CPS 100

DATENSCHUTZ

KONFORMITÄTS BEWERTUNGS PROGRAMM

Inhaltsverzeichnis

Vorwort

Vielen Dank für Ihr Interesse am Datenschutz.
Wir legen hiermit ein Konformitätsbewertungsprogramm in Gestalt einer Broschüre vor, die Ihnen den Aufbau von Datenschutzmaßnahmen in einem Unternehmen erleichtern soll. Zum besseren Verständnis möchten wir einige Erklärungen voranstellen.
Konformitätsbewertung ist definiert* als „Darlegung, dass festgelegte Anforderungen bezogen auf ein Produkt, einen Prozess, ein System, eine Person oder eine Stelle erfüllt sind".
Ein Konformitätsbewertungsprogramm stellt demnach einen Rahmen zur Verfügung, um eine Konformitätsbewertung erbringen zu können. Konformitätsbewertungen finden sowohl auf rechtlich ungeregelter Basis statt, als auch auf der Grundlage gesetzlicher Regelungen (so genannter „geregelter Bereich").
Eine nachgewiesene Konformität kann die Grundlage einer Zertifizierung darstellen. Es werden sowohl staatliche als auch privatrechtliche Zertifizierungen angeboten.
Privatrechtliche Zertifizierungen finden dort ihre Berechtigung, wo rechtliche Grundlagen für eine staatliche Zertifizierung entweder nicht vorgesehen sind, oder aber eine staatliche Zertifizierung die wirtschaftlichen Möglichkeiten von zu Zertifizierenden übersteigen würde.
Die EU DSGVO konzentriert sich auf die Zertifizierung von Datenschutz-Produkten und Datenschutz-Dienstleistungen. Hingegen sind Zertifizierungen von Datenschutz-Management-Systemen nicht vorgesehen.
Die Vorgabe einer Struktur für den Aufbau und die Sicherstellung der Durchführung von Datenschutzmaßnahmen sind der staatlichen Zertifizierung entzogen.

* internationale Norm ISO/IEC 17000 „Begriffe und allgemeine Grundlagen"

Diese Begutachtung bleibt damit privaten Auditoren vorbehalten. Diese greifen dabei vorteilhafterweise auf ein bestehendes Konformitätsbewertungsprogramm zurück, um möglichst objektiv und nachvollziehbar den Datenschutz-Status eines Unternehmens beurteilen und dieses Status bestätigen, also auch zertifizieren zu können.
Da Geschäftsführungen für den Datenschutz-Status ihres Unternehmens direkt haften, ist die Vorhaltung einer Dokumentation anzuraten, um Haftung begrenzen oder ausschließen zu können.

CPS© – Certified Privacy Standard

CPS ist im Datenschutz der Oberbegriff für Verfahren, Anweisungen sowie für Konformitätsbewertungsprogramme, welche durch die IITR Cert GmbH erarbeitet und standardisiert werden.

Die Unternehmen IITR Datenschutz GmbH sowie IITR Cert GmbH haben sich entschlossen, nach CPS 300 (Auftragsdatenverarbeitung, Veröffentlichung Januar 2022) nun auch CPS 100 öffentlich zugänglich zu machen.

Derzeit sind folgende **Zertifizierungs**standards verfügbar:

- CPS 100: Zertifizierung des Datenschutz-Status bei mittelständischen Unternehmen
- CPS 300: Zertifizierung von Auftragsverarbeitern nach Art. 28 DSGVO
- CPS 600: Zertifizierung des Datenschutz-Status bei kleinen Unternehmen

Dabei stellt CPS 100 das Konformitätsbewertungsprogramm für den datenschutz-konformen Prozessaufbau bei einem mittelständischen Unternehmen dar. CPS 100 findet seit zwei Jahren Verwendung, unter anderem bei den durch die IITR Datenschutz GmbH betreuten Unternehmen.

Die hier vorgelegte Broschüre umfasst zusätzlich einen **Anwender-Leitfaden**, der zur Implementierung der Datenschutzanforderungen gemäß CPS 100 in einem Unternehmen herangezogen werden kann.

Was noch erwähnt werden muss:

1. Dem **Compliance-Kit 2.0** (Datenschutz Management System der IITR Datenschutz GmbH, www.iitr.de) liegt der hier vorgestellte CPS 100 zugrunde. Darin sind neben vielen sinnvollen Funktionen ca. 100 weitere vorgefertigte Arbeitsbögen enthalten, die den professionellen Umgang mit dem Datenschutz stark vereinfachen.
2. Das **Compliance-Kit 2.0** kann im Falle einer ISO 27701-Zertifizierung als Grundlage herangezogen werden.

Weiterhin werden folgende Prüfstandards verwendet:

- CPS 051: Prüfung von Bewerber-Management
- CPS 061: Prüfung von Videoüberwachungsanlagen
- CPS 071: Prüfung von Heimarbeit und mobilem Arbeiten
- CPS 091: Prüfung der IT-Basics
- CPS 350: Prüfung von Auftragsverarbeitern nach Art. 28 DSGVO
- CPS 501: Prüfung Informationssicherheit bei Dienstleistern für ISO 27001
- CPS 911: Prüfung Personalabteilung allgemein
- CPS 921: Prüfung IT-Abteilung allgemein
- CPS 931: Prüfung Vertrieb und Marketing

privASSIST

Eine Überprüfung aller CPS (Zertifizierungs- als auch Prüf-Standards) kann durch privASSIST durchgeführt werden.

privASSIST ist ein Instrument der IITR Cert GmbH. Es dient der webbasierten Fern-Auditierung von datenschutzrelevanten Vorgängen. Jede dieser Auditierungen umfaßt eine speziell entwickelte Art von

- dokumentierter Befragung, gelegentlich unter
- Hinzuziehung hochzuladender Dokumente,
- rechnergestützte Prüfung u. a. auf Vollständigkeit und Plausibilität
- Vergleichs-Betrachtungen,
- Sichtung und Beurteilung,
- Erstellung eines Audit-Berichts, mit
- Hinweis auf kritische Findings sowie
- Aufzeigen von Optimierungs-Potential

privASSIST findet vor allem Verwendung im Haftungsmanagement der Geschäftsführung, der Ermittlung sowie dem Tracking des eigenen Datenschutz-Status, bei der Erfüllung von Nachweis- und Rechenschaftspflichten, dem Vorgang der Erteilung einer Auftragsverarbeitung sowie zur Vorbereitung von Zertifizierungen.

KONFORMITÄTS-BEWERTUNGSPROGRAMM

CPS 100

(Stand 08.02.2022)

1 Rahmenbedingungen des Konformitätsbewertungsprogramms

1.1 Allgemeines

Die informationelle Selbstbestimmung und der damit einhergehende Umgang mit personenbezogenen Daten durch Organisationen haben in unserer Gesellschaft einen hohen Stellenwert. Um das Vertrauen der Mitarbeiter, der Kunden und der Geschäftspartner aufrechtzuerhalten bzw. zu verbessern müssen Organisationen einen datenschutzkonformen Umgang mit personenbezogenen Daten sicherstellen und nachweisen.

1.2 Ziel

Ziel dieses Konformitätsbewertungsprogramms ist die Überprüfung der von einer Organisation zur Verarbeitung von personenbezogenen Daten implementierten Maßnahmen und Prozesse hinsichtlich ihrer Fähigkeit, die Vorgaben dieses CPS 100 zu erfüllen.

1.3 Nachweis

Der Nachweis zur Umsetzung der Implementierung von Maßnahmen und Prozessen, die eine datenschutzkonforme Verarbeitung ermöglichen, erfolgt durch eine Bewertung der von der Organisation bereitgestellten dokumentierten Informationen. Das vorliegende Konformitätsbewertungsprogramm ist die Grundlage, an der sich die Zertifizierungsstelle bei ihrer Zertifizierungsentscheidung orientiert.

1.4 Grundsätze

Als Basis für die Zertifizierung sind die allgemeinen Grundsätze zur Verarbeitung personenbezogener Daten definiert. Dies sind im Einzelnen

- die Rechtmäßigkeit
- die Zweckbindung
- die Beschränkung
- die Richtigkeit
- die Speicherbegrenzung
- die Integrität und Vertraulichkeit

1.5 Zertifizierung

1.5.1 Grundlage

Die Anforderungen an das Zertifizierungsaudit basieren auf verschiedenen Kriterien. Diese sind immer auf die zu zertifizierende Organisation bezogen und im Einzelnen abhängig von

- der Tätigkeitsbranche
- der Anzahl und Art der Datenverarbeitungstätigkeiten
- der Anzahl der in die Datenverarbeitung involvierten Mitarbeiter
- der Anzahl der relevanten Datenverarbeitungsstandorte
- der Anzahl der eingesetzten Subunternehmer

1.5.2 Bewertung

Die Umsetzungsbewertung der in Ziffer 3 beschriebenen Vorgaben erfolgt im Rahmen einer Einsichtnahme in die von der zu zertifizierenden Organisation eingereichten dokumentierten Informationen. Diese können aus Richtlinien, Prozessanweisungen, Arbeitsanweisungen sowie Nachweisen zur Umsetzung bestehen. Bei nicht eindeutig zu bewertenden Sachverhalten oder widersprüchlichen Angaben

werden im Einzelfall weitere zur Sachverhaltsklärung erforderliche dokumentierte Informationen bei der zu zertifizierenden Organisation angefordert. Die Ermittlung der Konformität erfolgt immer auf Basis einer Stichprobenprüfung. Dabei werden die eingereichten dokumentierten Informationen (Richtlinien, Prozessanweisungen, Arbeitsanweisungen sowie Nachweise zur Umsetzung) hinsichtlich ihrer Plausibilität und Anwendbarkeit beurteilt. Im Einzelfall werden weitere öffentlich zugängliche Informationen und Angaben der obersten Leitung der zu zertifizierenden Organisation berücksichtigt und in die Konformitätsbewertung einbezogen. Dabei wird bewertet, ob die von der zu zertifizierenden Organisation getroffenen Maßnahmen zum Schutz personenbezogener Daten als angemessen und ausreichend eingestuft werden können. Dabei werden die Art der verarbeiteten personenbezogenen Daten, die Standorte der Datenverarbeitungsanlagen, die eingesetzten Dienstleister und die damit einhergehenden Schutzrechte der von der Datenverarbeitung Betroffenen berücksichtigt.

1.5.3 Überwachung

Die Konformitätsüberwachung erfolgt im zweijährlichen Turnus. Hier muss die zu überwachende Organisation alle neuen, geänderten und aus der Verwendung genommenen dokumentierten Informationen zur Konformitätsbewertung einreichen. Zusätzlich muss die Anwendung und Aufrechterhaltung der in Ziffer 3 geforderten Vorgaben durch geeignete dokumentierte Informationen (Richtlinien, Prozessanweisungen, Arbeitsanweisungen, Nachweise zur Umsetzung) nachgewiesen werden. Dies können neben der Einsichtnahme in die eingereichten Informationen auch Gespräche mit den in der Organisation Beschäftigten sein.

1.5.4 Ergebnis

Im Rahmen des Audits werden die von der Organisation bereitgestellten dokumentierten Informationen auf ihre Konformität zu den in Ziffer 3 genannten Bewertungsvorgaben geprüft.

Werden dabei Nichtkonformitäten festgestellt, muss die Organisation Korrekturmaßnahmen definieren und diese innerhalb von 90 Tagen nachweisbar umsetzen. Erst dann kann ein Zertifikat erteilt werden.

2 Gegenstand der Konformitätsbewertung

Gegenstand der Konformitätsbewertung sind die in Ziffer 3 beschriebenen Bewertungsvorgaben. Diese werden regelmäßig im Rahmen der Konformitätsbewertung vom Herausgeber des CPS 100 überprüft und mit den allgemeinen und besonderen Anforderungen an den Schutz personenbezogener Daten überprüft und aktualisiert.
Sollte im Rahmen der regelmäßigen Überprüfung festgestellt werden, dass der CPS 100 nicht mehr dazu geeignet ist, dem Anwender die Grundlage und Umsetzungsbegleitung für einen wirksamen Datenschutz in seiner Organisation zu ermöglichen, wird der CPS 100 umgehend von der für die Konformitätsbewertung verantwortlichen Stelle unter Berücksichtigung der neuen Anforderungen aktualisiert und die Anwender werden informiert. Sollte eine Aktualisierung in der Folge von äußeren Einflüssen nicht möglich sein, so wird die für die Konformitätsbewertung verantwortliche Stelle entsprechende Maßnahmen zur Information der Anwender ergreifen.

3 Detaillierte Bewertungsvorgaben

Ein Zertifikat kann nur erteilt werden, wenn die nachfolgend beschriebenen Rahmenbedingungen von der antragstellenden Organisation eingehalten und nachgewiesen werden.

3.1 Allgemeines

3.1.1 Datenschutz-Vorgaben

Die Organisation muss eine Datenschutz-Richtlinie oder ein Datenschutz-Handbuch wirksam implementieren, das die Anforderungen aus dem Datenschutz an die Organisation angemessen berücksichtigt.

3.1.2 Organisationsstruktur

Die Organisation muss ihre Organisationsstruktur abbilden. Dabei müssen alle datenverarbeitenden Stellen innerhalb der Organisation berücksichtigt und dargestellt werden. Alle Standorte, an denen eine Datenverarbeitung erfolgt, müssen dargestellt werden. Hierbei muss für jeden Standort die organisatorische Eingliederung in die Gesamtorganisation erkennbar sein.

3.1.3 Verarbeitungstätigkeiten

Die Organisation muss eine Übersicht über seine Datenverarbeitungstätigkeiten erstellen. Dabei muss jeder Verarbeitungstätigkeit ein Verantwortlicher zugewiesen sein. Jede Verarbeitungstätigkeit muss transparent dokumentiert sein und Angaben zu den folgenden Inhalten bereitstellen:

- Angaben zu den von der Datenverarbeitung betroffenen personenbezogenen Daten
- Angaben zu den von der Datenverarbeitung betroffenen Kategorien personenbezogener Daten

- Angaben zu den bei der Datenverarbeitung Beteiligten
- Angaben zu den bei der Datenverarbeitung eingesetzten Software-Systemen
- Angaben zu den beteiligten externen Stellen
- Angaben zu den Löschfristen der betroffenen personenbezogenen Daten
- Angaben zur Bewertung hinsichtlich besonderer Risiken für die von der Verarbeitung Betroffenen
- Angaben zu den implementierten technischen und organisatorischen Maßnahmen

Hierbei müssen insbesondere mindestens die nachfolgend genannten Verarbeitungstätigkeiten erfasst werden, sofern diese für die Organisation anwendbar sind:

- Benutzeranlage DV-Systeme
- Beschaffung und Einkauf
- Bewerbermanagement
- Dienstleisterbetreuung
- Dienstplanerstellung
- Dokumentenmanagement-Archivierung
- Elektronischer Zahlungsverkehr
- Entgeltabrechnung
- E-Mail-Dienst
- Homepage-Kontaktformular
- Homepage-Tracking
- Internet-Dienst
- Kundenbetreuung
- Newsletter
- Personaldatenverarbeitung
- Reisekostenabrechnung
- TK-Anlage
- Videoüberwachung
- Zeiterfassung Anwesenheit
- Zutrittskontrolle

3.1.4 Grundsätze der Datenverarbeitung

Die Organisation muss Regelungen zu den Grundsätzen der Datenverarbeitung implementieren. Diese Regelungen müssen Maßnahmen beinhalten zur:

- Rechtmäßigkeit und Transparenz der Datenverarbeitung
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität, Vertraulichkeit und Verfügbarkeit

Die Regelungen zu den Grundsätzen der Datenverarbeitung müssen als dokumentierte Informationen zur Verfügung stehen und den mit der Datenverarbeitung beauftragten Personen bekannt gemacht sein.

3.2 Datenschutzbeauftragter (DSB)

3.2.1 Bestellung DSB

Die Organisation muss einen Datenschutzbeauftragten bestellen, sofern mehr als 19 Personen mit der Verarbeitung von personenbezogenen Daten beschäftigt sind.

3.2.2 Meldung des DSB bei der Aufsichtsbehörde

Die Organisation muss sicherstellen, dass der Datenschutzbeauftragte bei der zuständigen Datenschutz-Aufsichtsbehörde gemeldet ist, sofern eine gesetzliche Bestellpflicht besteht.

3.2.3 Unabhängigkeit des DSB

Die Organisation muss die organisatorische Unabhängigkeit des Datenschutzbeauftragten sicherstellen, damit es bei der Tätigkeit des Datenschutzbeauftragten nicht zu Interessenskonflikten kommen kann.

3.2.4 Qualifikation des DSB

Die Organisation muss sicherstellen, dass der Datenschutzbeauftragte ausreichend für die ihm übertragenen Aufgaben qualifiziert ist. Bei einem internen Datenschutzbeauftragten muss die Organisation die regelmäßige Fortbildung zur Aufrechterhaltung der Qualifikation sicherstellen. Bei einem externen Datenschutzbeauftragten muss die Organisation regelmäßig Nachweise zur Aufrechterhaltung der Qualifikation einfordern.

3.3 Kontext und interessierte Parteien

3.3.1 Kontext

Die Organisation muss die externen und internen Themen bestimmen, die für die Zwecke der Datenverarbeitung relevant sind und sich auf ihre Fähigkeit auswirken, die beabsichtigten Ergebnisse bei der Datenverarbeitung zu erreichen.

3.3.2 Interessierte Parteien

Die Organisation muss die interessierten Parteien, die für die Datenverarbeitung relevant sind, und deren Anforderungen mit Bezug zur Datenverarbeitung bestimmen.

3.3.3 Anwendungsbereich

Die Organisation muss die Grenzen und die Anwendbarkeit ihrer Vorgaben zum Datenschutz dokumentieren. Hierbei muss die Organisation auch die unter 3.3.1 geforderten externen und internen Themen, die unter 3.3.2 genannten Anforderungen der interessierten Parteien und die Schnittstellen und Abhängigkeiten zwischen den Verarbeitungstätigkeiten berücksichtigen. Dies muss unabhängig davon erfolgen, ob die Datenverarbeitung durch die Organisation selbst oder durch eine andere Organisation im Auftrag durchgeführt wird. Der Anwendungsbereich (zu zertifizierender Bereich) muss als dokumentierte Information verfügbar sein. Der Anwendungsbereich kann sich

auch nur auf einzelne Bereiche oder einzelne Standorte beschränken. Funktionen einer Organisation, die zwingend für die Sicherstellung des Datenschutzes erforderlich sind, können nicht aus dem Anwendungsbereich ausgeschlossen werden.

3.3.4 Maßnahmen zum Schutz personenbezogener Daten

Die Organisation muss entsprechend den hier beschriebenen Anforderungen Maßnahmen zum Schutz personenbezogener Daten planen, verwirklichen, aufrechterhalten und fortlaufend verbessern. Dies muss dokumentierte Prüf- und Überwachungszyklen für die Datenverarbeitung und die Unternehmens-IT sowie die Bestätigung der obersten Leitung hinsichtlich der Einhaltung von IT-Mindeststandards (wie in Ziffer 3.7 definiert) beinhalten.

3.4 Führung und Verantwortung

3.4.1 Verpflichtung

Die oberste Leitung muss in Bezug auf den Datenschutz Führung und Verpflichtung übernehmen und hierbei sicherstellen, dass die Datenschutzpolitik und die Datenschutzziele festgelegt und mit der strategischen und operativen Ausrichtung der Organisation im Einklang sind. Die oberste Leitung muss sicherstellen,

- dass die Anforderungen des Datenschutzes in die Geschäfts- und Datenverarbeitungsprozesse der Organisation implementiert werden
- dass die für die Einführung und Aufrechterhaltung des Datenschutzes erforderlichen Ressourcen zur Verfügung stehen
- dass die Bedeutung eines wirksamen Datenschutzes vermittelt wird
- dass die Wichtigkeit der Erfüllung der Anforderungen des Datenschutzes vermittelt wird
- dass der Datenschutz sein beabsichtigtes Ergebnis bzw. seine beabsichtigten Ergebnisse erzielt

- dass die beteiligten Personen angeleitet und unterstützt werden, damit diese zur Wirksamkeit des Datenschutzes beitragen können
- dass die fortlaufende Verbesserung des Datenschutzes gefördert wird
- dass die Führungskräfte unterstützt werden, um die Wichtigkeit des Datenschutzes in ihrem jeweiligen Verantwortungsbereich deutlich zu machen
- Datenschutzpolitik / Datenschutzleitlinie oder Datenschutzpolitik / Datenschutzleitlinie

3.4.2 Politik / Leitlinie

Die oberste Leitung muss eine Datenschutzpolitik / Datenschutzleitlinie festlegen, und dabei sicherstellen,

- dass diese für den Zweck der Organisation angemessen ist
- dass die Datenschutzpolitik / Datenschutzleitlinie den Rahmen zur Definition von Datenschutzzielen bietet
- dass die Datenschutzziele beinhaltet sind
- dass eine Verpflichtung zur Erfüllung der Anforderungen mit Bezug zum Datenschutz vorhanden ist
- dass eine Verpflichtung zur fortlaufenden Verbesserung des Datenschutzes vorhanden ist

Die Datenschutzpolitik / Datenschutzleitlinie muss als dokumentierte Information verfügbar sein und in der Organisation bekannt gemacht sein. Für interessierte Parteien muss die Datenschutzpolitik / Datenschutzleitlinie verfügbar sein, soweit diese ein berechtigtes Interesse daran begründen können.

3.4.3. Verantwortlichkeiten

Die Rollen und Verantwortlichkeiten für die datenverarbeitenden Bereiche müssen zugewiesen und im Unternehmen bekannt gemacht sein. Ebenso müssen die Befugnisse, die zur Sicherstellung des Datenschutzes erforderlich sind, eindeutig zugewiesen sein. Hierbei müssen auch Regelungen zu Berichten über etwaige Anforderungen,

Änderungen, Risiken und Abweichungen beim Datenschutz und den Datenverarbeitungsverfahren definiert und bekannt gemacht sein. Im Einzelnen müssen die

- Verantwortlichkeiten für Verarbeitungstätigkeiten gemäß Art. 30 Abs. 1 DS-GVO
- Verantwortlichkeiten für die Sicherstellung der Wahrung der Betroffenenrechte gemäß Art. 13 bis 21 DS-GVO (vgl. Ziffer 3.9)
- Verantwortlichkeit für die Bearbeitung von Datenschutzverletzungen gemäß Art. 33 und 34 DS-GVO (vgl. Ziffer 3.10)

definiert und zugewiesen werden.

3.5 Planung

3.5.1 Allgemeines

Bei der Planung des Datenschutzes muss die Organisation den Kontext (vgl. Ziffer 3.3.1) und die Anforderungen der interessierten Parteien (vgl. Ziffer 3.3.2) berücksichtigen.

3.5.2 Risiken

Die Organisation muss die Risiken ermitteln und bewerten, die den Datenschutz gefährden oder negative Auswirkungen für den Datenschutz haben können. Die identifizierten Risiken müssen bearbeitet werden mit dem Ziel einer nachhaltigen Risikominimierung. Die Wirksamkeit der Maßnahmen muss bewertet und überwacht sein.

3.5.3 Ziele

Die Organisation muss die Datenschutzziele für alle relevanten Funktionen und Bereiche festlegen. Bei der Definition der Datenschutzziele muss sichergestellt werden,

- dass die Ziele mit der Datenschutzpolitik im Einklang stehen
- dass die Ziele messbar sind
- dass die Ziele und deren Ergebnisse die Risiken berücksichtigen
- dass die Ziele in der Organisation vermittelt werden
- dass die Ziele aktualisiert werden, sofern dies in Folge geänderter Rahmenbedingungen erforderlich ist

Die Organisation muss dokumentierte Informationen zu den Datenschutzzielen aufbewahren. Zur Erreichung der Datenschutzziele muss die Organisation die hierfür notwendigen Maßnahmen und Ressourcen definieren. Ebenso muss für jedes Ziel die Verantwortung zugewiesen werden. Im Rahmen der Überwachung muss die Organisation die Ergebnismessung sicherstellen.

3.6 Unterstützung

3.6.1 Ressourcen

Die Organisation muss die erforderlichen Ressourcen für den Aufbau, die Umsetzung und die fortlaufende Verbesserung des Datenschutzes bestimmen und bereitstellen.

3.6.2 Kompetenzen

Die Organisation muss die Kompetenzen bestimmen, die für die Sicherstellung des Datenschutzes erforderlich sind. Sie muss die mit der Datenverarbeitung beauftragten Personen auf die Einhaltung des Datenschutzes verpflichten. Die Organisation muss dokumentierte Informationen zum Nachweis der Kompetenzen führen.

3.6.3 Bewusstsein

Die Organisation muss sicherstellen, dass den mit der Datenverarbeitung beauftragten Personen die Datenschutzpolitik vermittelt ist und diese sich ihres Beitrags zur Sicherstellung des Datenschutzes bewusst sind. Die Organisation muss die mit der Datenverarbeitung beauftragten Personen regelmäßig schulen und sensibilisieren. Etwaige Dienstleister mit Zugang zu personenbezogenen Daten müssen angemessen berücksichtigt werden. Weiter muss die Organisation die Folgen der Nichteinhaltung des Datenschutzes vermitteln. Die

Organisation muss dokumentierte Informationen zum Nachweis der Bewusstseinsvermittlung aufbewahren.

3.6.4 Kommunikation

Die Organisation muss die datenschutzrelevante interne und externe Kommunikation festlegen. Hierbei muss die Organisation definieren, wer mit wem wann und worüber kommuniziert. Die Organisation muss dokumentierte Informationen über die Kommunikation führen.

3.6.5 Dokumentierte Informationen

Die Organisation muss dokumentierte Informationen erstellen, aufrechterhalten und weiterentwickeln, die sie für die Wirksamkeit und die Nachweisefähigkeit des Datenschutzes bestimmt hat. Hierbei muss die Organisation ihre Größe und Struktur, die Art ihrer Tätigkeiten, die Prozesse, die Produkte und Dienstleistungen sowie deren Komplexität berücksichtigen. Die Organisation kann die dokumentierten Informationen in Papierform oder in elektronischer Form mit der Möglichkeit alle elektronischen Informationen auszudrucken aufrechterhalten. Die benötigten dokumentierten Informationen müssen gelenkt sein. Die Organisation muss dokumentierte Informationen über die Methodik zur Lenkung der dokumentierten Informationen aufbewahren.

3.7 Technische und organisatorischen Maßnahmen

Die Organisation muss geeignete technische und organisatorische Maßnahmen zum Schutz aller personenbezogenen Daten implementieren, die unter die Verantwortung der Organisation fallen. Hierbei muss die Organisation neben dem Stand der Technik (diese sollte sich z. B. an ISO 27001, ISIS 12 o. ä. orientieren) auch die Art der verarbeiteten Daten und den damit einhergehenden Schutzbedarf berücksichtigen.
Als geeignete Maßnahmen können je nach Art der Verarbeitungstätigkeit insbesondere die in der Anlage beschriebenen Kriterien herangezogen werden. Dabei ist zu beachten, dass die in der Anlage beschriebenen Kriterien nicht abschließend sind und immer einzelfallbezogen betrachtet werden müssen. Vor dem Einsatz neuer Datenverarbeitungen muss die Organisation immer im Rahmen der Planung die in Ziffer 3.1.4 genannten Grundsätze angemessen berücksichtigten. Hierzu muss die Organisation ein Verfahren implementieren, welches die Berücksichtigung des Datenschutzes und den Umgang mit personenbezogenen Daten vollständig gewährleistet.

3.8 Spezifische Maßnahmen zum Datenschutz

Die Organisation muss Aussagen treffen zu den organisationsspezifischen Maßnahmen zum Schutz der personenbezogenen Daten. Hierbei muss die Organisation die nachfolgenden Themen in allen Bereichen angemessen berücksichtigten:

- die Organisationsstruktur
- die Orte der Datenverarbeitung
- die Mitarbeiter
- die Art der verarbeiteten personenbezogenen Daten
- die zur Datenverarbeitung eingesetzten Systeme
- die zur Datenverarbeitung eingesetzten Dienstleister
- die Schnittstellen zwischen den verschiedenen an einer Datenverarbeitung beteiligten Bereichen und Systemen.

Die Organisation muss ein Verfahren planen, verwirklichen und aufrechterhalten, damit besondere Risiken für die Rechte und Freiheiten der Betroffenen berücksichtigt werden, die durch eine Datenverarbeitung entstehen können. Hierbei muss die Organisation sicherstellen, dass die notwendige Fachkompetenz zur Beurteilung des Sachverhalts intern oder extern bereitgestellt ist.

3.9 Wahrung der Betroffenenrechte

3.9.1 Information der von der Datenverarbeitung Betroffenen

Die Organisation muss sicherstellen, dass die von der Verarbeitung personenbezogener Daten Betroffenen gemäß Art. 13 und 14 DS-GVO informiert werden.

3.9.2 Anfragen und Eingaben der von der Datenverarbeitung Betroffenen

Sofern ein Betroffener bei der Organisation das Recht auf

- Auskunft
- Berichtigung
- Löschung
- Einschränkung
- Mitteilungspflicht
- Datenübertragung
- Widerspruch

geltend macht, muss die Organisation sicherstellen, dass das Ersuchen eines Betroffenen unverzüglich und vollständig bearbeitet wird.

3.9.3 Webseite

Sofern die Organisation eine oder mehrere Webseiten/online-Auftritte als Verantwortlicher gemäß Art. 4 Nr. 7 DS-GVO bereitstellt muss sie sicherstellen, dass

- die Besucher über die Verarbeitung Ihrer personenbezogenen Daten umfassend informiert werden
- die Verarbeitung personenbezogener Daten der Besucher im Einklang mit den Vorgaben der DS-GVO erfolgt (vor allem auch zur Besucherverfolgung / zum Tracking)
- Dritt-Dienstleister datenschutzkonform eingesetzt werden

3.10 Verletzung des Datenschutzes

Die Organisation muss ein Verfahren zur Identifikation und Bearbeitung von Datenschutzverletzungen implementieren. Hierzu muss die Organisation die Verantwortlichkeiten für die Bearbeitung von Datenschutzverletzungen und die dazu notwendigen Prozesse implementieren und bekannt machen. Dabei müssen auch etwaige Datenschutzverletzungen außerhalb der Organisation berücksichtigt werden, sofern diese im Zusammenhang mit der Datenverarbeitung bzw. in der Verantwortung der Organisation stehen.

3.11 Bewertung

3.11.1 Überwachung, Messung, Analyse und Bewertung

Die Organisation muss die Wirksamkeit des Datenschutzes bewerten. Hierzu muss die Organisation folgendes festlegen:

- Definition, was im Datenschutz überwacht und gemessen werden soll, einschließlich der hierzu notwendigen Prozesse und Maßnahmen
- Definition der Methoden zur Überwachung, Messung, Analyse und Bewertung (sofern zutreffend)
- Zeitpunkt, an dem die Überwachung und Messung durchzuführen ist
- Zuweisung der Verantwortung für die Überwachung und Messung
- Definition, wie die Ergebnisse der Überwachung und Messung zu analysieren und zu bewerten sind
- Zuweisung der Verantwortung für die Analyse und Bewertung der Ergebnisse

Die Organisation muss als Nachweis der Überwachung, Messung, Analyse und Bewertung dokumentierte Informationen aufbewahren.

3.11.2 Internes Audit

Die Organisation muss regelmäßig interne Audits durchführen, um Informationen über den Stand des Datenschutzes zu erhalten. Hierzu muss die Organisation Audits planen und durchführen. Dabei sind für jedes Audit der Auditumfang und die Auditkriterien festzulegen. Bei der Durchführung des Audits muss die Unparteilichkeit des Auditors und eine objektive Beurteilung sichergestellt werden. Über die durchgeführten Audits müssen dokumentierte Informationen aufbewahrt werden. Das Ergebnis eines Audits muss den für die Organisation und den auditierten Bereich verantwortlichen Personen zugänglich gemacht werden.

3.11.3 Review

Die oberste Leitung muss den Datenschutz in der Organisation regelmäßig (mindestens einmal p.a.) bewerten, damit die fortdauernde Eignung, die Angemessenheit und die Wirksamkeit sichergestellt werden. Hierbei müssen die folgenden Themen berücksichtigt werden:

- Veränderungen bei internen Themen die den Datenschutz betreffen (Bereiche, Prozesse, Verantwortlichkeiten, Mitarbeiter)
- Veränderungen bei externen Themen die den Datenschutz betreffen (Dienstleister, Prozesse, Verantwortlichkeiten)
- Rückmeldung zu Nichtkonformitäten und Korrekturmaßnahmen
- Ergebnisse der Überwachungen und Messungen
- Ergebnisse der durchgeführten Audits
- Ergebnis der Zielerreichung
- Rückmeldungen der interessierten Parteien
- Ergebnisse zur Beurteilung und Behandlung der Risiken
- Maßnahmen und Möglichkeiten zur fortlaufenden Verbesserung des Datenschutzes

Die Ergebnisse des Reviews müssen Möglichkeiten der fortlaufenden Verbesserung sowie den notwendigen Änderungsbedarf im Datenschutz beinhalten und müssen der obersten Leitung zur weiteren Entscheidung vorgelegt werden.

3.12 Verbesserung

3.12.1 Nichtkonformitäten und Verbesserung

Bei aufgetretenen Datenschutzverletzungen oder sonstigen Nichtkonformitäten muss die Organisation die möglichen negativen Auswirkungen identifizieren und Maßnahmen zur Verringerung oder Abstellung ergreifen. Hierbei muss die Organisation immer mit dem Ziel der zukünftigen und nachhaltigen Risikovermeidung agieren.

3.12.2 Fortlaufende Verbesserung

Die Organisation muss die Eignung, die Angemessenheit und die Wirksamkeit des Datenschutzes fortlaufend verbessern. Hierzu müssen neben den Nichtkonformitäten und den daraus resultierenden Verbesserungen auch die Eingaben der Mitarbeiter und der interessierten Parteien einbezogen werden.

Anlage zu Ziffer 3.7

A 1 Räumliche Anforderungen und Zutrittsschutz

A 1.1
Die Organisation muss sicherstellen, dass Gebäude und Büroräume mit Datenverarbeitungsgeräten über einen wirksamen Zutrittsschutz verfügen.

A 1.2
Die Organisation muss sicherstellen, dass Serverräume bzw. Server über eine wirksamen Zutrittsschutz verfügen, bei dem nur die IT-Administratoren Zutritt zu den Servern haben.

A 1.3
Die Organisation muss sicherstellen, dass wirksame Sicherungsmaßnahmen für den Schutz der Server vorhanden sind (z. B. Schutz gegen Einbruch oder Sabotage, Schutz die Einwirkung von Umwelteinflüssen (z. B. Feuer, Wasser, Temperatur, Stromversorgung, usw.).

A 1.4
Die Organisation muss sicherstellen, dass Sie jederzeit Kenntnis darüber hat, welche organisationsfremden Personen sich in den Räumlichkeiten aufhalten.

A 2 Zugangsschutz

A 2.1
Die Organisation muss sicherstellen, dass eine dokumentierte und personifizierte Benutzerregistrierung, Benutzeränderung und Benutzerlöschung im Netzwerk vorhanden ist. Das Benutzerberechtigungskonzept muss hierbei rollen- oder gruppenbasiert aufgebaut sein. Dabei muss sichergestellt sein, dass auch cloudbasierte Anwendungen berücksichtigt werden und dass der jeweilige Dateneigner den Zugang zu personenbezogenen Daten autorisiert. Das „need to know Prinzip" muss ebenfalls eingehalten werden.

A 2.2
Die Organisation muss sicherstellen, dass bei Zugang zum Netzwerk der Organisation von außerhalb der Organisation ein ausreichender Schutz der Verbindung mittels VPN oder dergleichen vorhanden ist. Hierbei muss die Organisation auch sicherstellen, dass eine Zugangsprotokollierung vorhanden ist.

A 2.3
Die Organisation muss sicherstellen, dass eine Multi-Faktor-Authentifizierung bei Zugängen von außerhalb der Geschäftsräume zu Netzwerk oder Daten der Organisation durch Beschäftigte vorhanden ist.

A 2.4
Die Organisation muss sicherstellen, dass eine Multi-Faktor-Authentifizierung bei Zugang auf cloudbasierte Anwendungen mit risikobehafteten Daten vorhanden ist. Risikobehaftete Daten sind z. B. besondere Arten personenbezogener Daten (z. B. Gesundheitsdaten), Zahlungsdaten (z. B. Kontodaten) oder Daten, die für den Betrieb der eigenen Organisation essenziell erforderlich sind (z. B. Kundenkartei).

A 2.5
Die Organisation muss sicherstellen, dass eine Mobile-Device-Management-Software (MDM) bei Nutzung von privaten Endgeräten durch Beschäftigte vorhanden ist.

A 2.6
Die Organisation muss sicherstellen, dass komplexe Passwörter mit mindestens 8 Zeichen für den Zugang zum Netzwerk verwendet werden. Dabei müssen mindestens 3 der folgenden Zeichen (Großbuchstabe, Kleinbuchstabe, Ziffer, Sonderzeichen) verwendet werden.

A 3 Weitergabeschutz

A 3.1
Die Organisation muss sicherstellen, dass eine TLS-Mail-Verschlüsselung und zusätzlich die Möglichkeit einer „Ende zu Ende Verschlüsselung" beim E-Mail-Versand vorhanden ist. Die Organisation muss sicherstellen, dass eine HTTPS-Verschlüsselung mit mindestens TLS 1.2 und Perfect Forward Secrecy (PFS) vorhanden ist.

A 3.2
Die Organisation muss sicherstellen, dass Datenströme im Unternehmensnetzwerk überwacht und ausgewertet werden.

A 4 Technische Maßnahmen

A 4.1
Die Organisation muss sicherstellen, dass keine Server im Live-Einsatz sind, bei denen keine Sicherheits-Updates verfügbar sind (z. B. Windows Server 2003).

A 4.2
Die Organisation muss sicherstellen, dass keine Betriebssysteme im Live-Einsatz sind, bei denen keine Sicherheits-Updates verfügbar sind (z. B. Windows XP, Windows 7).

A 4.3
Die Organisation muss sicherstellen, dass ein durchgängiges und dokumentiertes Patch-Management für die IT-Hardware (Server, Switches, Router, etc.) vorhanden ist.

A 4.4
Die Organisation muss sicherstellen, dass ein durchgängiges und dokumentiertes Patch-Management für Endgeräte vorhanden ist.

A 4.5
Die Organisation muss sicherstellen, dass ein regelmäßiges, mehrstufiges und dokumentiertes Backup-Verfahren vorhanden ist.

A 4.6
Die Organisation muss sicherstellen, dass das Backup-System vom Hauptserver räumlich getrennt ist.

A 4.7
Die Organisation muss sicherstellen, dass verschlüsselte Backups (mit AES-256 Verschlüsselung) erstellt werden.

A 4.8
Die Organisation muss sicherstellen, dass eine technische Sicherung von Servern vorhanden ist. Dies sind unter anderem redundante Systeme, aktueller Virenscanner, aktuelle Firewall, Next Generation Firewall, Malewareschutz mit Sandboxing und Intrusion-Prevention-System/Intrusion-Detection-System.

A 4.9
Die Organisation muss sicherstellen, dass eine technische Sicherung von Endgeräten vorhanden ist. Dies sind unter anderem ein lokaler Virenscanner und eine lokale Firewall.

A 4.10
Die Organisation muss sicherstellen, dass ein IT-Betriebshandbuch zur Sicherstellung eines dokumentierten und geordneten IT-Betrieb vorhanden ist.

A 4.11
Die Organisation muss sicherstellen, dass ein Notfallhandbuch vorhanden ist.

A 4.12
Die Organisation muss sicherstellen, dass Rücksicherungs-/Wiederherstellungstests regelmäßig durchgeführt werden.

A 4.13
Die Organisation muss sicherstellen, dass alle Notebooks über eine Festplattenverschlüsselung verfügen, sofern nicht ausgeschlossen werden kann, dass personenbezogene Daten auf dem Notebook gespeichert werden.

A 4.14
Die Organisation muss sicherstellen, dass der Einsatz von mobilen Speichermedien verboten ist oder beim Einsatz von mobilen Speichermedien ausschließlich verschlüsselte und im Eigentum der Organisation stehende Speichermedien verwendet werden.

A 4.15
Die Organisation muss sicherstellen, dass Beschäftigte im Standard keine lokalen Admin-Rechte auf den Endgeräten haben. Für die Vergabe von lokalen Admin-Rechten muss die Organisation einen dokumentierten Freigabeprozess implementiert haben.

A 4.16
Die Organisation sollte sicherstellen, dass innerhalb der Organisation redundante und räumlich getrennte Datenverarbeitungssysteme vorhanden sind.

A 4.17
Die Organisation sollte sicherstellen, dass regelmäßige und dokumentierte Penetrationstests auf die internen IT-Systeme durchgeführt werden.

A 4.18
Die Organisation sollte sicherstellen, dass regelmäßige und dokumentierte Penetrationstests auf online-shops durchgeführt werden.

A 5 Testdaten

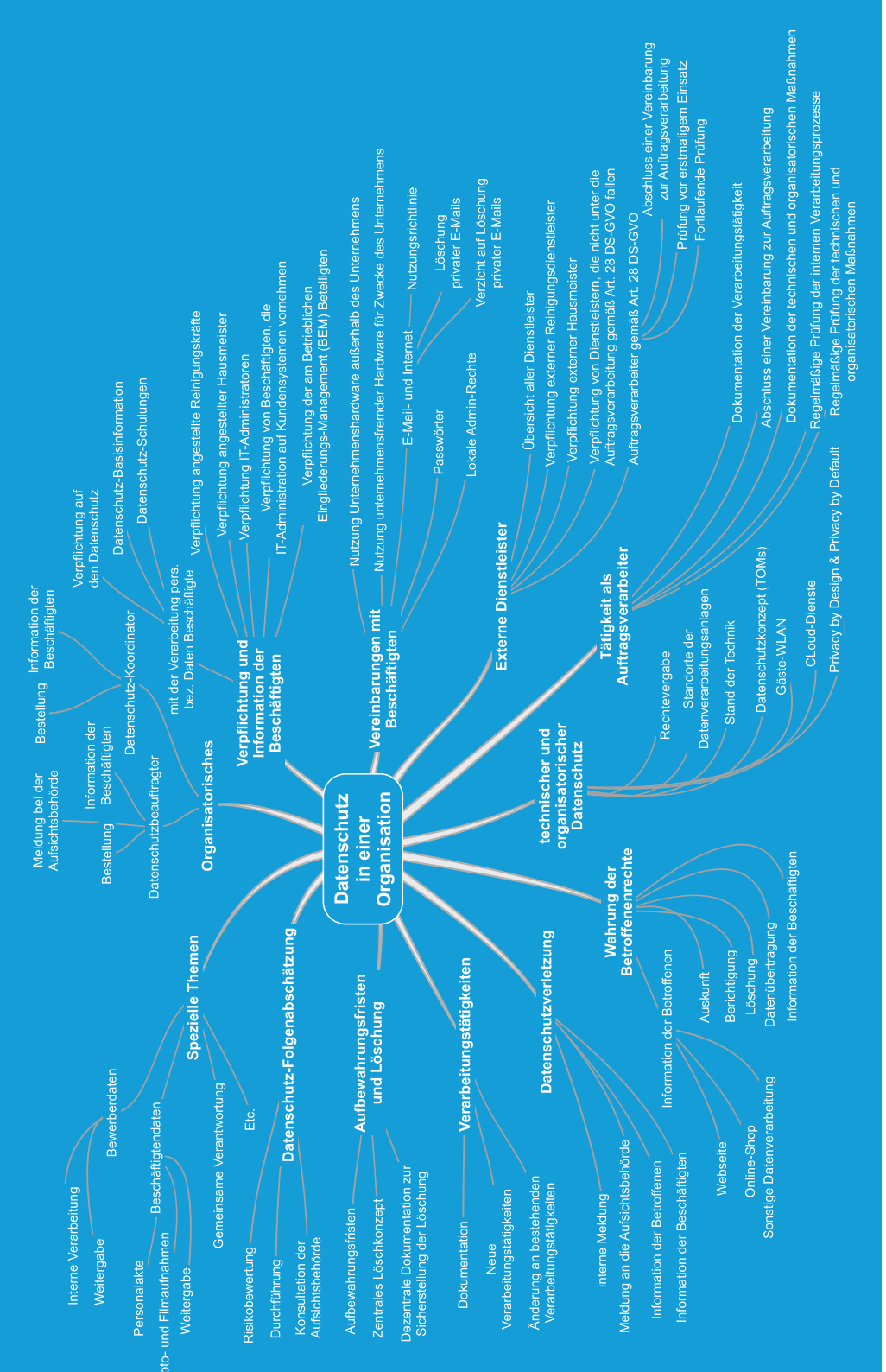
A 5.1
Die Organisation muss sicherstellen, dass auf Testumgebungen keine personenbezogenen Echtdaten genutzt werden. Sollte eine Test mit personenbezogenen Daten zwingend erforderlich sein, muss die Organisation sicherstellen, dass die Zugriffsberechtigungen sowie die technischen und organisatorischen Maßnahmen vergleichbar sind wie die auf die entsprechenden Echtdaten zur Anwendung kommenden technischen und organisatorischen Maßnahmen.

A 6 Trennung von Daten

A 6.1
Die Organisation muss sicherstellen, dass Daten von unterschiedlichen Auftraggebern sicher voneinander getrennt sind.

UMSETZUNG DES DATENSCHUTZES IN IHRER ORGANISATION

Um eine Organisation datenschutzkonform aufzustellen müssen eine Vielzahl von Themenfeldern bearbeitet werden. Nachfolgend sind die verschiedenen Themenfelder gegliedert dargestellt. Diese soll Ihnen die Bearbeitung erleichtern.



1 Organisatorisches

1.1 Datenschutzbeauftragter

1.1.1 Bestellung

Sofern in Ihrer Organisation mehr als 19 Personen mit der Verarbeitung von personenbezogenen Daten beschäftigt sind, müssen Sie einen Datenschutzbeauftragten bestellen. Bitte beachten Sie, dass personenbezogene Daten alle Daten sind, die eine natürliche Person näher identifizieren. Dies sind regelmäßig Name, Vorname, Anschrift, etc., aber auch die personifizierten E-Mail-Adressen einer Organisation sind personenbezogene Daten. Für die Praxis bedeutet dies, dass jede Person (sowohl Beschäftigte als auch Inhaber/Geschäftsführer) in Ihrer Organisation personenbezogene Daten verarbeitet, sobald diese Person Zugang zu einem E-Mail-Postfach oder einem ERP-System hat.

Die Bestellung eines Datenschutzbeauftragten muss schriftlich erfolgen. Dabei ist sowohl die Bestellung eines internen Datenschutzbeauftragten als auch eines externen Datenschutzbeauftragten möglich. Im Rahmen der Bestellung müssen die Aufgaben, Befugnisse und die Kompetenzen des Datenschutzbeauftragten dokumentiert sein.

Sofern in Ihrer Organisation ein interner Datenschutzbeauftragter bestellt werden soll, muss die Unabhängigkeit und die Weisungsfreiheit zwingend sichergestellt werden. Dies bedeutet, dass ein interner Datenschutzbeauftragter regelmäßig keine Führungsposition in Ihrer Organisation begleiten darf und auch nicht mit Mitgliedern der Geschäftsführung oder Geschäftsleitung privat verbunden sein darf. Ebenso sollte sichergestellt sein, dass der interne Datenschutzbeauftragte nicht in der IT oder im Personalbereich beschäftigt ist, da es hier regelmäßig schnell zu Interessenskonflikten kommen kann. Bitte beachten Sie, dass eine unwirksame Bestellung in Folge einer feh-

lenden Unabhängigkeit oder Weisungsfreiheit einer Nichtbestellung gleichkommt. Dies kann ggfs. zu einem Bußgeld wegen Nichtbestellung des gesetzlich geforderten Datenschutzbeauftragten führen.
Bei einem externen Datenschutzbeauftragten ist die Unabhängigkeit regelmäßig dadurch sichergestellt, dass der externe Datenschutzbeauftragte keine weiteren Tätigkeiten in Ihrer Organisation ausübt. Auch hier muss darauf geachtet werden, dass keine private Verbindung zwischen dem Datenschutzbeauftragten und einem Mitglied der Geschäftsführung oder Geschäftsleitung besteht, durch welche die Unabhängigkeit Weisungsfreiheit des externen Datenschutzbeauftragten in Frage gestellt werden könnte.

1.1.2 Meldung bei der Datenschutz-Aufsichtsbehörde

Sie müssen einen bestellten Datenschutzbeauftragten an die für Ihre Organisation zuständige Datenschutz-Aufsichtsbehörde melden. Zur Durchführung der Meldung haben Sie in der Regel zwei Alternativen:

Alternative 1:
Prüfen Sie zunächst, ob die für Ihre Organisation zuständige Datenschutz-Aufsichtsbehörde auf ihrer Webseite die Möglichkeit zur online-Meldung des Datenschutzbeauftragten anbietet. Hier können Sie die Meldung online vornehmen und Sie erhalten in der Regel eine automatisierte Eingangsbestätigung.

Alternative 2:
Melden Sie den Datenschutzbeauftragten per Post oder Telefax an die für Ihre Organisation zuständige Datenschutz-Aufsichtsbehörde.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 05-03-03 DE Meldung DSB an Aufsicht.
Stellen Sie die revisionssichere Archivierung der Meldung des Datenschutzbeauftragten an die Datenschutz-Aufsichtsbehörde und die Eingangsbestätigung der Datenschutz-Aufsichtsbehörde sicher.

1.1.3 Information der Beschäftigten über die Bestellung eines Datenschutzbeauftragten

Die Beschäftigten müssen über die Bestellung eines Datenschutzbeauftragten informiert werden, da jeder Beschäftigte das Recht hat, sich bei Fragen zu seiner Person und den damit einhergehenden Schutzrechten direkt an den Datenschutzbeauftragten zu wenden. Die direkten Kontaktdaten des Datenschutzbeauftragten müssen den Beschäftigten zur Möglichkeit einer direkten Kontaktaufnahme zur Verfügung gestellt werden.
Sofern Ihre Organisation einen externen Datenschutzbeauftragten bestellt hat, ist es empfehlenswert, alle geschäftlichen Fragestellungen und Themen immer über einen internen Datenschutz-Koordinator an den externen Datenschutzbeauftragten zu kommunizieren. Dies verbessert die Kommunikation und verringert regelmäßig den Abstimmungsaufwand zwischen Ihrer Organisation und dem externen Datenschutzbeauftragten.
Hinsichtlich der Datenschutz-Themen, die die Beschäftigten und damit einhergehend ihre Schutzrechte direkt betreffen, ist jedoch immer eine direkte Kommunikation zwischen Beschäftigten und dem externen Datenschutzbeauftragten erforderlich.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 05-03-04 DE MitarbeiterInfo Bestellung DSB.
Stellen Sie die revisionssichere Archivierung des Nachweises zur Information der Beschäftigten sicher.

1.2 Datenschutz-Koordinator

1.2.1 Bestellung

Zusätzlich zur Bestellung eines externen Datenschutzbeauftragten kann ein interner Datenschutz-Koordinator benannt werden. Ein interner Datenschutz-Koordinator bildet die Schnittstelle zwischen Ihrer Organisation und dem externen Datenschutzbeauftragten. Er

koordiniert die Zusammenarbeit der Fachbereiche und der Beschäftigten mit dem externen Datenschutzbeauftragten. Bei größeren Organisationen oder bei Organisationen mit mehreren Standorten kann es zweckmäßig sein, mehrere Datenschutz-Koordinatoren zu benennen. Sofern Sie mehrere Datenschutz-Koordinatoren benennen, sollten Sie intern eine klare Zuordnung der Aufgaben und Themenbereiche sicherstellen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 05-03-05 DE Datenschutzkoordinator.
Stellen Sie die revisionssichere Archivierung der Bestellung zum Datenschutz-Koordinator sicher.

1.2.2 Information der Beschäftigten über die Bestellung eines Datenschutz-Koordinators

Sofern sie einen oder mehrere interne(n) Datenschutz-Koordinator(en) bestellt haben, müssen Sie die Beschäftigten darüber informieren und die internen Kommunikationswege hinsichtlich der Datenschutzthemen in Ihrer Organisation festlegen.

2 Verpflichtung und Information der Beschäftigten

2.1 Verpflichtung der mit der Verarbeitung personenbezogener Daten Beschäftigten

Alle mit der Verarbeitung personenbezogener Daten Beschäftigten müssen auf die Einhaltung des Datenschutzes verpflichtet werden. Die Verpflichtung umfasst damit alle Beschäftigten, die im Rahmen ihrer Tätigkeit personenbezogene Daten verarbeiten oder Zugang zu personenbezogenen Daten haben.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 07-02-01 DE Verpflichtung Datenschutz.
Stellen Sie die revisionssichere Archivierung der erfolgten Verpflichtung der Beschäftigten sicher.

2.2 Basisinformation zum Datenschutz für die Verpflichtung mit der Verarbeitung personenbezogener Daten Beschäftigten

Zur Information der Beschäftigten über die Maßnahmen, die zur Sicherstellung des Datenschutzes (innerhalb und außerhalb Ihrer Organisation) erforderlich sind, sollten Sie eine Richtlinie bzw. ein Vorgabedokument erstellen. Diese Richtlinie sollte mindestens Vorgaben zu den nachfolgenden Themen beinhalten:

- Geltungsbereich der Richtlinie
- Grundsätze beim Umgang mit personenbezogenen Daten
- Technische und organisatorische Maßnahmen
- Arbeiten im privaten Umfeld

- Arbeiten auf Reisen
- E-Mail- und Internetnutzung
- Externe Dienstleister
- Kontaktdaten des Ansprechpartners für Fragen zum Datenschutz

Diese Themenbereiche stellen die Mindestanforderungen dar. Sie können hier jederzeit weitere organisationsspezifische Regelungen hinzufügen.
Die Datenschutz-Information müssen Sie allen Beschäftigten zur Verfügung stellen. Dies kann in Papierform, per E-Mail oder in einem Intranet erfolgen. Wichtig ist, dass Sie die Datenschutz-Information auch allen zukünftigen Beschäftigten zur Verfügung stellen. Diese kann z. B. im Rahmen des Einstellungs-/Einarbeitungsprozesses erfolgen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 07-03-03 DE Datenschutz-Information.
Stellen Sie die revisionssichere Archivierung der Information der Beschäftigten über die Datenschutz-Information sicher.

2.3 Verpflichtung der in Ihrer Organisation angestellten Reinigungskräfte

Sofern Sie in Ihrer Organisation angestellte Reinigungskräfte haben, müssen diese ebenfalls auf die Einhaltung des Datenschutzes verpflichtet werden, da die Reinigungskräfte im Rahmen Ihrer Tätigkeit regelmäßig Zugang zu personenbezogenen Daten (in der Regel Papierdokumente) haben. Die Verpflichtung sollte u. a. Regelungen zur Geheimhaltung und zum Umgang mit personenbezogenen Daten im Rahmen der Reinigungstätigkeiten beinhalten, so zum Beispiel zur datenschutzkonformen Entsorgung von Papierdokumenten.

Hinweis: Wenn Sie hingegen einen externen Reinigungsdienstleister mit der Reinigung Ihrer Geschäftsräume beauftragt haben, müssen

Sie eine andere Vorlage verwenden. Weitere Informationen zur Verpflichtung von externen Reinigungsdienstleistern finden Sie in Ziffer 4.2.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-06 DE Vertraulichkeitsverpflichtung Reinigungsmitarbeiter.
Stellen Sie die revisionssichere Archivierung der Verpflichtung der angestellten Reinigungskräfte sicher.

2.4 Verpflichtung des in Ihrer Organisation angestellten Hausmeisters

Ein in Ihrer Organisation angestellter Hausmeister muss ebenfalls auf die Einhaltung des Datenschutzes verpflichtet werden, da ein Hausmeister im Rahmen seiner Tätigkeit regelmäßig Zugang zu personenbezogenen Daten haben kann. Die Verpflichtung sollte u. a. Regelungen zur Geheimhaltung und zum Umgang mit personenbezogenen Daten beinhalten, die ein Hausmeister im Rahmen seiner Tätigkeit regelmäßig zur Kenntnis bekommt.

Hinweis: Wenn Sie hingegen einen externen Hausmeister mit Hausmeistertätigkeiten für Ihre Organisation beauftragt haben, müssen Sie eine andere Vorlage verwenden. Weitere Informationen zur Verpflichtung eines externen Hausmeisters finden Sie in Ziffer 4.3.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-07 DE Vertraulichkeitsverpflichtung Hausmeister.
Stellen Sie die revisionssichere Archivierung der Verpflichtung eines angestellten Hausmeisters sicher.

2.5 Verpflichtung der IT-Administratoren

IT-Administratoren haben bedingt durch ihre Tätigkeit regelmäßig weitreichende Zugriffsmöglichkeiten auf personenbezogene Daten, die in den Datenverarbeitungssystemen gespeichert sind. Daher gilt für diesen Personenkreis eine besondere Pflicht zur Geheimhaltung und zur Vertraulichkeit. IT-Administratoren müssen daher zusätzlich auf die Einhaltung der Vorgaben des § 3 Abs. 1 bis 3 TTDSG verpflichtet werden.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-21 DE Zusatzverpflichtung IT-Administratoren. Stellen Sie die revisionssichere Archivierung der Zusatzverpflichtung der IT-Administratoren sicher.

2.6 Verpflichtung von Beschäftigten, die IT-Administration auf Kundensystemen vornehmen

Wenn Sie Beschäftigte in Ihrer Organisation haben, die Wartungs- und Supporttätigkeiten auf Datenverarbeitungssystemen Ihrer Kunden vornehmen, ist es empfehlenswert, diesen Personenkreis auf die Geheimhaltung und Vertraulichkeit beim Umgang mit Daten der Kunden zu verpflichten. Dies ist insofern wichtig, da die Support-Mitarbeiter ggfs. auf dem Kundensystem Admin-Rechte haben und somit im Rahmen ihrer Supporttätigkeiten weitreichende Zugriffe auf Informationen und Daten haben. Daher sollten Sie diesen Personenkreis zusätzlich auf die Einhaltung der Vorgaben des § 3 Abs. 1 bis 3 TTDSG und des § 203 StGB verpflichten.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-30 DE Zusatzverpflichtung IT-Administratoren und Support_Ma.

Stellen Sie die revisionssichere Archivierung der Zusatzverpflichtung der IT-Administratoren und Support-Mitarbeiter sicher.

2.7 Verpflichtung der am BEM beteiligten Beschäftigten

2.7 Verpflichtung der am Betrieblichen Eingliederungs-Management (BEM) beteiligten Beschäftigten

Sofern Sie in Ihrer Organisation ein Betriebliches Eingliederungs-Management (BEM) implementiert haben, können Sie die am BEM beteiligten Beschäftigten zusätzlich auf die besondere Verschwiegenheit nach den Vorgaben des Sozialgesetzbuchs unter Bezugnahme auf den § 167 Abs. 2 SGB IX. 2 SGB IX verpflichten.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 07-02-05 DE Verpflichtung BEM-Beteiligte.
Stellen Sie die revisionssichere Archivierung der Verpflichtung der am Betrieblichen Eingliederungsmanagement beteiligten Beschäftigten sicher.

3 Vereinbarungen mit Beschäftigten

3.1 Nutzung der organisationseigenen Hardware außerhalb der Organisation

Wenn Beschäftigte die organisationseigene Hardware außerhalb der Organisation nutzen, müssen besondere Maßnahmen zum Schutz der von der Verarbeitung betroffenen personenbezogenen Daten ergriffen werden. Hier sollten Sie eine Vereinbarung mit den Beschäftigten abschließen und darin die von den Beschäftigten genutzte Hardware benennen sowie die Regelungen spezifizieren, die bei Arbeiten außerhalb der Organisationsräumlichkeiten eingehalten werden müssen. Mindestanforderungen sind ggfs. eine Regelung zur

- Nutzung der Hardware für private Zwecke
- Regelmäßigen Aktualisierung von Virenschutz etc.
- Weitergabe/Nutzung des Gerätes an/durch Dritte
- Sicheren Verwahrung des Gerätes
- Trennung der Organisationsdaten von anderen Daten
- Verwendung von Blickschutzfilter
- Etc.

Wichtig ist bei der Nutzung von „Home-Office/Telearbeitsplätzen", dass die Organisation hier ein Zutrittsrecht vereinbart, um ggfs. die Einhaltung des Datenschutzes kontrollieren zu können. Die Aufsichtsbehörde hat im Übrigen ein gesetzliches Zutrittsrecht zu allen Arbeitsplätzen, an denen eine Verarbeitung von personenbezogenen Daten erfolgt. Bei rein „mobilem Arbeiten" kann auf die Passage zum Zutrittsrecht verzichtet werden.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-22 DE Hardware im privaten Umfeld.

Stellen Sie die revisionssichere Archivierung der Regelungen zur Hardware im privaten Umfeld sicher.

3.2 Nutzung von organisationsfremder Hardware für Zwecke der Organisation

Wenn Beschäftigte organisationsfremde Hardware (in der Regel private Hardware) für Zwecke bzw. für den Zugriff auf personenbezogene Daten der Organisation des nutzen, müssen besondere Maßnahmen zum Schutz der von der Verarbeitung betroffenen personenbezogenen Daten durch die Organisation ergriffen werden. Hier sollten Sie eine Vereinbarung mit den Beschäftigten abschließen und darin die von den Beschäftigten genutzte private Hardware benennen und die Regelungen spezifizieren, die bei Arbeiten für Zwecke der Organisation mit dieser Hardware zwingend eingehalten werden müssen. Mindestanforderungen sind ggfs. eine Regelung zur

- Installation einer Firewall auf der Hardware
- Nutzung eines aktuellen Virenprogramms und regelmäßiger automatisierter Aktualisierung
- Einsatz einer Festplattenverschlüsselung (mind. bei Nutzung eines Notebooks)
- Einsatz eines sicheren Passworts mit mindestens 8 Zeichen
- Zugriff auf Daten der Organisation durch Dritte
- Trennung der Daten der Organisation von den sonstigen Datenbeständen
- Löschung etwaiger Daten der Organisation nach Auftragsabschluss
- Löschung etwaiger Daten der Organisation, bevor die Hardware einem Dritten übergeben wird (bspw. bei Reparaturen)
- Etc.

Bitte beachten Sie, dass beim Einsatz von privater Hardware für Zwecke der Organisation regelmäßig umfangreiche Sicherungsmaßnah-

men zur Gewährleistung des Stands der Technik erforderlich sind, wie z. B. eine Multifaktor-Authentifizierung bzw. 2-Faktor-Authentifizierung und ein Mobile Device Management System (MDM).

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-23 DE Nutzung unternehmensfremder Hardware.
Stellen Sie die revisionssichere Archivierung der Verpflichtung der Regelung zur Nutzung organisationsfremder Hardware sicher.

3.3 Nutzung von E-Mail und Internet

Hinsichtlich der Nutzung des geschäftlichen E-Mail-Postfachs und des geschäftlichen Internetzugangs müssen Sie aus Sicht des Datenschutzes und ggfs. unter Berücksichtigung des Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) eine verbindliche Regelung treffen. Generell sollte die private Nutzung des geschäftlichen E-Mail-Postfachs verboten werden, damit die Organisation nicht in das Risiko gerät, mit dem Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) zu kollidieren. Die private Nutzung des geschäftlichen Internetzugangs kann hingegen rechtskonform geregelt werden. Bei einer erlaubten privaten Nutzung des geschäftlichen Internetzugangs sollten Sie eine Regelung der nachfolgenden Themen sicherstellen:

- Allgemeine Verhaltensregeln bei der Internetnutzung
- Private Nutzung während der Arbeitszeit oder nur in den Pausen
- Download von Musikdateien
- Download von sonstigen ausführbaren Dateien
- Nutzung von kostenpflichtigen Informationen
- Nutzung des geschäftlichen Internetanschlusses für etwaige geschäftliche Zwecke, die nicht im Zusammenhang mit Ihrer Organisation stehen
- Umgang mit rechtsextremen, pornographischen oder Gewalt verherrlichenden Seiten

- Teilnahme in sozialen Netzwerken oder sonstigen Foren
- Umgang mit Passwörtern
- Maßnahmen bei Missachtung
- Protokollierung der Internetnutzung
- Einwilligung der Betroffenen die Protokollierung der privaten Internetnutzung

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-24 DE Nutzung E-Mail und Internet.
Stellen Sie die revisionssichere Archivierung der Regelung zur Nutzung von E-Mail und Internet sicher.

3.4 Löschbestätigung privater E-Mails

Wenn Sie in der Vergangenheit die private Nutzung des geschäftlichen E-Mail-Postfachs erlaubt bzw. geduldet haben, müssen Sie davon ausgehen, dass in den E-Mail-Postfächern der Beschäftigten auch private E-Mails gespeichert sind. Die Beschäftigten sollten in dokumentierter Form aufgefordert werden, alle privaten E-Mails aus dem geschäftlichen E-Mail-Postfach zu löschen und die Löschung auch in dokumentierter Form zu bestätigen. Dann kann der Arbeitgeber ohne weitere Risiken auf ein E-Mail-Postfach Zugriff nehmen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-26 DE Loeschungsbestaetigung private E-Mail.
Stellen Sie die revisionssichere Archivierung der Regelung zur Löschung privater E-Mails sicher.

3.5 Verzicht auf die Löschung von privaten E-Mails

Sofern ein Beschäftigter keine Löschung seiner privaten E-Mails aus dem geschäftlichen E-Mail-Postfach vornehmen möchte, kann er der Organisation die Einwilligung erteilen, dass dieses auf das E-Mail-Postfach Zugriff nehmen kann. Diese Einwilligung muss dokumentiert werden.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-27 DE Zugriff E-Mail-Postfach.
Stellen Sie die revisionssichere Archivierung der Regelung zum Verzicht auf die Löschung privater E-Mails sicher.

3.6 Verwendung von Passwörtern

Passwörter sind ein wichtiges Kriterium zum Schutz personenbezogener Daten. Außerdem dient ein Passwort in Verbindung mit einem Benutzernamen regelmäßig zur eindeutigen Identifizierung eines Betroffenen am Datenverarbeitungssystem. Sofern Sie eine systemseitige bzw. technische Passwort-Richtlinie haben, benötigen Sie ggfs. keine separate Verpflichtung der Beschäftigten auf die Einhaltung einer Passwort-Richtlinie. Wenn Sie hingegen keine systemseitige bzw. technische Passwort-Richtlinie haben, sollten Sie die Einhaltung der Vorgaben zur Nutzung von sicheren Passwörtern im Rahmen einer separaten Verpflichtung der Beschäftigten gewährleisten. Hier sollten Sie die nachfolgenden Themen berücksichtigten.

- Startpasswörter, die die Benutzer im Rahmen der ersten Anmeldung erhalten, müssen umgehend durch eigene (individuelle) Passwörter ersetzt werden
- Passwörter dürfen nicht aufgeschrieben oder am Arbeitsplatz hinterlegt werden
- Passwörter dürfen nicht an Dritte (auch nicht an Kollegen oder Vorgesetzte) weitergegeben werden

- Verbot der Anmeldung mit den Anmeldedaten eines anderen Benutzers
- Bei der Eingabe von Passwörtern ist darauf zu achten, dass Dritte Passwörter nicht zur Kenntnis nehmen
- Passwörter müssen mindestens 8 Zeichen haben
- Passwörter müssen mindestens einen Großbuchstaben, einen Kleinbuchstaben, eine Ziffer und ein Sonderzeichen enthalten
- Trivialpasswörter dürfen nicht verwendet werden (z. B. qwertz, 12345678, abcdefg)
- Das Geburtsdatum darf nicht als Passwort oder als Bestandteil des Passworts verwendet werden
- Passwörter müssen bei Verdacht einer Kompromittierung gewechselt werden
- Der Benutzername darf nicht Bestandteil des Passwortes sein
- Passwörter dürfen ohne entsprechende Schutzmechanismen nicht in dem EDV-System (bspw. im Browser) gespeichert werden
- Die innerhalb der Organisation (Netzwerk) verwendeten Passwörter dürfen nicht im Internet oder im privaten Umfeld verwendet werden

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-31 DE Umgang mit Passwoertern.
Stellen Sie die revisionssichere Archivierung der Regelung zum Umgang mit Passwörtern sicher.

3.7 Lokale Administrationsrechte

Lokale Admin-Rechte führen zu einem hohen Risiko für die Organisation, da die Beschäftigten mit lokalen Admin-Rechten weitreichende Berechtigungen auf einem Endgerät haben. Dies stellt für die Organisation ein nicht unerhebliches Sicherheitsrisiko dar, da durch die lokalen Administrationsrechte ggfs. auch organisationsinterne Schutz- und Sicherheitsmaßnahmen außer Kraft gesetzt bzw.

umgangen werden können. Daher sollten Sie die Beschäftigten, die lokale Admin-Rechte haben, auf die Einhaltung der nachfolgenden Vorgaben verpflichten.

- Keine Installation von aus dem Internet geladener Software oder sonstige Fremdsoftware ohne Kenntnis und Zustimmung der IT-Administration
- Keine Änderung der prüfen ggfs.: hardware-spezifischen Sicherheitseinstellungen, der Sicherheitseinstellung im E-Mail-Programm und der Sicherheitseinstellung im Internetbrowser ohne Kenntnis und Zustimmung der IT-Administration

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-32 DE Lokale Adminrechte.
Stellen Sie die revisionssichere Archivierung der Regelung zum Umgang mit lokalen Admin-Rechten sicher.

4 Externe Dienstleister

Der Einsatz von externen Dienstleistern erfordert regelmäßig Regelungen zur Sicherstellung des Datenschutzes bei der Verarbeitung von personenbezogenen Daten. Hier ist zwischen der Auftragsverarbeitung gemäß Art. 28 DS-GVO und der sonstigen Dienstleistung bzw. Leistungserbringung in eigener Verantwortung zu unterscheiden.
In der Praxis ist ein „Einsatz von externen Dienstleistern" dann gegeben, wenn ein externer Dienstleister

- Zugang oder Zugriff auf Datenverarbeitungssysteme hat, mit denen personenbezogene Daten verarbeitet werden,
- Zugang oder Zugriff auf Datenverarbeitungstätigkeiten hat, mit denen personenbezogene Daten verarbeitet werden,

unabhängig davon, ob der Betrieb des Datenverarbeitungssystems durch Ihre Organisation selbst oder durch einen externen Dienstleister erfolgt.
Dasselbe gilt für den Betrieb, die Wartung oder den Support von Rechenzentren oder Cloud-basierten Datenverarbeitungssystemen.

4.1 Übersicht der externen Dienstleister

Zunächst sollten Sie sich einen Überblick über alle von Ihrer Organisation beauftragten externen Dienstleister verschaffen. Dazu sollten die Verantwortlichen aller Bereiche bzw. Abteilungen die in ihrem Verantwortungsbereich eingesetzten externen Dienstleister auflisten. Dabei sollten die Verantwortlichen Informationen zu den nachfolgenden Punkten bereitstellen.

- Name und Anschrift des Dienstleisters
- Kontaktdaten des Ansprechpartners beim Dienstleister
- Beschreibung der Tätigkeiten, die der Dienstleister für Ihre Organisation erbringt

- Information, ob der Dienstleister einen Zugang/Zugriff auf die EDV-Systeme Ihrer Organisation hat
- Information, ob der Dienstleister personenbezogene Daten verarbeitet oder Zugang zu diesem hat, sofern sich diese Daten in Ihrer Verantwortung befinden
- Information, welche personenbezogene Daten oder Datenkategorien der Dienstleister verarbeitet
- Information, ob der Dienstleister eine Cloud-Anwendung bereitstellt
- Information zu den zugriffsberechtigten Standardbenutzern
- Information zu den zugriffsberechtigten administrativen Benutzern
- Information zu den personenbezogenen Daten, die in der Cloud verarbeitet werden
- Information zu den zugriffsberechtigten externen Dienstleistern
- Information zur Zugriffssicherung (2-Faktor-Authentifizierung)
- Information zur Datensicherung
- Information zu den geschlossenen Verträgen

Diese detaillierte Auflistung erleichtert dem Datenschutzbeauftragten die Beurteilung hinsichtlich der Notwendigkeit von datenschutzrechtlich Vereinbarungen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-02-12 DE Uebersicht Dienstleister.
Stellen Sie die revisionssichere Archivierung der Übersicht der externen Dienstleister sicher.

4.2 Verpflichtung eines externen Reinigungsdienstleisters

Ein in Ihrer Organisation eingesetzter externer Reinigungsdienstleister muss ebenfalls auf die Einhaltung des Datenschutzes verpflichtet werden, da Reinigungskräfte im Rahmen Ihrer Tätigkeit regelmäßig

Zugang zu personenbezogenen Daten (in der Regel Papierdokumente) haben.
In der Praxis kann es sinnvoll sein, neben dem Reinigungsdienstleister (das Unternehmen) zusätzlich auch die in Ihren Geschäftsräumen mit den Reinigungstätigkeiten beauftragten Beschäftigen des Reinigungsdienstleisters auf die Einhaltung des Datenschutzes zu verpflichten. Sie sind aber nicht dazu verpflichtet, da dies in der Regel die Aufgabe Ihres Reinigungsdienstleisters ist. Die Praxis zeigt aber, dass hier immer wieder Lücken in der Verpflichtungskette vorhanden sind. In der Folge kann der falsche Umgang mit personenbezogenen Daten durch Reinigungskräfte zu Datenschutzverletzungen führen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlagen 08-03-82 DE Vertraulichkeitsverpflichtung externe Reinigungsdienstleister und 08-03-83 DE Vertraulichkeitsverpflichtung für Mitarbeiter externe Reinigungsdienstleister.
Stellen Sie die revisionssichere Archivierung der Vertraulichkeitsverpflichtung externer Reinigungsdienstleister sicher.

4.3 Verpflichtung eines externen Hausmeisters

Ein in Ihrer Organisation eingesetzter externer Hausmeister muss ebenfalls auf die Einhaltung des Datenschutzes verpflichtet werden, da ein Hausmeister im Rahmen seiner Tätigkeit regelmäßig Zugang zu personenbezogenen Daten (in der Regel Papierdokumente) hat.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-82 DE Vertraulichkeitsverpflichtung externe Reinigungsdienstleister und passen diese inhaltlich an.
Stellen Sie die revisionssichere Archivierung der Vertraulichkeitsverpflichtung externer Hausmeister sicher.

4.4 Verpflichtung von Dienstleistern, die nicht unter die Auftragsverarbeitung gemäß Art. 28 DS-GVO fallen

Alle Dienstleister, die keinen Zugang zu Datenverarbeitungsanlagen mit personenbezogenen Daten haben bzw. nicht mit der Verarbeitung von personenbezogenen Daten beauftragt sind, müssen nicht zwingend auf die Einhaltung des Datenschutzes verpflichtet werden. Dennoch wird an dieser Stelle empfohlen, alle diese Dienstleister auf die Geheimhaltung sowie Einhaltung des Datenschutzes und das Vorhandensein von angemessenen technischen und organisatorischen Maßnahmen zu verpflichten.

Hinweis: Diese Art der Vertraulichkeitsverpflichtung ist nur für solche Dienstleister, die keine Auftragsverarbeitung gemäß Art. 28 DS-GVO durchführen. Sie ist somit keine Alternative zu einer Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-81 DE Vertraulichkeitsverpflichtung externe Dienstleister.
Stellen Sie die revisionssichere Archivierung der Vertraulichkeitsverpflichtung externer Dienstleister sicher.

4.5 Verpflichtung von Dienstleistern, die unter die Auftragsverarbeitung gemäß Art. 28 DS-GVO fallen

Alle Dienstleister, die im Rahmen der Auftragsverarbeitung tätig werden, müssen gemäß den Vorgaben des Art. 28 DS-GVO verpflichtet werden. Dies erfordert neben einer dokumentierten Vereinbarung auch das Vorhandensein der beim Auftragsverarbeiter eingerichteten technischen und organisatorischen Maßnahmen zum Datenschutz. Für die Praxis bedeutet dies, dass Sie immer sicherstellen müssen, dass die technischen und organisatorischen Maßnahmen vom Auftragsverarbeiter als Anlage bei der abgeschlossenen Vereinbarung zur Auftragsverarbeitung beigefügt sind.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-02-09-02 DE Auftragsverarbeitung Formular.
Stellen Sie die revisionssichere Archivierung der mit den Auftragnehmern abgeschlossenen Vereinbarungen zur Auftragsverarbeitung sicher.

4.6 Prüfung einer Vereinbarung zur Auftragsverarbeitung

Sofern Sie von einem Auftraggeber oder Auftragsverarbeiter eine Vereinbarung zur Auftragsverarbeitung zur Unterzeichnung vorgelegt bekommen, sollten Sie diese inhaltlich auf Vollständigkeit überprüfen. Damit stellen Sie sicher, dass die Vereinbarung allen Vorgaben der DS-GVO entspricht. Im Detail müssen Sie prüfen, ob die nachfolgenden Punkte in der Vereinbarung berücksichtigt sind.

- Beschreibung der zu erbringenden Leistungen bzw. Tätigkeiten und der Zweck der Verarbeitung
- Angaben zur Laufzeit der Vereinbarung
- Angaben zu den Arten der personenbezogenen Daten, die verarbeitet werden
- Angaben zu den Kategorien der personenbezogenen Daten, die verarbeitet werden
- Angaben zu den besonderen Kategorien der personenbezogenen Daten, die verarbeitet werden
- Angaben zur Wahrung der Betroffenenrechte gemäß Art. 12 bis 22 DS-GVO
- Angaben zur Bearbeitung von Datenschutzverletzungen gemäß Art. 33 und 34 DS-GVO
- Angaben zur Durchführung von Datenschutz-Folgenabschätzungen gemäß Art. 35 DS-GVO
- Angaben zur Verpflichtung einer weisungs- und zweckgebundenen Datenverarbeitung

- Angaben zu weisungsberechtigten Personen
- Angaben zu Weisungsempfängern
- Angaben zum Umgang mit Weisungen, die gegen Datenschutzrecht verstoßen
- Angaben zu den einzuhaltenden technischen und organisatorischen Maßnahmen
- Angaben zur separierten Speicherung der Daten
- Angaben zur regelmäßigen Sicherung der Daten
- Angaben zur regelmäßigen Überprüfung der Verarbeitungsergebnisse
- Angaben zur Unterstützungspflicht des Auftragnehmers hinsichtlich der Verpflichtungen aus den Artt. 12 bis 22 und 32 bis 35 DS-GVO
- Angaben zur Verpflichtung der mit der Verarbeitung Beschäftigten
- Angaben zu etwaigen besonderen Geheimhaltungsverpflichtungen, denen der Auftraggeber unterliegt
- Angaben zum Datenschutzschutzbeauftragten bzw. Datenschutzverantwortlichen
- Angaben zum Einsatz von Subunternehmern
- Angaben zu Überprüfungsrechten des Auftraggebers
- Angaben zur den Prüfpflichten des Auftragsverarbeiters
- Angaben zur Löschung bzw. Rückgabe der Daten
- Angaben zur Verarbeitung der Daten im Home-Office bzw. beim mobilen Arbeiten

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-02-10 DE Pruefung AV–Vertrag.
Stellen Sie die revisionssichere Archivierung der Prüfung von Vereinbarungen zur Auftragsverarbeitung sicher.

5 Tätigkeiten als Auftragsverarbeiter

Sofern Ihre Organisation als Auftragsverarbeiter gemäß Art. 28 DS-GVO tätig ist, müssen Sie zu zusätzliche Dokumentationspflichten erfüllen.
Dies sind

- die Dokumentation der Verarbeitungstätigkeit, die für den Auftraggeber erbracht wird,
- der Abschluss einer Vereinbarung zur Auftragsverarbeitung und
- die Dokumentation der in Ihrer Organisation eingerichteten technischen und organisatorischen Maßnahmen.

5.1 Dokumentation der Verarbeitungstätigkeit

Als Auftragsverarbeiter müssen Sie die Verarbeitungstätigkeit gemäß Art. 30 Abs. 2 DS-GVO dokumentieren, die Sie im Rahmen der Auftragsverarbeitung gemäß Artikel 28 DS-GVO für einen Auftraggeber erbringen. Sie müssen dieses Dokument auf Anforderung der Datenschutz-Aufsichtsbehörde sowie dem Auftraggeber zur Verfügung stellen. Die Dokumentation muss Angaben zu den nachfolgenden Punkten beinhalten.

- Angaben zu Ihrer Organisation und den gesetzlichen Vertretern
- Angaben zum Datenschutzbeauftragten
- Angaben zur Organisation des Auftraggebers
- Angaben zum Datenschutzbeauftragten des Auftraggebers
- Angaben zur Verarbeitungstätigkeit
- Angaben zu Datenübermittlungen in Drittstaaten und etwaigen geeigneten Garantien
- Angaben zu den in Ihrer Organisation eingerichteten technischen und organisatorischen Maßnahmen

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-01-07 DE Datenverarbeitungsverfahren 30_2 DS-GVO.
Stellen Sie die revisionssichere Archivierung der Verarbeitungsdokumentation gemäß Art. 30 Abs. 2 DS-GVO sicher.

5.2 Abschluss einer Vereinbarung zur Auftragsverarbeitung

Ein Dienstleister, der im Rahmen der Auftragsverarbeitung tätig wird, ist ebenso wie der Auftraggeber datenschutzrechtlich in der Verantwortung und damit einhergehend in der Haftung für den Abschluss einer Vereinbarung zur Auftragsverarbeitung gemäß Art. 28 DS-GVO. Dies bedeutet, dass Sie als Auftragsverarbeiter mitverantwortlich sind, dass eine Vereinbarung zur Auftragsverarbeitung abgeschlossen ist. Es bietet sich an, mit Ihrem Auftraggeber zu klären, ob dieser Ihnen eine Vereinbarung zur Auftragsverarbeitung zur Verfügung stellt, oder ob Sie eine Vereinbarung zur Verfügung stellen sollen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-02-09-02 DE Auftragsverarbeitung Formular.
Stellen Sie die revisionssichere Archivierung der mit den Auftraggebern abgeschlossenen Vereinbarungen zur Auftragsverarbeitung sicher.

6 Technischer und organisatorischer Datenschutz

Die DS-GVO stellt eine Vielzahl von Anforderungen an Ihre Organisation hinsichtlich des Schutzes personenbezogener Daten. Hier sind im Wesentlichen aber nicht abschließend

- Art. 32 DS-GVO – Sicherheit der Verarbeitung
- Art. 24 DS-GVO – Verantwortung des für die Verarbeitung Verantwortlichen
- Art. 29 DS-GVO – Verarbeitung unter Aufsicht des Verantwortlichen oder des Auftragsverarbeiters
- Art. 5 DS-GVO – Grundsätze für die Verarbeitung personenbezogener Daten und die Rechenschaftspflicht

zu nennen.
Die DS-GVO stellt vor allem beim technischen Datenschutz nur bedingt messbare Angaben zur Verfügung. Hier kann z. B. auf die Anforderungen der Controls der ISO 27001/27002 oder der TISAX etc. zurückgegriffen werden. Generell muss eine Organisation in der Lage sein, den Stand der Technik zu gewährleisten und nachzuweisen. Bei der Definition der erforderlichen Maßnahmen müssen auch die verarbeiteten personenbezogenen Daten und die damit einhergehenden Schutzrechte für die Betroffenen angemessen berücksichtigt werden.

6.1 Rechtevergabe

Die Rechtvergabe ist ein wesentlicher Baustein zur Sicherstellung des Datenschutzes und der Datensicherheit. Es muss generell sichergestellt werden, dass Beschäftigte nur auf die Daten Zugriff nehmen können, die sie für die ihnen zugewiesenen Tätigkeiten benötigen. Daher muss die Berechtigungsvergabe für den Zugang und den Zugriff zu den Datenverarbeitungssystemen in einem geregelten und doku-

mentierten Verfahren erfolgen. Hierbei müssen Sie auch sicherstellen, dass Zugriffe auf Datenverzeichnisse und auf personenbezogene Daten immer vom jeweiligen Dateneigner autorisiert werden. Daher ist für die Rechtevergabe immer ein 4-Augenprinzip zu implementieren. Bitte beachten Sie, dass die eingerichteten Berechtigungen regelmäßig (mindestens einmal jährlich) hinsichtlich ihrer Aktualität und Richtigkeit geprüft werden müssen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 07-02-04 DE Rechtevergabe.
Stellen Sie die revisionssichere Archivierung der Regelung und Nachweisführung zur Rechtevergabe sicher.

6.2 Standorte der Datenverarbeitungsanlagen

Für einen umfassenden Überblick über die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten ist eine Kenntnis über alle Standorte der Datenverarbeitungsanlagen unerlässlich. Dabei sollten immer die Standorte und Räumlichkeiten hinsichtlich ihrer Eignung als Serverraum betrachtet und dokumentiert werden. Dabei ist jeder Serverraum innerhalb der Organisation für sich zu betrachten und zu bewerten. Ebenso sind externe Serverstandorte (i.d.R. Rechenzentren und Cloud-Dienste) zu berücksichtigen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-01-03 DE Standorte von Datenverarbeitungsanlagen.
Stellen Sie die revisionssichere Archivierung der Dokumentation der Standorte der Datenverarbeitungsanlagen sicher.

6.3 Stand der Technik

Der Stand der Technik beschreibt detailliert, wie die IT-Abteilung die technische Sicherheit der Datenverarbeitungssysteme gewährleistet. Hier sollte immer eine detaillierte Erfassung der in Ihrer Organisation eingerichteten Maßnahmen zur Gewährleistung des Stand der Technik erfolgen. Wichtig ist, dass Sie alle Maßnahmen zur Sicherheit der Datenverarbeitung berücksichtigen, u. a.

- Angaben zur IT-Infrastruktur, Netzwerk und den Servern
- Angaben zu den Endgeräten
- Angaben zu den Regelungen der E-Mail- und Internetnutzung
- Angaben zu den Sicherheitsmaßnahmen bei Servern und Endgeräten
- Angaben zur Datensicherung
- etc.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-01-04 DE Stand der Technik.
Stellen Sie die revisionssichere Archivierung der Dokumentation zum Stand der Technik sicher.

6.4 Datenschutzkonzept

Das Datenschutzkonzept beschreibt die in Ihrer Organisation eingerichteten technischen und organisatorischen Maßnahmen zum Schutz der personenbezogenen Daten. Sofern Ihre Organisation als Auftragsverarbeiter gemäß Art. 28 DS-GVO tätig wird benötigen Sie das Datenschutzkonzept in der Regel auch als Nachweis zur Auftragsverarbeitung gemäß Art. 28 DS-GVO für Ihre Auftraggeber. Das Datenschutzkonzept sollte alle technischen und organisatorischen Maßnahmen beschreiben, die in Ihrer Organisation zum Schutz der personenbezogenen Daten vorhanden sind. Dabei können Sie sich z. B. an der folgenden Struktur orientieren.

Technische und organisatorische Maßnahmen zur

- Vertraulichkeit
- Zutrittskontrolle
- Zugangskontrolle
- Zugriffskontrolle
- Pseudonymisierung
- Tennungskontrolle
- Integrität
- Weitergabekontrolle
- Eingabekontrolle
- Auftragskontrolle
- Verfügbarkeit und Belastbarkeit
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung
- zur Gewährleistung von datenschutzfreundlichen Voreinstellungen
- Ggfs. weiteren organisationsspezifischen Maßnahmen

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-01-05 DE Datenschutzkonzept.
Stellen Sie die revisionssichere Archivierung der Dokumentation zum Datenschutzkonzept sicher.

6.5 Gäste-WLAN

Wenn Ihre Organisation für Besucher oder organisationsfremde Endgeräte ein Gäste-WLAN zur Verfügung stellt, müssen Sie die Nutzer des Gäste-WLAN über die Verarbeitung ihrer personenbezogenen Daten informieren. Hier können Sie die Gäste/Nutzer auch über die einzuhaltenden Verhaltensmaßnahmen bei der Nutzung des Gäste-WLAN informieren.
Sofern technisch möglich sollten Sie die Informationen auf der Login-Seite des Gäste-WLAN bereitstellen. Sofern dies technisch nicht möglich ist können Sie die Informationen auch an anderer Stelle (z. B. durch Auslegen oder Aushang in den Besprechungsräumen oder durch Information im Rahmen der Besucherregistrierung) zur Verfügung stellen.
Wenn Sie in Ihrer Organisation ein Gäste-WLAN bereitstellen, das für alle Benutzer ein und dasselbe Zugangspasswort beinhaltet, dann sollten Sie dieses Passwort in regelmäßigen Abständen wechseln.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-25 DE Gaeste-WLAN.
Stellen Sie die revisionssichere Archivierung der Dokumentation zur Umsetzung der Regelung zum Gäste-WLAN sicher.

6.6 Cloud-Dienste

Der Einsatz von Cloud-Diensten erfordert regelmäßig besondere Regelungen zur Sicherstellung des Datenschutzes bei der Verarbeitung von personenbezogenen Daten. Dabei müssen sowohl die Zugriffsberechtigungen zur operativen Datenverarbeitung als auch die Zugriffsberechtigungen zur administrativen Datenverarbeitung berücksichtigt werden. Ebenso muss beim Einsatz von Cloud-Diensten auch immer die Sicherheit der Daten und die Verfügbarkeit der Daten angemessen berücksichtigt werden. Nachfolgend finden Sie ein eine Aufstellung von Maßnahmen, die für einen sicheren Betrieb von Cloud-Diensten unverzichtbar sind.

- Für jeden verwendeten Cloud-Dienst muss eine verantwortliche Person festgelegt werden
- Der für einen Cloud-Dienst Verantwortliche muss eine jederzeit aktuelle Übersicht aller aktiven Benutzer des Cloud-Dienstes führen
- Für jeden Benutzer eines Cloud-Dienst muss ein eigener personifizierter Benutzer eingerichtet werden, die Verwendung von

Sammelbenutzern ist unzulässig und bedarf im Einzelfall einer dokumentierten Freigabe durch den Datenschutzbeauftragten
- Benutzer müssen angewiesen werden, ihr personifiziertes Passwort für den Cloud-Dienst geheim zu halten. Personifizierte Passwörter dürfen nicht an Kollegen oder den Vorgesetzten weitergegeben werden
- Passwörter, die für die Anmeldung bei Cloud-Diensten verwendet werden, dürfen nicht für den Zugang zu anderen Datenverarbeitungssystemen des Unternehmens verwendet werden
- Ein in einem Cloud-Dienst eingerichteter Benutzer muss unverzüglich gelöscht werden, wenn dieser Benutzer den Zugriff nicht mehr benötigt (z. B. bei Kündigung, Versetzung oder Änderung der Aufgaben)
- Cloud-Dienste müssen über ein sicheres Login-Verfahren mit einer 2-Faktor-Authentifizierung verfügen

6.7 Privacy by design & Privacy by default

Sofern Ihre Organisation eine Software zur Verarbeitung personenbezogener Daten bereitstellt, kann es sinnvoll sein, die von Ihrer Organisation umgesetzten Maßnahmen zum datenschutzkonformen Einsatz der Software zu beschreiben. Damit verringern Sie die Anzahl der Rückfragen Ihrer Auftraggeber und Sie schaffen Transparenz hinsichtlich des datenschutzkonformen Einsatzes der Software. Die Dokumentation sollte mindestens Angaben zu den nachfolgenden Punkten beinhalten.
- Angaben zum Betrieb der Software
- Angaben zum Berechtigungskonzept
- Angaben zum Passwort-Management
- Angaben zum Zugriffskonzept
- Angaben zu den verschiedenen Berechtigungen
- Angaben zur Möglichkeit der Sperrung von einzelnen Felder für Benutzer

- Angaben zur Identifizierbarkeit von personenbezogenen Daten innerhalb der Software
- Angaben zu den Möglichkeiten zur Wahrung der Betroffenenrechte
- Angaben zu den technischen Maßnahmen zum Schutz der Daten

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-01-06 DE Datenschutz bei Software.
Stellen Sie die revisionssichere Archivierung der Dokumentation zur Umsetzung des Datenschutzes bei Software sicher.

7 Information der Betroffenen zur Datenverarbeitung und Datenschutz bei Webseiten

Wenn Ihre Organisation eine eigene Webseite betreibt, bietet es sich an, die Informationen für die Betroffenen gemäß Art. 13 und 14 DS-GVO in die Webseiten-Datenschutzerklärung aufzunehmen und in der E-Mail-Signatur auf die Webseiten-Datenschutzerklärung zu verlinken. Bei der Webseiten-Datenschutzerklärung müssen Sie sicherstellen, dass diese „top site" verlinkt ist (also von jeder Seite aus zugänglich ist). Die Erreichbarkeit muss auch dann gegeben sein, wenn Sie ein Consent-Management-Tool auf Ihrer Webseite installiert haben und der Webseitenbesucher noch keine Auswahl im Consent-Management-Tool getroffen hat.
Bei der Bereitstellung einer Webseite ist zu beachten, dass eine aktuelle und auf der Webseite zugeschnittene Datenschutzerklärung vorhanden sein muss. Dies bedeutet, dass Sie alle Verarbeitungen von personenbezogenen Daten in der Webseiten-Datenschutzerklärung benennen müssen, die Sie auf der Webseite vornehmen. Bitte achten Sie darauf, dass Sie in der Webseiten-Datenschutzerklärung auch nur die Verarbeitungen von personenbezogenen Daten aufnehmen dürfen, die tatsächlich vorhanden sind.
Die Informationspflicht gemäß Art. 13 und 14 DS-GVO für die Verarbeitung von Bewerberdaten, Beschäftigtendaten, Kunden- und Interessentendaten sowie Lieferanten- und Dienstleisterdaten können Sie zusätzlich in die webseiten-Datenschutzerklärung aufnehmen. Sie müssen hierzu für die verschiedenen Betroffenengruppen Angaben zu den nachfolgenden Themen bereitstellen.

- Angaben zu den betroffenen Daten
- Angaben zum Verarbeitungszweck
- Angaben zu den Kategorien von Empfängern

- Angaben zum Drittlandtransfer
- Angaben zur Dauer der Datenspeicherung

Wenn Sie diese hier empfohlene Variante zur Information der Betroffenen verwenden, müssen Sie in Ihrer Organisations-E-Mail-Signatur den nachfolgenden Hinweis aufnehmen.

Informationen zur Datenverarbeitung gemäß Art. 13 und 14 EU-Datenschutzgrundverordnung finden sie unter [hier den Adresse Ihrer Webseiten-Datenschutzerklärung eintragen]

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-61 DE Homepage Datenschutzerklaerung.
Stellen Sie die revisionssichere Archivierung der Dokumentation zur Information zur Datenverarbeitung gemäß Art. 13 und 14 DS-GVO sicher.

8 Information der Betroffenen zur Nutzung von Videokonferenz- und Webinar-Software

Sofern Sie eine Videokonferenz- und Webinar-Software nutzen, müssen Sie auch hier die Informationen zur Datenverarbeitung gemäß Art. 13 und 14 DS-GVO sicherstellen, da Sie personenbezogene Daten im Rahmen der Kommunikation mit den Betroffenen verarbeiten.
Bei der Informationspflicht gemäß Art. 13 und 14 DS-GVO für die Verarbeitung von personenbezogenen Daten der Teilnehmer von Videokonferenzen und Webinaren müssen Sie Angaben zu den nachfolgenden Themen bereitstellen.

- Angaben zu den betroffenen Daten
- Angaben zum Verarbeitungszweck
- Angaben zu den Kategorien von Empfängern
- Angaben zum Drittlandtransfer
- Angaben zur Dauer der Datenspeicherung

Die Information der Betroffenen kann z. B. im Rahmen der Einladung per E-Mail erfolgen. Alternativ könnte diese Information auch in der Datenschutzerklärung der Webseite Ihrer Organisation bereitgestellt werden. Hier kann dann über einen Link in der Einladung auf die Datenschutzerklärung verwiesen werden.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-03-10 DE Videokonferenz- und Webinar-Software.
Stellen Sie die revisionssichere Archivierung der Dokumentation zur Umsetzung der Information der Betroffenen zur Nutzung von Videokonferenz- und Webinar-Software sicher.

9 Wahrung der Betroffenenrechte

Jeder von der Verarbeitung personenbezogenen Betroffene hat das Recht auf Auskunft, Berichtigung, Löschung, Einschränkung und Übertragung der zu seiner Person verarbeiteten Daten.

9.1 Recht auf Auskunft

Jede von der Verarbeitung personenbezogener Daten betroffene Person kann vom Verantwortlichen (das ist in der Regel Ihre Organisation) Auskunft über die zu ihrer Person gespeicherten Daten verlangen. Bitte beachten Sie, dass ein Auskunftsersuchen unverzüglich innerhalb von maximal einem Monat zu beantworten ist. Sofern eine Beantwortung innerhalb eines Monats nicht möglich ist, muss dem Betroffenen eine Zwischennachricht übermittelt werden. Eine Negativauskunft (wenn Ihre Organisation keine Daten des Betroffenen gespeichert hat) muss ebenfalls erfolgen. Bitte beachten Sie, dass Sie neben der Beauskunftung der in Ihrer Organisation verarbeiteten personenbezogenen Daten dem Anfragenden auch die verarbeiteten Daten zur Verfügung stellen müssen. Dies ist insofern erforderlich, damit der Betroffene auch die inhaltliche Richtigkeit der gespeicherten personenbezogenen Daten prüfen kann.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-02-02-01 DE Auskunftsersuchen und 08-02-02-02 DE Beantwortung Auskunftsersuchen.
Stellen Sie die revisionssichere Archivierung der Dokumentation zur internen Bearbeitung und der Beantwortung von Auskunftsersuchen sicher.

9.2 Recht auf Berichtigung und Löschung

Jede von der Verarbeitung personenbezogener Daten betroffene Person kann vom Verantwortlichen (das ist in der Regel Ihre Organisation) die Berichtigung oder Löschung der zu ihrer Person gespeicherten Daten verlangen. Bitte beachten Sie, dass Ihre Organisation zur Berichtigung von personenbezogenen Daten verpflichtet ist, sofern die Daten in Ihrem Verantwortungsbereich inhaltlich falsch erfasst wurden.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-02-04 DE Berichtigung Loeschung
Stellen Sie die revisionssichere Archivierung der bearbeiteten Berichtigungs- und Löschungsersuchen sicher.

9.3 Recht auf Datenübertragung

Jede von der Verarbeitung personenbezogener Daten betroffene Person kann vom Verantwortlichen (das ist in der Regel Ihre Organisation) die Zurverfügungstellung der von ihr zur Verfügung gestellten Daten verlangen. Bitte beachten Sie, dass Ihre Organisation zur Datenübertragung verpflichtet ist, sofern die personenbezogenen Daten des Betroffenen elektronisch erhoben wurden. Hinsichtlich des elektronischen Formats, in dem die personenbezogenen Daten bereitgestellt werden müssen, gibt es keine abschließenden Vorgaben. Hier kann z. B. eine CSV-Datei oder eine TXT-Datei verwendet werden.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-02-06 DE Datenuebertragung.
Stellen Sie die revisionssichere Archivierung der bearbeiteten Dokumente zur Datenübertragung sicher.

9.4 Information der Beschäftigten

Die Beschäftigten in Ihrer Organisation müssen sich über die zwingende Notwendigkeit hinsichtlich der internen Meldung bei eingehenden Forderungen eines von der Datenverarbeitung Betroffenen bewusst sein. Daher sollten die Beschäftigten jede Anfrage eines von der Verarbeitung personenbezogener Daten Betroffenen an eine zentrale Stelle innerhalb Ihrer Organisation zur Bearbeitung weiterleiten. Die Bearbeitung und Beantwortung sollten immer nur von einer Stelle im Unternehmen erfolgen. Wichtig ist, dass Sie die Informationen über die Maßnahmen zur Sicherstellung der Wahrung der Betroffenenrechte auch allen zukünftigen Beschäftigten zur Verfügung stellen. Diese kann z. B. im Rahmen des Einstellungs-/Einarbeitungsprozesses erfolgen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 07-03-07 DE Info Beschaeftigte Auskunft Berichtigung Loeschung.
Stellen Sie die revisionssichere Archivierung der erfolgten Information der Beschäftigten sicher.

10 Datenschutzverletzungen

Eine Datenschutzverletzung ist in der Regel immer dann gegeben, wenn personenbezogene Daten einer unberechtigten Person zur Kenntnis gelangen und damit ein Risiko für die Schutzrechte der von der Datenschutzverletzung Betroffenen einhergeht. Dabei ist keine Unterscheidung notwendig, ob es sich bei der unberechtigten Person um einen Beschäftigten Ihrer Organisation oder um einen Dritten handelt.
Bitte beachten Sie, dass innerhalb Ihrer Organisation generell jede Verletzung des Schutzes personenbezogener Daten gemeldet werden muss. Nur so können Sie auch im Falle einer Meldepflicht dieser innerhalb von 72 Stunden nach Bekanntwerden der Verletzung nachkommen. Hierzu bedarf es entsprechender interner Melde- und Bearbeitungsprozesse.

10.1 Interne Meldung einer Datenschutzverletzung

Gemäß Art. 33 Abs. 5 DS-GVO sind jede Verletzung des Schutzes personenbezogener Daten und die in diesem Zusammenhang ergriffenen Maßnahmen zu dokumentieren. Generell sollte jede interne Meldung einer Datenschutzverletzung an den Datenschutzbeauftragten übermittelt werden, damit dieser bei der Bearbeitung und Bewertung einer internen Meldung unterstützten kann.

10.2 Meldung einer Datenschutzverletzung an die Aufsichtsbehörde

Sofern eine Datenschutzverletzung zu einem Risiko für den Schutzes personenbezogener Daten führt oder führen kann, sind Sie zur Meldung der Datenschutzverletzung an die für Ihre Organisation zuständige Datenschutz-Aufsichtsbehörde binnen 72 Stunden nach Bekanntwerden verpflichtet. Bei der Entscheidungsfindung und der Durchführung einer Meldung unterstützt Sie Ihr Datenschutzbeauftragter. Für der Durchführung der Meldung haben Sie in der Regel zwei Alternativen:

Alternative 1:
Prüfen Sie zunächst, ob die für Ihre Organisation zuständige Datenschutz-Aufsichtsbehörde auf ihrer Webseite die Möglichkeit zur online-Meldung einer Datenschutzverletzung anbietet. Hier können Sie dann die Meldung der Datenschutzverletzung online durchführen und Sie erhalten eine automatisierte Eingangsbestätigung.

Alternative 2:
Melden Sie die Datenschutzverletzung per Post und vorab per Telefax an die für Ihre Organisation zuständige Datenschutz-Aufsichtsbehörde.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie für die Alternative 2 die Word-Vorlage 08-04-02 DE Interne Meldung Datenschutzverletzung und 08-04-03 DE Externe Meldung Datenschutzverletzung.
Stellen Sie die revisionssichere Archivierung der dokumentierten Datenschutzverletzungen sicher.

10.3 Information der von einer Datenschutzverletzung Betroffenen

Sofern eine Datenschutzverletzung zu einem hohen Risiko für Schutzrechte der von der Verletzung personenbezogener Daten Betroffenen führt oder führen kann, müssen Sie zusätzlich zur Meldung an die zuständige Datenschutz-Aufsichtsbehörde, die von der Datenschutzverletzung Betroffenen informieren. Hier müssen Sie den Betroffenen neben den Angaben zur Verletzung Ihrer personenbezogenen Daten auch mitteilen, welche Schutzmaßnahmen in Folge der Datenschutzverletzung durch die Betroffenen erforderlich sind.

10.4 Information der Beschäftigten

Sie müssen sicherstellen, dass die Beschäftigen Ihrer Organisation wissen, was unter einer Datenschutzverletzung zu verstehen ist. Hierzu sollten Sie den Beschäftigten anhand von Beispielen verdeutlichen, was alles unter einer Datenschutzverletzung zu verstehen ist. Nachfolgend sind einige Beispiele genannt, die regelmäßig eine Datenschutzverletzung zur Folge haben.

- Wenn ein Notebook abhanden kommt, das keine verschlüsselte Festplatte hat
- Wenn ein unverschlüsselter USB-Stick oder ein sonstiger unverschlüsselter elektronischer Datenträger abhandenkommen und nicht ausgeschlossen werden kann, dass auf dem Speicher personenbezogene Daten gespeichert sind
- Wenn ein verschlüsselter USB-Stick oder eine verschlüsselte Festplatte abhandenkommen und die Daten nur auf diesem abhandengekommenen Medium gespeichert waren
- Erpressungs- oder Verschlüsselungstrojaner personenbezogene Daten verschlüsselt
- Wenn eine E-Mail mit personenbezogenen Daten einem falschen Empfänger übermittelt wurde

- Wenn Kontodaten oder Entgeltabrechnungsdaten an einen falschen Empfänger geschickt wurden
- Wenn generell personenbezogene Daten an einen falschen Empfänger übermittelt wurden (per Post, per Fax, per E-Mail)
- Wenn Hacker die Möglichkeit zur Abfrage von Kundendaten, Passwörter oder Bestellhistorien aus einem online-Shop haben oder hatten
- Wenn Ein Kunde die Daten eines oder mehrerer anderen Kunden in Folge eines Fehlers im Datenverarbeitungssystem einsehen oder gar abrufen konnte
- Wenn eine werbliche Ansprache per E-Mail über einen für alle sichtbaren Verteiler erfolgt ist (die Adressen wurden in das „An" oder „Cc" Feld eingetragen anstatt in das „Bcc" Feld)
- Wenn Dokumente mit personenbezogenen Daten verloren oder entwendet wurden

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 07-03-06 DE Info Beschaeftigte Datenschutzverletzung.
Stellen Sie die revisionssichere Archivierung der dokumentierten Information der Beschäftigten über die Maßnahmen bei Datenschutzverletzungen sicher.

11 Verarbeitungstätigkeiten

Gemäß Art. 30 Abs. 1 DS-GVO muss Ihre Organisation alle Verarbeitungen von personenbezogenen Daten dokumentieren, die in der Verantwortung Ihrer Organisation vorgenommen werden. Dies ist zwingend erforderlich, damit die in Art. 5 DS-GVO geforderte Rechenschaftspflicht erbracht werden kann.
Mit der Dokumentation der Verarbeitungstätigkeiten beginnen Sie am besten in der Form, dass Sie alle Verarbeitungstätigkeiten nach Bereichen sortiert dokumentieren. Dabei sollte jeder Bereich bzw. jede Abteilung die von ihr vorgenommenen Verarbeitungen von personenbezogenen Daten in einer Übersichtstabelle dokumentieren.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 01-02-01 DE Uebersicht Verarbeitungstaetigkeiten oder die Excel-Vorlage 01-02-02 DE Datenverarbeitungsprozesse.
Stellen Sie die revisionssichere Archivierung der Übersicht der Datenverarbeitungstätigkeiten sicher.

11.1 Deckblatt zu den Verarbeitungstätigkeiten

Für die Dokumentation der Verarbeitungstätigkeiten muss einmalig das Deckblatt erstellt werden. In diesem Deckblatt erfassen Sie die nachfolgenden Angaben.

- Benennung der verantwortlichen Stelle (Unternehmensname gemäß HR-Eintragung) und Anschrift der verantwortlichen Stelle
- Ggfs. Weiterer Verantwortlicher gemäß Art. 26 DS-GVO
- Kontaktdaten des gesetzlichen Vertreters der verantwortlichen Stelle
- Kontaktdaten des Datenschutzbeauftragten

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-01-01-01 DE Verarbeitungstaetigkeit 30 DS-GVO Deckblatt.
Stellen Sie die revisionssichere Archivierung des Deckblatt zu den Verarbeitungstätigkeiten sicher.

11.2 Detaillierte Verarbeitungstätigkeiten

Für jede in der bereichs- bzw. abteilungsspezifischen Übersicht genannte Verarbeitungstätigkeit müssen Sie eine detaillierte Beschreibung vornehmen. Dabei müssen für jede Verarbeitungstätigkeit Angaben zu den nachfolgenden Themen vorhanden sein.

- Name und Kontaktdaten des für die Verarbeitungstätigkeit operativ Verantwortlichen
- Ggfs. weiterer Verantwortlicher gemäß Art. 26 DS-GVO
- Bezeichnung und Zweck der Verarbeitungstätigkeit
- Ggfs. Hinweise zu weiterführenden Dokumentationen der Verarbeitungstätigkeit
- Von der Verarbeitung betroffene Personen bzw. Personengruppen
- Von der Verarbeitung betroffene Daten oder Datenkategorien
- Zugriffsberechtigte Personen, Dienstleister und ggfs. Empfänger der Daten
- Geeignete Garantien, sofern eine Übermittlung in ein Drittland erfolgt
- Dienstleister für Hosting, Wartung oder Support
- Löschung der Daten inklusive Löschfristen und deren Umsetzung
- Datenübertragung, sofern die Daten von einem Betroffenen elektronisch erhoben wurden
- Rechtsgrundlage für die Verarbeitung
- Schutzbedarf der Verarbeitung
- Risiken für die Betroffenen
- Sicherheit der Verarbeitung

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-01-01-02 DE Verarbeitungstaetigkeit 30 DS-GVO Spezifikation.
Stellen Sie die revisionssichere Archivierung der dokumentierten Verarbeitungstätigkeiten sicher.

11.3 Interne Meldung neuer Verarbeitungstätigkeiten

Aus Sicht des Datenschutzes muss sichergestellt werden, dass neue Datenverarbeitungsverfahren bzw. neue Datenverarbeitungstätigkeiten bereits in der Planungsphase datenschutzrechtlich geprüft werden. Daher sollten Sie in Ihrer Organisation einen Prozess für die Meldung von neuen Datenverarbeitungsverfahren bzw. neuer Datenverarbeitungstätigkeiten implementieren und die verantwortlichen Beschäftigten über die Notwendigkeit zur Dokumentation und Freigabe neuer Verarbeitungstätigkeiten informieren.
Die interne Meldung sollte Angaben zu den nachfolgenden Themen beinhalten.

- Name und Kontaktdaten des für die Verarbeitungstätigkeit operativ Verantwortlichen
- Bezeichnung und Zweck der Verarbeitungstätigkeit
- Von der Verarbeitung betroffene Personen bzw. Personengruppen
- Von der Verarbeitung betroffene Daten oder Datenkategorien
- Zugriffsberechtigte Personen, Dienstleister und ggfs. Empfänger der Daten
- Geeignete Garantien, sofern eine Übermittlung in ein Drittland erfolgt
- Dienstleister für Hosting, Wartung oder Support
- Löschung der Daten inklusive Löschfristen und deren Umsetzung
- Datenübertragung, sofern die Daten von einem Betroffenen elektronisch erhoben wurden
- Rechtsgrundlage für die Verarbeitung
- Schutzbedarf der Verarbeitung

- Risiken für die Betroffenen
- Sicherheit der Verarbeitung

Die interne Meldung hilft dem Datenschutzbeauftragten bei der Beurteilung der Zulässigkeit der Verarbeitungstätigkeit.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-01-02 DE Meldung neue Verarbeitungstaetigkeit.
Stellen Sie die revisionssichere Archivierung der internen Meldung neuer Verarbeitungstätigkeiten sicher.

12 Datenschutz-Folgenabschätzung

Wenn Sie Verarbeitungstätigkeiten durchführen, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben, müssen Sie ggfs. vor Aufnahme der Verarbeitung eine Datenschutz-Folgenabschätzung durchführen. Bei einer Datenschutz-Folgenabschätzung wird detailliert geprüft, ob besondere Risiken für die Schutzrechte der von der Verarbeitung personenbezogener Daten Betroffenen bestehen und welche Maßnahmen zur Minimierung der Risiken ergriffen werden können. Dies bedeutet, dass eine Datenschutz-Folgenabschätzung immer aus Sicht der Betroffenen durchzuführen ist und nicht aus Sicht Ihrer Organisation. Die Datenschutz-Folgenabschätzung sollte Angaben zu den nachfolgenden Themen beinhalten.

- Name des Erstellers der Datenschutz-Folgenabschätzung
- Datum der Erstellung
- Name der Verarbeitungstätigkeit
- Beschreibung der Verarbeitungstätigkeit
- Beschreibung der von der Verarbeitung Betroffenen
- Beschreibung der betroffenen Datenkategorien
- Besondere Risiken für die Betroffenen
- Risikoverursacher
- Maßnahmen zur Reduzierung der Risiken
- Umsetzungsmöglichkeiten der Maßnahmen vor Beginn der Verarbeitung
- Erforderlichkeit der Konsultation der zuständigen Datenschutz-Aufsichtsbehörde

Wichtig ist auch, dass die für die Verarbeitungstätigkeiten verantwortlichen Personen über die Notwendigkeit und die Maßnahmen zur Durchführung einer Datenschutz-Folgenabschätzung informiert werden.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlage 08-02-08 DE Datenschutz-Folgenabschaetzung.
Stellen Sie die revisionssichere Archivierung der durchgeführten Datenschutz-Folgenabschätzungen sicher.

13 Unternehmensspezifische Themen zum Datenschutz

13.1 Videoüberwachung

Die Videoüberwachung stellt hohe Anforderungen hinsichtlich des Datenschutzes. So dürfen öffentliche Bereiche nicht ohne weiteres überwacht werden. Daher sollte der Datenschutzbeauftragte bereits bei der Planung von Videoüberwachungsanlagen beratend hinzugezogen werden. Eine Videoüberwachung erfordert eine eindeutige Kennzeichnung der überwachten Bereiche. Das bedeutet, dass ein von der Videoüberwachung Betroffener vor Betreten eines überwachten Bereichs auf den Umstand der Überwachung hingewiesen werden muss. Hierzu müssen Sie

- Betroffene vor dem Betreten von videoüberwachten Bereichen auf diesen Umstand hinweisen
- Betroffenen eine vollständige Information über die Videoüberwachung und die damit einhergehenden Rechte der Betroffenen an zentraler Stelle zur Verfügung stellen
- Einen Lageplan erstellen, aus dem die Kamerastandorte und die überwachten Bereiche hervorgehen

Der Lageplan muss dabei nicht veröffentlich werden, er dient nur zur internen Dokumentation und als Anlage für die dokumentierte Verarbeitungstätigkeit gemäß Art. 30 Abs. 1 DS-GVO.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlagen 08-03-29-1 DE Hinweis Videoueberwachung, 08-03-29-2 DE Zuatzinfo Videoueberwachung und 08-03-29-3 DE Lageplan Videoueberwachung.

Die revisionssichere Archivierung der Dokumentation zur Videoüberwachung können Sie im Nachweis-Verzeichnis vornehmen.

13.2 Nutzung von Foto- und Filmaufnahmen

Bei der Nutzung von Foto- oder Filmaufnahmen von Beschäftigten oder Dritten ist regelmäßig zu prüfen, ob eine Einwilligung des Betroffenen notwendig ist. Generell ist von einer Pflicht zur Einholung der Einwilligung auszugehen, wenn der Betroffene im Mittelpunkt des Bildnisses ist. Bitte beachten Sie, dass Sie im Rahmen der Einwilligungseinholung einen Betroffenen umfassend darüber informieren müssen, für welche Zwecke sie die Foto- bzw. Filmaufnahmen verwenden wollen und über welche Kanäle eine Veröffentlichung erfolgen soll. Im Rahmen der Einwilligungseinholung müssen Sie auch auf das Recht der Verweigerung der Einwilligung und das Recht zum jederzeitigen Widerruf der Einwilligung hinweisen.

Bei Einsatz des IITR Compliance-Kit 2.0 verwenden Sie hierzu die Word-Vorlagen 08-03-02 DE Einwilligung Nutzung Foto und Film.
Die revisionssichere Archivierung der Dokumentation zur Nutzung von Foto- und Filmaufnahmen können Sie im Nachweis-Verzeichnis vornehmen.

Über die IITR Cert GmbH

Ralf Zlamal
Geschäftsführer
Auditor

Dr. Sebastian Kraska
Geschäftsführer
RA/Dipl.-Kfm.

IITR CERT GmbH · Marienplatz 2 · 80331 München
Auditierung und Zertifizierung
Telefon: +49 89 189 17 36 - 0
E-Mail: email@iitr.de

Herausgeber

IITR DATENSCHUTZ. RECHT. EINFACH.

Anbieter von Datenschutz-Management-Systemen
Datenschutz-Schulungen · Externe Datenschutzbeauftragte
EU-Vertreter nach Artikel 27 DSGVO

IITR Datenschutz GmbH · Eschenrieder Str. 62c · 82194 Gröbenzell
Geschäftsführer: Dr. Sebastian Kraska (auch Verantwortlicher im Sinne des Presserechts)
Registerangaben: AG München, HRB 170081

ISBN: 978-3-9816281-1-1

1. Auflage. Stand März 2022.