] WP 243, 2.4., professional qualification in the case of public authorities

1.2.4 Erweitertes Fachwissen

Zusätzlich zum grundlegenden Fachwissen sind je nach Branche, spezieller Unternehmens- oder Einsatzbereiche des Datenschutzbeauftragten weitere Spezialisierungen in den Bereichen Recht, Technik und Organisation in Abhängigkeit der Kerntätigkeit des Verantwortlichen oder Auftragsverarbeiters[4] erforderlich. Dieses können auch Verhaltensregeln[5] der entsprechenden Branche sein.

1.2.5 Aktualität der Fachkunde

Datenschutzbeauftragte aktualisieren und vertiefen ihr Fachwissen regelmäßig[6]. Dies bezieht insbesondere gesetzliche Änderungen und aktuelle Rechtsprechung zum Datenschutz sowie neue technische Entwicklungen ein.

1.3 Weitere persönliche Voraussetzungen

1.3.1 Persönliche Integrität

Datenschutzbeauftragte, die nicht über eine ausreichende persönliche Integrität verfügen, sind für die Erfüllung der Aufgaben nicht geeignet. Dies gilt auch für Personen, die

- rechtskräftig verurteilt wurden wegen Verletzungen des Geheimnisschutzes des persönlichen Lebensbereiches oder
- infolge strafgerichtlicher Verurteilung die Fähigkeit zur Bekleidung öffentlicher Ämter nicht besitzen.

Die Tätigkeiten sollen außerdem nicht von Personen ausgeübt werden, die innerhalb der letzten zwei Jahre wegen Verletzung von Datenschutzvorschriften, IT- oder Computerstrafrecht rechtskräftig gekündigt wurden[7].

[4] WP 234, 2.1.2 Kerntätigkeit, [5] Art. 40 DS-GVO, [6] WP 243, 3.2 erforderliche Ressourcen,
[7] Verstöße gegen Berufsgeheimnisse, siehe Art. 90 Abs. 1 Satz 2 DS-GVO

1.2.4 Extended expertise

In addition to the basic expertise, special business areas or fields of use of the data protection officer may, depending upon the core activities of the controller, require further specialisation in the areas of law, technology and organisation, depending on the core activity of the controller or processor[4]. This can also include codes of conduct[5] for the business sector concerned.

1.2.5 Topicality of expert knowledge

Data protection officers update and improve their expertise on a regular basis[6]. This applies particularly for legal amendments and current jurisdiction concerning data protection and new technical developments.

1.3 Other personal requirements

1.3.1 Personal integrity

Data protection officers who do not have sufficient personal integrity are not suited to fulfilling the tasks. This also applies to persons who

- have been convicted of infringements of personal secrecy or
- due to a conviction for a criminal offence are not able to hold public office.

The occupation should also not be exercised by persons who have been legally dismissed due to infringement of data protection regulations, or IT or computer crime within the past two years[7].

[4] WP 234, 2.1.2 Core activity, [5] Article 40 GDPR, [6] WP 243, 3.2 Resources required,
[7] For violations of trade secrets, refer to the second sentence of Article 90(1) GDPR

1.3.2 Beratungskompetenzen

Datenschutzbeauftragte verfügen unabhängig von Branche und Größe des Unternehmens bzw. der Behörde über Fertigkeiten und Fähigkeiten, die zur selbständigen Organisation ihres Arbeitsbereiches erforderlich sind. Datenschutzbeauftragte entwickeln konstruktive Vorschläge für datenschutzkonforme Lösungen unter Berücksichtigung unterschiedlicher Interessen und sind in der Lage, Empfehlungen, Stellungnahmen und Positionen zu vertreten. Hier sind Kompetenzen wie bspw. Kommunikations- und Moderationstechniken, Problemlösungstechniken erforderlich.

1.3.3 Durchsetzungsfähigkeit des eigenen Status

Datenschutzbeauftragte können übertragene Aufgaben selbständig ausführen, den Status einfordern und Einschränkungen abwenden. Zum Status gehören insbesondere die Unabhängigkeit und die Weisungsfreiheit[8].

[8] Art. 38 Abs. 3 mit ErwGr 97 DS-GVO

1.3.2 Advisory competence

Data protection officers, irrespective of the business sector and size of the company or the public authority, have the necessary skills and capabilities for independently organising their field of work. Data protection officers propose constructive proposals for data protection-compliant solutions that consider different interests and are able to advocate recommendations, opinions and positions. This requires skills such as communication and moderation techniques and problem-solving techniques.

1.3.3 Assertiveness of own professional status

Data protection officers can perform delegated tasks independently, assert their status and avert limitations. The status includes independence and the authority to act autonomously[8] in particular.

[8] Article 38(3) with Recital 97 GDPR

2 DATENSCHUTZMANAGEMENTSYSTEM

2.1 Datenschutzmanagement

Um die Anforderungen des Datenschutzes vorausschauend, nachhaltig, effizient und risikobasiert in einer Organisation zu implementieren, ist ein Datenschutzmanagementsystem von der Leitung zu etablieren und verbindlich zu betreiben[9]. Die Umsetzung eines angemessenen Organisations- bzw. Managementsystems orientiert sich an den Datenschutzanforderungen der Organisationsstruktur und deren Verarbeitungsprozesse.

Das Datenschutzmanagementsystem stellt die Wirksamkeit der datenschutzrelevanten technischen und organisatorischen Maßnahmen in der Organisation, in Prozessen und Systemen sicher. Das Datenschutzmanagementsystem sorgt dafür, dass Datenschutzbeauftragte frühzeitig in alle datenschutzrelevanten Sachverhalte eingebunden werden.[10]

In Anlehnung an bestehende Managementsysteme (z.B. DIN EN ISO 9001 Qualitätsmanagement oder DIN ISO/IEC 27001 Informationssicherheitsmanagement) sichert ein iterativer Verbesserungsprozess eine regelmäßige Überprüfung der Einhaltung und eine nachhaltige und effiziente Umsetzung der Datenschutzanforderungen in der Organisation.[11] Datenschutzbeauftragte überprüfen die Umsetzung und Einhaltung der Vorgaben des Datenschutzmanagementsystems und informieren die Leitung über das Ergebnis.[12]

2.2 Grundsätze und Prozesse

Das Datenschutzmanagementsystem stellt die planmäßige Umsetzung datenschutzrechtlicher Grundsätze[13] bei der Datenverarbeitung personenbezogener Daten unter Berücksichtigung eines dem Risiko angemessenen Schutzniveaus sicher. Innerhalb des Datenschutzmanagementsystems sind Prozesse zu definieren und regelmäßig auf ihre Wirksamkeit zu überprüfen, um die Pflichten der Verantwortlichen als interne Vorgabe für Organisation festschreiben. Datenschutzbeauftragte sind bei der Er-

[9] Art. 24 mit ErwGr 74 DS-GVO, [10] WP 243 3.1, [11] Art. 32 Abs. 1 lit. d,
[12] Art. 39 Abs. 1 lit. b, WP 243 4.1, [13] Art. 5 DS-GVO

2 DATA PROTECTION MANAGEMENT SYSTEM

2.1 Objectives and tasks of the data protection management system

In order to implement the data protection requirements proactively, sustainably, efficiently and risk-based within an organisation, a data protection management system is to be established and bindingly operated by the management[9]. The implementation of an appropriate organisational or management system is orientated toward the data protection requirements of the organisational structure and its processing procedures.

The data protection management system ensures the efficacy of the technical and organisational measures relevant to data protection within the organisation, processes and systems.The data protection management system ensures that data protection officers are integrated into all circumstances relevant to data protection at an early stage.[10]

Based on existing management systems (DIN EN ISO 9001 quality management or DIN ISO/IEC 27001 information security management), an iterative improvement process ensures regular auditing of compliance, and sustainable and efficient implementation of the data protection requirements within the organisation.[11]
Data protection officers monitor the implementation and compliance of the requirements of the data protection management system and inform management about the result. [12]

2.2 Basic principles and processes

The data protection management system ensures the systematic implementation of basic data protection principles[13] during the processing of personal data, taking into account a level of protection appropriate to the risk. Within the data protection management system, processes which stipulate the obligations of controllers as an internal requirement of the organisation must be defined and audited regularly to determine their effectiveness. Data protection officers are not bound by instruc-

[9] Article 24 with Recital 74 GDPR, [10] WP 243 3.1, [11] Art. 32(1)(d),
[12] Article 39(1)(b), WP 243 4.1, [13] Article 5 GDPR

füllung ihrer Aufgaben weisungsfrei und berichten in ihrer Funktion der Leitung. Weisungen innerhalb der Organisation sind durch die Leitungen zu erteilen.[14] Die Leitung bleibt für alle Aufgaben, Prozesse und deren Umsetzung im Datenschutzmanagementsystem verantwortlich.[15]

Die Dokumentation der Überprüfung des Datenschutzmanagementsystems und der daraus abgeleiteten Maßnahmen stellen den Nachweis der Leitung über die Rechtmäßigkeit der Verarbeitungstätigkeit im Einklang mit den geltenden Datenschutzvorschriften und der Wirksamkeit der Datenschutzorganisation dar. Diese Aufgabe kann von den Datenschutzbeauftragten mit bearbeitet werden.[16]

Zum Datenschutzmanagementsystem gehören insbesondere:

- ein Risikomanagement bezogen auf Datenschutzrisiken und die Sicherheit der Verarbeitung, welches die Analyse, Umsetzung, regelmäßige Überprüfung und Anpassung technischer und organisatorischer Maßnahmen umfassen[17]
- Prozesse zur Umsetzung der Datenschutzanforderungen durch Technikgestaltung und datenschutzfreundliche Voreinstellungen[18]
- die Dokumentation der Verarbeitungstätigkeiten[19]
- die Zusammenarbeit mit der Aufsichtsbehörde[20]
- das Verfahren von erforderlichen Meldungen an die Aufsichtsbehörde[21]
- die Sicherstellung der Rechte betroffener Personen insbesondere die Behandlung von Anfragen von betroffenen Personen
- die Informationspflichten und die Benachrichtigung betroffener Personen bei einer Verletzung des Schutzes personenbezogener Daten
- das Erkennen der Erforderlichkeit und die Durchführung einer Datenschutz-Folgenabschätzung
- Umsetzung und Weiterentwicklung des Sensibilisierungs- und Schulungskonzepts[22]

[14] WP 243 2.1, [15] WP 243 4.1, [16] WP 243 4.5, [17] Art. 24, Art. 32 DS-GVO, [18] Art. 25 DS-GVO, [19] Art. 30 DS-GVO, [20] Art. 39 Abs. 1 lit. d, [21] Art. 31, 33 und 36 DS-GVO, [22] Art. 39 DS-GVO

tions when fulfilling their tasks, and report, in their capacity, to the management. Instructions within the organisation are to be issued by the management.[14] The management shall remain responsible for all tasks, processes and their implementation in the data protection management system.[15]

Documentation of the audit of the data protection management system and the measures derived from it constitutes objective evidence for the management of the legitimacy of the processing activity in compliance with the applicable data protection regulations and the effectiveness of the data protection organisation. This task may be co-processed by Data Protection Officers.[16]

The data protection management system includes, in particular:

- A risk management system, with reference to data protection risks and the security of processing, which includes analysis, implementation, regular auditing and adaptation of technical and organisational measures.[17]
- Processes for implementing the data protection requirements through data protection by design and data protection-enhancing default settings[18]
- Documentation of processing activities[19]
- Co-operation with the supervisory authority[20]
- The process of enhancing to the supervisory authority[21]
- Safeguarding the rights of data subjects, particularly the handling of enquiries from data subjects
- The duty to inform and the notification of data subjects in the event of a personal data breach
- Recognition of the necessity and the implementation of a data protection impact assessment
- Implementation and further development of the awareness-raising and training concept[22]

[14] WP 243 2.1, [15] WP 243 4.1, [16] WP 243 4.5, [17] Article 24, Article 32 GDPR, [18] Article 25 GDPR, [19] Article 30 GDPR, [20] Art. 39(1)(d), [21] Article 31, 33 and 36 GDPR, [22] Article 39 GDPR

3 AUFGABEN UND LEISTUNGEN DER DATENSCHUTZBEAUFTRAGTEN

3.1 Übersicht der Aufgaben der Datenschutzbeauftragten

Aufgabe	Quelle (DSGVO)	Beschreibung
Managementaufgaben	Art. 24 Art. 38 Abs.1 ErwGr 97	• Einbindung des Datenschutzbeauftragten durch den Verantwortlichen in datenschutzrelevante Managementsysteme • Beratung zu Zielen und Aufgaben sowie bei der Fortschreibung des Datenschutzmanagementsystems • Review des Datenschutzmanagementsystems
Beraten	Art. 38 Abs. 1, 4 Art. 39 ErwGr 77, 97 Art. 35 Art. 88 ErwGr 155	• Beratung der Leitung • Beratung der Bereiche, insbesondere der Fachabteilungen • Beratung der betroffenen Personen (Beschäftigte, Kunden, Geschäftspartner) • Beratung in Zusammenhang mit der Datenschutz-Folgenabschätzung • Beratung der Mitarbeitervertretung
Überwachen	Art. 39 ErwGr 81	• Risikoorientierte Festlegung datenschutzrelevanter Prüfungen • Veranlassen, begleiten oder durchführen von Auditierungen und Prüfungen inkl. erforderlicher Dokumentation • Überwachung der Prüfungen ◦ der datenverarbeitenden Geschäftsprozesse und Regelungen ◦ von IT-Systemen ◦ der datenschutzrelevanten Verträge ◦ der Dokumentation von Verarbeitungsvorgängen inkl. deren Risiko, insbesondere des Verzeichnisses von Verarbeitungstätigkeiten ◦ der Angemessenheit und Einhaltung der technischen und organisatorischen Maßnahmen ◦ von Verfahren, die einer Datenschutz-Folgenabschätzung unterliegen ◦ von Garantien externer Dienstleister (Auftragsverarbeiter) • Überwachung der Bearbeitung von Beschwerden und sicherheitsrelevanten Vorfällen
Berichten und informieren	Art. 39	• Regelmäßige Unterrichtung der Leitung • Zusammenarbeit mit der Aufsichtsbehörde • Regelmäßige Tätigkeitsberichte an den Verantwortlichen

3 TASK AND SERVICES OF THE DATA PROTECTION OFFICER

3.1 Overview of tasks of the Data Protection Officer

Task	Source (GDPR)	Description
Management tasks	Article 24 Article 38(1) Recital 97	• Involvement of the data protection officer by the controller in management systems relevant to data protection • Advice on objectives and tasks, as well as with the updating of the data protection management system • Review of the data protection management system
Advising	Article 38 (1, 4) Article 39 Recital 77, 97 Article 35 Article 88 Recital 155	• Advising the management • Advising the areas, particularly the specialist departments • Advising of data subjects (staff, customers, business partners) • Advising in relation to data protection impact assessment • Advising staff representatives
Monitoring	Article 39 Recital 81	• Risk-based establishing of checks relevant to data protection • Arranging for, collaborating on or carrying out audits and checks, incl. the required documentation • Supervising ◦ the auditing of data processing business procedures and regulations ◦ IT systems of data protection ◦ relevant contracts ◦ The documentation of processing activities, incl. the associated risk, particularly the list of processing activities ◦ The appropriateness of, and compliance with, technical and organisational measures ◦ Processes subject to data protection impact assessment ◦ Guarantees of external service providers (processors) • Monitoring the processing of complaints and security-relevant incidents
Reporting and informing	Article 39	• Regular briefing of management • Co-operation with the supervisory authority • Regular progress reports to the controller

Der Verantwortliche hat Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen einzubinden, damit diese ihre Aufgaben wahrnehmen können. Datenschutzbeauftragte erfüllen ihre Aufgaben unter Berücksichtigung des Risikos für betroffene Personen.[23]

3.2 Managementaufgaben

Datenschutz ist eine Managementaufgabe der Leitung. Datenschutzbeauftragte unterstützen und beraten hierzu. Idealerweise werden die Anforderungen aufgrund der DS-GVO in Managementsysteme des Unternehmens oder der Behörde mit eingebunden. Verantwortliche binden die Datenschutzbeauftragten in datenschutzrelevante Managementsysteme und -prozesse mit ein.

Datenschutzbeauftragte beraten zu den Zielen und Aufgaben sowie bei der Fortschreibung des Datenschutzmanagementsystems. Sie überprüfen in einem Review, ob im Managementsystem alle datenschutzrelevanten Anforderungen berücksichtigt sind.

3.3 Beraten

Datenschutzbeauftragte beraten die Leitung, alle Fachbereiche der Verantwortlichen, sowie betroffene Personen anlassbezogen bei allen Fragen zum Datenschutz, bei der Ausgestaltung von Maßnahmen zum Datenschutz und auf Anfrage bei der Datenschutz-Folgenabschätzung.

3.3.1 Beratungsmaßstab

Datenschutzbeauftragte beraten zur Einhaltung des Datenschutzes mit folgenden Zielen:

- Schutz des Persönlichkeitsrechts der betroffenen Personen
- Gesetzeskonforme Verarbeitung des Verantwortlichen

[23] Art. 39 DS-GVO Abs. 2

The controller shall ensure that data protection officers are involved, properly and in a timely manner, in all issues which relate to the protection of personal data, to enable them to undertake their tasks. Data protection officers fulfil their tasks taking into account the risk for data subjects.[23]

3.2 Management tasks

Data protection is a management task of the management. Data protection officers support and advise, in this respect. Ideally, the requirements are co-integrated into management systems of the company or the public authority based on the GDPR. Controllers integrate the data protection officers into management systems and processes relevant to data protection.

Data protection officers advise on objectives and tasks, as well as with the updating of the data protection management system. They check, in a review, whether all the requirements relevant to data protection have been taken into consideration in the management system.

3.3 Advising

Data protection officers advise the management, all specialist departments of the controller and also, if relevant, data subjects on all matters pertaining to data protection, designing of data protection measures and data protection impact assessment.

3.3.1 Advisory standards

Data protection officers advise on compliance with data protection regulations with the following aims:

- Protection of personal rights of data subjects
- Processing by the controller in conformity with applicable law

[23] Article 39 (2) GDPR

Neben diesen Zielen sind auch die Wirksamkeit, Wirtschaftlichkeit, Praktikabilität, Angemessenheit sowie Akzeptanz der Maßnahmen zu berücksichtigen. Ziel der Beratung ist auch, mit einem hohen Datenschutzniveau zu einem Wettbewerbsvorteil beizutragen.

3.3.2 Beratung der Leitung

Datenschutzbeauftragte beraten die Leitung in allen Angelegenheiten, die den Datenschutz betreffen. Sie geben Hinweise auf die notwendige Festlegung der Verarbeitungszwecke, auf Benachrichtigungspflichten, zu Pflichten zur Datenschutz-Folgenabschätzung, über Meldepflichten, sowie auf die Rechtskonformität geplanter Verfahren personenbezogener Datenverarbeitung. Bei der Festlegung der technischen oder organisatorischen Schutzmaßnahmen wirken sie im Rahmen einer Angemessenheitsabwägung mit der Leitung auf die datenschutzfreundlichste Alternative hin. Datenschutzbeauftragte können auf Wunsch der Leitung u. a. beim Aufbau einer Datenschutzorganisation zusätzliche Aufgaben übernehmen, in dem sie z. B. Vorlagen für Datenschutzrichtlinien zur Verfügung stellen.

3.3.3 Beratung der Bereiche, insbesondere Fachabteilungen

Datenschutzbeauftragte beraten alle relevanten Bereiche des Verantwortlichen, der personenbezogene Daten verarbeitet. Sie beraten insbesondere auf Anforderung des Verantwortlichen hinsichtlich der rechtlichen Voraussetzungen, bei der Planung und Durchführung der technischen und organisatorischen Maßnahmen zum Datenschutz und bei der Gestaltung von datenverarbeitenden Prozessen und Verfahren unter Berücksichtigung von Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen. Datenschutzbeauftragte können bei der Erstellung von Datenschutzkonzepten für Verarbeitungstätigkeiten mitwirken. Sie können Muster zur Umsetzung, z. B. Handlungs- oder Arbeitsanweisungen, Informationspflichten oder Einwilligungserklärungen zu Verfügung stellen.

In addition to these aims, the effectiveness, cost-efficiency, practicability, appropriateness and acceptability of the measures must be taken into account. The aim of the advice is also to contribute to a competitive advantage through a high standard of data protection.

3.3.2 Advising the management

Data protection officers advise the management on all matters pertaining to data protection. They give advice on the necessary determination of processing aims, duty of notification, duty to carry out data protection impact assessment, registration duty, and on the legal conformity of planned personal data processing procedures. In determining technical or organisational protective measures, they work with management within the framework of an evaluation of appropriateness to obtain the most data protection-friendly alternative.

Data protection officers may, if required by the management, take on, inter alia, additional tasks when setting up a data protection organisation, involving, for example, providing templates for data protection guidelines.

3.3.3 Advising the divisions, particularly the specialist departments

Data protection officers advise on all relevant areas of the controller who processes personal data. In particular, at the controller's request, they advise on the legal requirements and on the planning and implementation of technical and organisational data protection measures, the design of data processing procedures, and processes taking into account data protection by design and data protection-friendly default settings. Data protection officers may collaborate in creating data protection concepts for processing activities. They may provide templates for implementation, e.g. operating procedures or job instructions, information reporting obligations or declarations of consent.

3.3.4 Beratung bei Datenschutz-Folgenabschätzung

Datenschutzbeauftragte beraten auf Anfrage die Bereiche und die Leitung bei der Durchführung der Datenschutz-Folgenabschätzung. Sie geben allgemeine Hinweise für die Durchführung von Datenschutz-Folgenabschätzungen und geben Hinweise für die Beurteilungen.

3.3.5 Beratung der betroffenen Person

Wenden sich betroffene Personen an Datenschutzbeauftragte, beraten diese umfassend und vertraulich. Sie unterstützen den Verantwortlichen dabei, den betroffenen Personen über die Verarbeitungen Auskunft zu erteilen. Sie beraten die betroffenen Personen über deren Rechte und die Möglichkeiten, diese wahrzunehmen ohne die Identität der betroffenen Person zu offenbaren.

3.3.6 Beratung der Mitarbeitervertretung

Datenschutzbeauftragte können auf Anforderung die Mitarbeitervertretung bei bestehenden und geplanten Verarbeitungen von personenbezogenen Daten im Beschäftigungskontext[24] beraten, um die schutzwürdigen Interessen der Beschäftigten sicherzustellen.

3.4 Überwachen

Datenschutzbeauftragte überwachen Geschäftsprozesse, Systeme und Organisationsstrukturen und die damit verbundenen technischen und organisatorischen Maßnahmen auf die Einhaltung datenschutzrechtlicher Vorgaben. Diese ergeben sich bspw. aus gesetzlichen Anforderungen, genehmigten Verhaltensregelungen,[25] aus Vorgaben eines (genehmigten) Zertifizierungsverfahrens oder aus unternehmensinternen Datenschutzvorschriften. Die Prüfungen haben sich am aktuellen Stand der Technik zu orientieren.

[24] Art. 88 mit ErwGr 155 DS-GVO, [25] Art. 40 DS-GVO

3.3.4 Advice with assessing the impact of data protection

Upon request, data protection officers advise the divisions and the management when carrying out a data protection impact assessment. They give general indications for carrying out data protection impact assessment and provide information in regard to the assessments.

3.3.5 Advising data subjects

If data protection officers are addressed by data subjects, they advise them fully and confidentially. They support the processor in providing the data subject with information on processing. They advise data subjects on their rights and their options of exercising these without disclosing the identity of the data subject.

3.3.6 Advising staff representatives

Data protection officers may, upon request, advise the staff representatives on existing and planned processing of personal data in the context of employment[24] in order to safeguard the legitimate interests of staff.

3.4 Monitoring

Data protection officers monitor business processes, systems and organisational structures and the associated technical and organisational measures for compliance with data protection requirements. These result, for example, from legal requirements, approved codes of conduct,[25] from requirements for an (approved) certification procedure, or from internal business data protection guidelines. The checks must be based on the current technical state of the art.

[24] Article 88 with Recital 155 GDPR, [25] Article 40 GDPR

Datenschutzbeauftragte erstellen ein Prüfkonzept, welches Umfang, Inhalte, Prüfzyklen und Schwerpunkte definiert. Dieses unterliegt der Weisungsfreiheit der Datenschutzbeauftragten und orientiert sich an möglichen Risiken für betroffene Personen. Die Prüfungsergebnisse werden strukturiert dokumentiert und der Leitung des Verantwortlichen berichtet. Hierbei ist auf festgestellte Risiken gesondert hinzuweisen.

3.4.1 Prüfmaßstäbe

Als Prüfmaßstab sind heranzuziehen:

- die Einhaltung der Rechtskonformität:
  - anzuwendende Gesetze
  - anzuwendende Verordnungen
  - Gerichtsurteile
  - Übergreifende Kollektivvereinbarungen (bspw. Tarifvereinbarungen)
- die IT-Sicherheitsgrundsätze und der Informationssicherheitsstandard, die sich am „Stand der Technik“ orientieren:
  - Vertraulichkeit, Integrität, Verfügbarkeit, Belastbarkeit
  - Vorgaben aus Informationssicherheitsstandards wie die ISO/IEC 27000-Reihe und Regelungen des BSI IT-Grundschutz,
- Anwendungen der Grundsätze „Datenschutz durch Technikgestaltung“ und „datenschutzfreundliche Voreinstellungen“.
- Anerkannte branchenspezifischen Vorgaben:
  - durch Verbände oder durch andere Vereinigungen erarbeitete Verhaltensregelungen, die der DS-GVO entsprechen und von Aufsichtsbehörden anerkannt sind
- individuelle vertragliche Vereinbarungen mit Partnern in Geschäftsbeziehungen, inkl. der Formulierung von Einwilligungserklärungen u.a.
  betriebsinterne Regelungen:
  - Unternehmensrichtlinien und Anweisungen (ggf. auch als Grundlage einer Zertifizierung)
  - Betriebs- bzw. Dienstvereinbarungen (Kollektivvereinbarungen[26])

[26] Art. 88 DS-GVO i. V. m. ErwGr. 155

Data protection officers develop an auditing concept which defines the scope, contents, audit cycles and key areas. This is subject to the data protection officer's authority to act autonomously and is based on potential risks for data subjects. The audit results are documented in a structured way and are reported to the controller management. Any potential risks identified should be brought to attention separately.

3.4.1 Auditing standards

The following shall be referred to as auditing standards:

- Conformity to legal requirements:
  - Applicable laws
  - Applicable regulations
  - Court decisions
  - Overall collective agreements (such as wage agreements)
- The basic IT security principles and the information security standard which are based on the technical “state of the art”:
  - Confidentiality, integrity, availability, resilience
  - Requirements of information security standards such as the ISO/IEC 27000 series and regulations of the basic BSI-IT principles,
- Application of the basic principles of “Data protection by design and by default”.
- Recognised domain-specific requirements:
  - Codes of conduct, developed by associations or other organisations, which comply with the GDPR and are recognised by supervisory authorities
- Individual contractual agreements with partners in business relations, including the formulation of declarations of consent, among others
- In-house regulations:
  - Corporate guidelines and instructions (possibly also as the basis for certification)
  - Corporate and/or employment contracts (collective bargaining agreements[26])

[26] Article 88 GDPR in conjunction with Recital 155

3.4.2 Prüfmethoden

Vor der Durchführung einer Prüf-und Kontrollaufgabe definieren Datenschutzbeauftragte das zu prüfende Projekt / den Prüfgegenstand. Sie bestimmen im Rahmen ihrer Weisungsfreiheit die notwendigen Prüfverfahren, wie bspw.:

- rechtliche Prüfung organisatorischer Vorgaben, Dokumente und Verträge
- Begehung von Örtlichkeiten
- Befragung verantwortlicher und ausführender Personen
- Stichprobenüberprüfung von Dokumenten und Daten
- automatisierte Testverfahren
- Auswertung von Aufzeichnungen von beispielsweise Log-Dateien, Protokollen, Logbücher

Das Prüfungsergebnis wird in einem Prüfbericht dokumentiert und an den Verantwortlichen kommuniziert

3.4.3 Überprüfung vor Einführung oder Änderung einer Verarbeitung

Der Verantwortliche bindet Datenschutzbeauftragte vor Einführung und Änderung einer Verarbeitung ordnungsgemäß und frühzeitig (z. B. bei Lastenheft, Ausschreibung) ein.[27] Datenschutzbeauftragte beraten im Rahmen der Datenschutz-Folgenabschätzung den Verantwortlichen[28] und prüfen die Einhaltung der anzuwendenden Datenschutzvorschriften.
Ist eine Datenschutz-Folgenabschätzung durchzuführen, wird diese maßgeblich durch die Datenschutzbeauftragten begleitet.[29]

3.4.4 Veranlassung und Begleitung von Prüfungen und Auditierungen

In Abstimmung mit dem Verantwortlichen begleiten Datenschutzbeauftragte die Durchführung von Auditierungen. Datenschutzbeauftragte formulieren Prüfgegenstände und bewerten Ergebnisse. Datenschutzbeauftragte können Korrekturmaßnahmen bei Abweichungen empfehlen. Sie können eigenverantwortlich Überprüfungen durchführen.

[27] Art. 38 Abs. 1 DS-GVO, [28] Art. 39 Abs. 1 lit. c. DS-GVO, [29] Art. 35 Abs. 2 DS-GVO,

3.4.2 Auditing methods

Before conducting an audit and monitoring task, data protection officers define the project or object to be audited or monitored. They determine the necessary auditing process in the context of their authority to act autonomously, such as:

- Legal review of organisational requirements, documents and contracts
- Site visits
- Questioning of responsible and implementing persons
- Random auditing of documents and data
- Automated auditing procedures
- Evaluation of records such as log files, reports, logbooks

The audit result must be documented in an audit report and communicated to the controller.

3.4.3 Audit prior to introduction or amendment of processing

The controller shall involve data protection officers properly in a timely manner prior to the introduction or alteration of processing (e.g. in the case of contract specifications, calls for tenders).[27] Data protection officers shall advise the controller[28] in the context of the data protection impact assessment and monitor compliance with the applicable data protection regulations.
If a data protection impact assessment is to be conducted, this shall be overseen to a significant extent by the data protection officers.[29]

3.4.4 Arranging for and accompanying checks and audits

In liaison with the controller, data protection officers oversee the implementation of audits. Data protection officers formulate auditing objects and assess the results. Data protection officers may recommend corrective action in the event of deviations. They may carry out checks on their own responsibility.

[27] Article 38(1) GDPR, [28] Article 39(1)(c) GDPR, [29] Article 35(2) GDPR,

3.5 Berichten und Informieren

Datenschutzbeauftragte informieren und berichten[30] gegenüber internen Stellen regelmäßig oder anlassbezogen. Empfänger ist insbesondere die Leitung. Darüber hinaus können anlassbezogen weitere Stellen wie bspw. Aufsichtsbehörden, betroffene Personen oder die Mitarbeitervertretung zu informieren sein.

3.5.1 Regelmäßige Unterrichtung der Leitung

Die Leitung ist als Verantwortlicher für den Datenschutz erster Empfänger von Berichten und Informationen der Datenschutzbeauftragten. Diese unterrichten die Leitung über

- Datenschutzsituationen an verarbeitenden Stellen im Allgemeinen
- Verstöße gegen gesetzliche, vertragliche und interne Vorschriften
- Umsetzungshindernisse oder Bearbeitungsrisiken
- Optimierungspotenziale
- Statusberichte zur Aktivitäts- und Maßnahmenplanung
- durchgeführte und geplante Tätigkeiten als Datenschutzbeauftragte
- Änderungen rechtlicher oder technischer Rahmenbedingungen

Darüber hinaus können Berichtslinien in der internen Datenschutzorganisation und mögliche Datenschutzkoordinatoren aus den Bereichen IT, HR etc. definiert werden. Unabhängig von beschriebenen Kommunikationspflichten sollten Datenschutzbeauftragte durch einen regelmäßigen Tätigkeitsbericht gegenüber der Leitung über den Stand zum Datenschutz berichten. Zu empfehlen ist ein jährlicher Bericht, wenn nicht Anforderungen des Verantwortlichen ein anderes Berichtsintervall angemessen erscheinen lassen.

3.5.2 Kommunikation mit der Datenschutzaufsichtsbehörde

Die Leitung ist verantwortlicher Ansprechpartner der Aufsichtsbehörde. Auf Verlangen der Leitung oder der Aufsichtsbehörde unterstützen Datenschutzbeauftragte den Verantwortlichen bei der Kommunikation mit der Aufsichtsbehörde.

[30] Art. 38 Abs. 3 Satz 3 DS-GVO

3.5 Reporting and informing

Data protection officers inform and report[30] to internal bodies regularly or with specific reason. The recipient in particular is the management. Furthermore, additional bodies such as supervisory authorities, data subjects or staff representatives can be notified when needed.

3.5.1 Regular reporting to the management

Management, as the controller for data protection, is the primary recipient of reports and information from data protection officers. The latter notify management about

- the data protection situation at processing bodies in general
- Infringements against legal, contractual and internal provisions
- Obstacles to implementation or handling risks
- Potential for optimisation
- Status reports for planning activities and measures
- Implemented and scheduled action as data protection officer
- Amendments to legal or technical framework conditions

Furthermore, reporting lines within the internal data protection organisation and potential data protection coordinators from the areas of IT, HR, etc. can be defined. Irrespective of the communication requirements described, data protection officers should report to the management on the data protection status through a regular progress report. An annual report is recommended, unless the requirements of the controller make a different reporting interval appropriate.

3.5.2 Communication with the data protection supervisory authority

The management is the contact responsible to the supervisory authority. At the request of the management or the supervisory authority, data protection officers assist the controllers in communicating with the supervisory authority.

[30] Article 38(3) sent. 3 GDPR

Darüber hinaus können Datenschutzbeauftragte nach eigenem Ermessen ihr Recht auf Zusammenarbeit[31] mit der Aufsichtsbehörde in Anspruch nehmen

- bei unlösbaren Konflikten um die Rechtmäßigkeit von Verfahren und Maßnahmen zwischen Verantwortlichem und Datenschutzbeauftragten
- wenn Zweifelsfälle bestehen
- sowie bei Konflikten um die Unabhängigkeit der Datenschutzbeauftragten

3.5.3 Umfang und Grenzen

Die Verschwiegenheit und Weisungsfreiheit entbinden Datenschutzbeauftragte nicht von ihren Informations- und Berichtspflichten. Die gesetzliche Vertraulichkeitsverpflichtung (z.B. gegenüber betroffenen Personen) kann diese Berichtspflicht begrenzen. Aus diesem Grund sollten Berichte und Informationen sachbezogen, ohne Nennung von betroffenen Personen erfolgen.

3.6 Schulungs- und Sensibilisierungsaufgaben

Die Schulung und Sensibilisierung[32] der Leitung und der Mitarbeiter ist eine grundlegende Voraussetzung für ein funktionierendes Datenschutzmanagementsystem. Datenschutzbeauftragte legen Inhalte und Umfang unter Berücksichtigung des Risikos für den Betroffenen in Abstimmung mit der Leitung fest.

Verantwortliche können Aufgaben in diesem Bereich delegieren. Datenschutzbeauftragte müssen Qualität und Umsetzung der Maßnahmen überwachen; sie können Schulungsaufgaben auch selbst übernehmen.

Schulungsinhalte und Umfang sind grundsätzlich nach Art der Verarbeitung und entsprechend der Datenschutzrisiken zu gestalten. Sie sind zielgruppenspezifisch und handlungsorientiert durchzuführen. Typische Zielgruppen sind neben Personen, die personenbezogene Daten verarbeiten, auch Führungskräfte und die Mitarbeitervertretung.

[31] Art. 39 Abs.1 lit. d DS-GVO, [32] Art. 39 Abs. 1 lit. b DS-GVO

Furthermore, data protection officers can take advantage at their own discretion of their right to co-operate[31] with the supervisory authority

- in the case of unresolvable conflicts relating to the lawfulness of processes and measures between the controller and the data protection officer,
- in cases of doubt,
- and in the case of conflicts relating to the independence of data protection officers.

3.5.3 Scope and limitations

The confidentiality and authority to act autonomously do not release data protection officers from their obligations to inform and report. The legal duty to confidentiality (such as towards data subjects) can limit this duty to report. For this reason, reports and information shall be factual without naming the data subject.

3.6 Training and awareness-raising tasks

The training and awareness-raising[32] of management and staff is a basic condition for a functioning data protection management system. Data protection officers determine the content and scope in consultation with the management, taking into account the risk for the data subject.

Controllers may delegate tasks in this area. Data protection offers need to monitor quality and implement the measures. They may also personally take on training tasks.

Training content and scope shall fundamentally be designed according to the type of processing and the data protection risks. They shall be carried out specifically for the target group and be activity-oriented. Typical target groups, besides persons who process personal data, are also managerial staff and staff representatives.

[31] Art. 39(1)(d) GDPR, [32] Article 39(1)(b) GDPR

4 ANFORDERUNG AN DIE BERUFSAUSÜBUNG

4.1 Haltung zur Berufsausübung

Datenschutzbeauftragte verstehen sich als Interessensvertreter sowohl der betroffenen Personen als auch der Verantwortlichen. Sie agieren daher in einem Spannungsfeld unterschiedlicher Positionen, in dem sie konstruktive Lösungen entwickeln müssen.

Datenschutzbeauftragte argumentieren auf gängigen Rechtsauffassungen, begründen nachvollziehbar und machen deutlich, wenn sie persönliche Ansichten vertreten. Datenschutzbeauftragte bemühen sich um neutrale und objektive Bewertungen von Sachverhalten.

Soweit Datenschutzbeauftragte einen Interessenskonflikt im Sinne von Kap. 3.5.4 erkennen, sollten diese den Sachverhalt den Verantwortlichen darlegen und sich ggf. auch mit der zuständigen Aufsichtsbehörde darüber abstimmen.

Datenschutzbeauftragte gewährleisten eine hohe Qualität ihrer Tätigkeit. Sie holen sich in Zweifelsfällen fachspezifische Unterstützung. Datenschutzbeauftragte sind in Bereichen tätig, für die sie ausreichendes Fachwissen besitzen. Bei neuen Anforderungen qualifizieren sie sich zeitnah. Sie setzen einen besonderen Fokus auf die Verarbeitung mit höheren Risiken und achten darauf, dass ihre Qualifikationen diesen Risiken angemessen sind.

4.2 Ansprechbarkeit

Datenschutzbeauftragte stellen sicher, dass sie für betroffene Personen in angemessener Weise und in angemessenem Umfang ansprechbar sind.[33] Dazu gehört es auch, dass Datenschutzbeauftragte in der Amtssprache des Landes des Verantwortlichen (z. B. in Deutschland: deutsch) sicher kommunizieren.[34] Für die Kommunikation mit anderssprachigen Stellen oder betroffenen Personen stellt der Verantwortliche gegebenenfalls Unterstützung für die Übersetzung zur Verfügung.

[33] WP 243, 2.5 Veröffentlichung und Mitteilung der Kontaktdaten des DSB,

[34] WP 243, 2.3 Leichte Erreichbarkeit von jeder Niederlassung

4 PROFESSIONAL PRACTICE REQUIREMENTS

4.1 Attitude towards professional practice

Data protection officers regard themselves as representatives of the interests not only of data subjects but also of controllers. They therefore act in a tension field of different positions in which they are called on to develop constructive solutions.

Data protection officers put forward argumentations about common interpretations of law, provide justifications in a comprehensible way and make it clear when they are putting forward personal views. Data protection officers endeavour to conduct a neutral and objective evaluation of the facts.

Should data protection officers identify a conflict of interests pursuant to Chapter 3.5.4, they should present the facts to the controllers and, if necessary, also come to an agreement with the responsible supervisory authority.

Data protection officers guarantee a high standard of quality in their work. They consult specialist support in cases of doubt. Data protection officers work in areas for which they have sufficient expertise. In the case of new requirements, they acquire the necessary qualifications in a timely manner. They place a special focus on the processing that involves greater risks, and take care to ensure that their qualifications are appropriate for such risks.

4.2 Responsiveness

Data protection officers ensure that they are available to respond to data subjects in an appropriate manner and scope.[33] The latter also includes data protection offers communicating with confidence in the official languages of the controller's country (e.g. German in Germany).[34] In regard to communication with offices or data subjects speaking other languages, the controller shall, if necessary, provide support for the translation.

[33] WP 243, 2.5 Publication and notification of the contact data of the data protection officer,

[34] WP 243, 2.3 Easy accessibility of every branch office

4.3 Überprüfbarkeit

Datenschutzbeauftragte dokumentieren ihr Handeln. Dokumentationen sind zutreffend und vollständig. Diese Dokumentationen können auch als Nachweise im Rahmen des Datenschutzmanagementsystems dienen.

4.4 Verschwiegenheit und Vertraulichkeit

Datenschutzbeauftragte sind zu strikter Einhaltung der Verschwiegenheit verpflichtet.[35] Diese Pflichten beziehen sich auf alles, was ihnen in Ausübung ihres Berufes bekannt wird. Dies gilt nicht für Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung unterliegen.

Datenschutzbeauftragte behandeln die Einzelheiten von Beschwerden, Datenschutzverletzungen oder die Identität von Informanten vertraulich. Sie halten die Identität der Beschwerdeführer geheim, sofern diese nicht ausdrücklich mit der Offenbarung ihrer Identität einverstanden sind.

Darüber hinaus sind sie zur Verschwiegenheit über alle personenbezogene Informationen sowie Amts-, Betriebs- und Geschäftsgeheimnisse, die sie während ihrer Tätigkeit Kenntnis erlangen, verpflichtet. Dies gilt auch über das Ende ihrer Tätigkeit als Datenschutzbeauftragte hinaus.

Beschäftigen Datenschutzbeauftragte oder die für die Verarbeitung Verantwortlichen Mitarbeiter mit Aufgaben in der Datenschutzorganisation (bspw. Datenschutzkoordinatoren), so sind diese zur gleichen Verschwiegenheit zu verpflichten. Gegenüber den Datenschutzaufsichtsbehörden bestehen diese Vertraulichkeitsverpflichtungen nur insoweit als sie der gebotenen Loyalität zum Verantwortlichen und der betroffenen Personen entsprechen.

[35] Art. 38 Abs. 5 DS-GVO

4.3 Verifiability

Data protection officers document their actions. Documentation provides an accurate picture and is complete. This documentation can also serve as verification in the context of the data protection management system.

4.4 Discretion and confidentiality

Data protection officers are duty bound to maintain strict confidentiality.[35] This duty applies to all information to which they are privy while exercising their office. This does not apply to facts that are evident or are not subject to confidentiality as a result of their level of significance.

Data protection officers treat the details of complaints, data protection violations or the identity of informants confidentially. They keep the identity of complainants confidential unless complainants expressly agree to the disclosure of their identity.

Furthermore, they are duty bound to keep confidential all personal information and all official, corporate and trade secrets to which they are privy during the course of their work. This also applies over and beyond the termination of their office as data protection officers.

Should data protection officers, or staff responsible for processing, deal with tasks in data protection organisation (such as data protection coordinators), then these persons shall be sworn to secrecy. Such confidentiality obligations shall only exist vis-à-vis data protection authorities to the extent that they are in line with the necessary loyalty to the controller and the data subjects.

[35] Article 38(5) GDPR

4.5 Qualitätssicherung der Aufgabenerfüllung

Zur Gewährleistung der zuverlässigen Berufsausübung sind geeignete Maßnahmen zur Qualitätskontrolle zu ergreifen.

4.5.1 Eigenkontrolle

Die Qualitätssicherung einer vollständigen und korrekten Aufgabenerfüllung sollen durch Eigenkontrolle und Reflektion gewährleistet werden. Als weitere Maßnahme ist ein regelmäßiger Austausch und Möglichkeiten zur Nutzung externer Fachkunde und von Netzwerken zu sehen. Dazu zählen auch Fort- und Weiterbildungen, die bspw. mit Prüfungen abschließen. Weitere Möglichkeiten ergeben sich aus Auditierungen sowie Beratungen mit Aufsichtsbehörden, um Ergebnisse und Einschätzungen zu optimieren.

4.5.2 Kontrolle durch den Berufsverband

Der Berufsverband der Datenschutzbeauftragten Deutschlands (BvD) e.V. stellt im Rahmen des Verfahrens zur Selbstverpflichtung geeignete Kontrollmaßnahmen zur Qualitätssicherung bereit. Die auf dieses Berufsbild verpflichteten Datenschutzbeauftragten müssen an diesen Kontrollmaßnahmen teilnehmen. Andernfalls wird das Siegel zur Selbstverpflichtung durch den Berufsverband entzogen. Das Verfahren ist transparent und in den Dokumenten zur Selbstverpflichtung (www.bvdnet.de) beschrieben. Das Siegel ist personalisiert und beim Berufsverband überprüfbar.

4.6 Benennung zum Datenschutzbeauftragten

4.6.1 Voraussetzung der Benennung

Voraussetzungen zu einer ordnungsgemäßen Benennung zum Datenschutzbeauftragten ergeben sich aus

- Persönlicher und fachlicher Voraussetzung (vgl. Kapitel 1)
- der Ausübung von Pflichten und Aufgaben in vollständiger Unabhängigkeit und ohne Interessenkonflikt[36]

[36] Art. 38 Abs. 6 mit ErwGr 97 DS-GVO

4.5 Quality assurance regarding the task completion

Suitable quality control measures shall be put in place to guarantee the reliable exercise of their office.

4.5.1 Self-monitoring

The quality assurance of full and correct completion of tasks should be ensured through self-monitoring and reflection. A further measure shall be a regular exchange and opportunities to use external specialist knowledge and networks. These also include further and advanced training which may, for example, be concluded by taking the respective examinations. Additional opportunities arise from audits and consultations with supervisory authorities in order to optimise results and appraisals.

4.5.2 Monitoring through professional association

The Association of Data Protection Officers of Germany (BvD) e.V. provides suitable control measures for quality assurance within the context of a voluntary commitment process. The data protection officers committed to this occupation must take part in these control measures. Otherwise, the voluntary commitment seal will be withdrawn by the professional association. This process is transparent and is described in the voluntary commitment documents (www.bvdnet.de). The seal is personalised and verifiable by the professional association.

4.6 Designation as data protection officer

4.6.1 Designation requirements

The conditions for due designation as a data protection officer result from

- Personal and professional qualifications (cf. Chapter 1)
- Exercising obligations and tasks completely independently and without any conflict of interest[36]

[36] Article 38(6) with Recital 97 GDPR

Zum Beauftragten für den Datenschutz können auch Personen bzw. externe Dienstleister auf Grundlage eines Dienstleistungsvertrages benannt werden.[37]

4.6.2 Stellung der Datenschutzbeauftragten

Auf Grund des Berichts- und Vortragsrechts gegenüber der höchsten Leitungsebene.[38] ist es erforderlich, den DSB direkt unterhalb der Leitung als Stabsstelle in die Organisation einzubinden. Durch geeignete organisatorische Maßnahmen ist die leichte Erreichbarkeit von jeder Niederlassung aus[39] sicherzustellen.

Den Datenschutzbeauftragten sind die zur Erfüllung ihrer Aufgaben erforderlichen räumlichen, technischen und organisatorischen Zugangsrechte einzuräumen. Datenschutzbeauftragte werden zu regelmäßigen Sitzungen des leitenden Managements eingeladen, damit diese in adäquater Weise als Ratgeber fungieren können. Bei einer Verletzung datenschutzrechtlicher Bestimmungen oder einem sonstigen Vorfall sind Datenschutzbeauftragte unverzüglich hinzuzuziehen.[40]

4.6.3 Form und Verfahren der Benennung

Datenschutzbeauftragte sind durch den Verantwortlichen, jeweils von der Leitung, schriftlich zu benennen. Datenschutzbeauftragte können ihre Aufgaben für mehrere miteinander verbundene und nicht verbundene Verantwortliche wahrnehmen, solange dies nicht ihre Unabhängigkeit gefährdet. Es können ein oder mehrere Stellvertreter benannt werden. Die Benennung ist der zuständigen Aufsichtsbehörde mitzuteilen und die Kontaktdaten sind zu veröffentlichen[41].

4.6.4 Dauer, Laufzeiten der Benennung

Die Benennung zum Datenschutzbeauftragten kann zeitlich befristet werden. Langfristige Benennungen werden empfohlen. Die Laufzeit für die Erstbenennung sollte fünf Jahre, die für Wiederbenennung drei Jahre nicht unterschreiten.

[37] Art. 37 Abs. 6 DS-GVO, WP 243revo1, 2.5. Im Rahmen eines Dienstleistungsvertrags beschäftigte DSB,
[38] Art. 38 Abs. 3 Satz 3 DS-GVO, [39] WP 243, 2.3 Leichte Erreichbarkeit von jeder Niederlassung aus,
[40] WP 243, 3.1 Einbindung des DSB,
[41] Art. 37 Abs. 7 DS-GVO; WP 243, 2.5 Veröffentlichung und Mitteilung der Kontaktdaten des DSB

Individuals or external service providers may also be designated data protection officers based on a service contract.[37]

4.6.2 Position of Data Protection Officers

Based on the right of reporting and presentation vis-à-vis the highest level of management,[38] it is necessary to integrate the data protection officer directly under the management as a staff position in the organisation. Easy accessibility from every branch office[39] is to be ensured through suitable organisational measures.

The data protection officers are to be granted the necessary spatial, technical and organisational access rights to perform their tasks. Data protection officers are invited to regular meetings of the executive management, so that the latter can act as advisers in an adequate manner. In the event of an infringement of data protection provisions or any other incident, data protection officers are to be called upon immediately.[40]

4.6.3 Designation form and procedure

Data protection officers shall be designated by the controller, from management, in writing. Data protection officers can perform their tasks for several affiliated or non-affiliated controllers, provided this does not compromise their independence. One or more representatives can be designated. The supervisory authority shall be notified of the designation, and the contact data is to be made known[41].

4.6.4 Duration, term of designation

The designation as data protection officer can be for a limited term. Long-term designations are recommended. The period of initial designation should be five years, and the period for redesignation should not be less than three years.

[37] Art. 37(6) GDPR, WP 243revo1, 2.5. Data protection officers employed under a service contract,
[38] Article 38(3) sent. 3 GDPR, [39] WP 243, 2.3 Easy accessibility from every branch office,
[40] WP 243, 3.1 Involvement of the Data Protection Officer
[41] Art. 37(7) GDPR; WP 243, 2.5 Publication and notification of the contact data of the data protection officer

4.6.5 Unabhängigkeit der Berufsausübung

Datenschutzbeauftragte müssen ihre Aufgaben in vollständiger Unabhängigkeit und Weisungsfreiheit ausüben können[42]. Unabhängig sind sie, wenn sie frei von fachlichen und zeitlichen Interessenkonflikten sind, ihre Datenschutztätigkeit weisungsfrei und eigenverantwortlich gestalten können und über ausreichende Ressourcen verfügen.

Interessenkonflikte liegen vor, wenn die Tätigkeiten der Datenschutzbeauftragten mit anderen Aufgaben z.B. in einem zeitlichen, fachlichen oder weisungsgebundenen Widerspruch stehen. Dies ist auch dann der Fall, wenn Datenschutzbeauftragte konkurrierende Aufgaben wahrnehmen, bspw. auch bei verbundenen Unternehmen.

4.6.6 Erforderliche Ressourcen

Verantwortliche sind verpflichtet, Datenschutzbeauftragten angemessene Ressourcen[43] zur Verfügung zu stellen und nötigen Zugang zu relevanten Informationen zu ermöglichen. Datenschutzbeauftragte schaffen sich räumlich, technisch und organisatorisch die erforderlichen Rahmenbedingungen für Vertraulichkeit und Sicherheit der Arbeitsmaterialien.

4.7 Haftung und Versicherungspflicht

Datenschutzbeauftragte haften nicht für die Datenverarbeitung oder Datenschutzverstöße des Verantwortlichen. Im Rahmen ihrer Stellung können Datenschutzbeauftragte keine Weisungen erteilen und Ursachen nicht selbst abstellen.

Zur Vermeidung eigener Haftung sind Datenschutzbeauftragte verpflichtet, dem Verantwortlichen auf ihnen bekannte Datenschutzverstöße und damit verbundene Melde- und Informationspflichten hinzuweisen. Dieses dokumentieren sie in nachvollziehbarer Weise.

[42] Art. 38 Abs. 6 mit ErwGr 97 DS-GVO,

[43] WP 243, 3.2 erforderliche Ressourcen wie Finanzmittel, Infrastrukturen sowie gegebenenfalls Personal

4.6.5 Independence of professional practice

Data protection officers must be able to perform their tasks completely independent and with the authority to act autonomously[42]. They are independent if they are free from professional and temporal conflicts of interest, can organise their data protection work on their own responsibility and without being bound by instructions, and have sufficient resources available.

Conflicts of interest are present if the activities of data protection officers are incompatible with other tasks due, for example, to temporal, professional or authoritative inconsistency. This is also the case if data protection officers perform competing tasks including, for example, in the case of affiliated companies.

4.6.6 Necessary resources

Controllers are obliged to provide data protection officers with adequate resources[43] and enable the necessary access to relevant information. Data protection officers create the framework conditions required for confidentiality and the security of work materials, in terms of spatial, technical and organisational aspects.

4.7 Liability and obligation to take out insurance

Data protection officers are not liable for the data processing activities or data protection violations of the controller. As part of their position, data protection officers may not issue any instructions, nor are they able to rectify any root causes.

In order to avoid any liability of their own, data protection officers are obliged to point out to the controller any data protection violations of which they are aware and any associated notification and reporting obligations. They shall document the latter in a comprehensible manner.

[42] Article 38(6) with Recital 97 GDPR,

[43] WP 243, 3.2 Necessary resources, such as funding, infrastructures and any staff

Bei der Übernahme zusätzlicher Aufgaben durch den Datenschutzbeauftragten, die insbesondere eine Weisungsbefugnis enthalten, können andere Haftungsbedingungen entstehen. Die Datenschutzbeauftragten sind hier angehalten, Tätigkeit und Empfehlungen genau zu dokumentieren und für eine Freigabe und Übernahme durch die Leitung des Verantwortlichen zu sorgen.

Soweit Datenschutzbeauftragte für durch sie schuldhaft verursachte Personen-, Sach- und Vermögensschäden haften, greifen für interne Datenschutzbeauftragte die durch die arbeitsrechtliche Rechtsprechung ausgeprägten Haftungsbeschränkungen für Angestellte Externe Datenschutzbeauftragte können in Geschäftsbesorgungsverträgen Haftungsbeschränkungen vorsehen.

Externe Datenschutzbeauftragte schließen darüber hinaus eine Berufshaftpflichtversicherung zur Deckung der sich aus ihrer Berufstätigkeit ergebenden Haftungsgefahren für Vermögensschäden ab und halten die Versicherung während der Dauer ihrer Benennung aufrecht.

When any additional tasks are taken on by data protection officers, which in particular include an authority to issue directives, other terms of liability may arise. The data protection officers are, in this case, required to document the activity and recommendations precisely, and ensure that the latter are approved and adopted by the controller's management.

Insofar as data protection officers are liable for injury, damage to property and pecuniary loss that they have culpably caused, internal data protection officers are subject to the labour law jurisdiction-based limitations of liability for employees. External data protection officers may stipulate limitations of liability in contracts of agency.

External data protection officers shall, moreover, conclude professional indemnity insurance to cover the liability risks in regard to pecuniary losses arising from the exercise of their office and maintain the insurance cover for the term of their designation.

4. Ausgabe 2018

Unter Berücksichtigung der

EU-Datenschutzgrundverordnung (DS-GVO)
BDSG-neu,
WP 243 und WP 243rev01

Stand: 14. März 2018

Revision:

Version 03:
2016 unter Berücksichtigung der DSGVO

Version 04:
2017/18 unter Berücksichtigung von

- WP 243, WP243rev01
  Guidelines on Data Protection Officers,
  der Article 29 Data Protection Working Party
- BDSG-n. F.,
- Datenschutzpapiere der DSK
  und des LDA Bayern

Das berufliche Leitbild des Datenschutzbeauftragten ist ein Arbeitsergebnis des Ausschusses Berufsbild mit den ständigen Mitgliedern:
Jörg Becker, Monika Egle, Jürgen Hartz, Sabine Idahl, Dr. Kai-Uwe Loser, Klaus Mönikes, Gerfried Riekewolt, Thomas Spaeing, Sebastian Stieldorf, Barbara Stöferle.

Edition 4/2018

Taking into account the

EU General Data Protection Regulation (GDPR),
Federal Data Protection Act (BDSG) new version
WP 243 and WP 243rev01

Last updated: 14/03/2018

Revision:

Version 03:
2016 into account the GDPR

Version 04:
2017/18 taking into account

- WP 243, WP243rev01
  Guidelines on Data Protection Officers,
  article 29 Data Protection Working Party
- Federal German Data Protection Act (BDSG), new Version
- data protection documents
  of the Data Protection Conference (DSK) and the

The professional code of practice for data protection officers is a result of the work of the Occupational Profile Working Committee with the following permanent members:
Jörg Becker, Monika Egle, Jürgen Hartz, Sabine Idahl, Dr. Kai-Uwe Loser, Klaus Mönikes, Gerfried Riekewolt, Thomas Spaeing, Sebastian Stieldorf, Barbara Stöferle.

Herausgeber | *Publisher*

Berufsverband der
Datenschutzbeauftragten Deutschlands (BvD) e.V.

Budapester Straße 31
10787 Berlin

Tel: +49 30 2636 77 60
Fax: +49 30 2636 77 63

E-Mail: bvd-gs@bvdnet.de
Internet: www.bvdnet.de

BvD e.V.
DATENSCHUTZ GESTALTEN