Risk Assessment & Datenschutz-Folgenabschätzung

Leitfaden

bitkom

Herausgeber

Bitkom e. V.
Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V.
Albrechtstraße 10 | 10117 Berlin

Ansprechpartner

Susanne Dehmel | Mitglied der Geschäftsleitung Vertrauen und Sicherheit
T 030 27576-223 | s.dehmel@bitkom.org

Verantwortliches Bitkom-Gremium

AK Datenschutz

Satz & Layout

Sabrina Flemming | Bitkom

Titelbild

© zazamaza – iStock.com

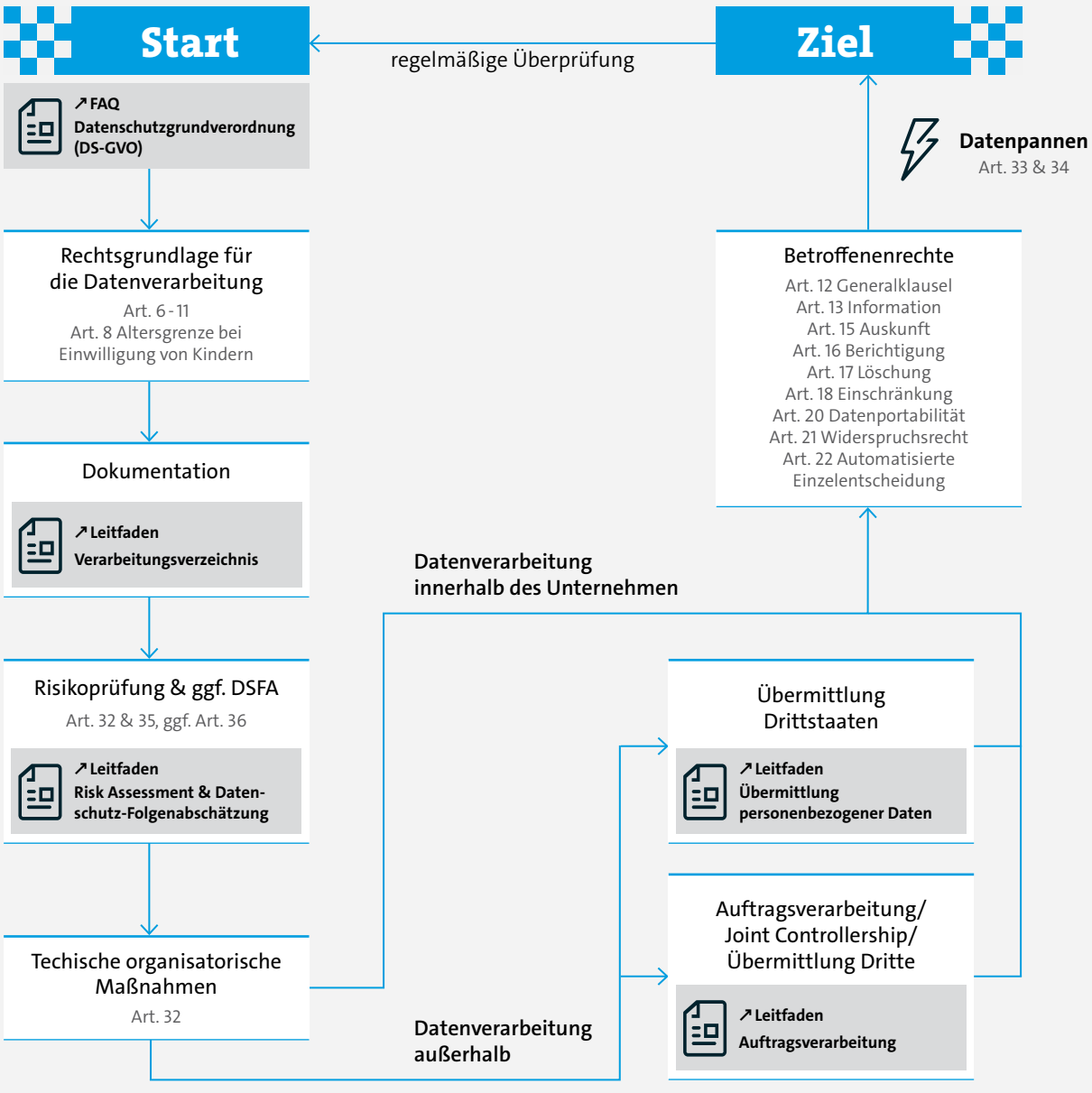
Risk Assessment & Datenschutz-Folgenabschätzung

Leitfaden

Datenschutzkonforme Datenverarbeitung

nach der EU-Datenschutz-Grundverordnung (DS-GVO)*

Art. 5 Datenschutzprinzipien & Art. 25 Datenschutz durch Technikgestaltung



*alle Artikel sind solche der DS-GVO

bitkom

Inhaltsverzeichnis

Vorwort

Mit der EU-Datenschutz-Grundverordnung gelten ab dem 25. Mai 2018 neue gesetzliche Verpflichtungen für die Gewährleistung von Datensicherheit in der Datenverarbeitung. Das übergeordnete Prinzip ist das der Rechenschaftspflicht (»Accountability«). Unternehmen müssen ihre Datenverarbeitungsprozesse nicht nur datenschutzkonform gestalten, sondern diese Konformität auch dokumentieren können. Diese Pflichten sind in der DS-GVO für bestimmte Bereiche sehr detailliert beschrieben. So implementiert Art. 32 DS-GVO einen risikobasierten Ansatz für die Umsetzung technischer und organisatorischer Maßnahmen, um Sicherheit in der Verarbeitung zu erreichen. Dies wird bedeuten, dass Unternehmen umfassende Risikobewertungen vornehmen müssen und sich die Bewertungen der IT-Sicherheit und des Datenschutzes weiter annähern. Mit der in Art. 35 DS-GVO geregelten Datenschutz-Folgenabschätzung besteht in Zukunft auch die Pflicht, umfangreiche Risikoanalysen sowie die geplanten Abhilfemaßnahmen formgerecht zu dokumentieren. Für besonders risikobehaftete Datenverarbeitungen wird eine Datenschutz-Folgenabschätzung vorgeschrieben.

Dieser Leitfaden bietet eine detaillierte Beschreibung, wie Unternehmen den Vorgaben der DS-GVO gerecht werden und ihr Risikomanagement an die DS-GVO anpassen können. Mit ausführlichen Anleitungen zur Gewährleistung von Sicherheit in der Verarbeitung und der Erstellung einer Datenschutz-Folgenabschätzung ist der Leitfaden ein wichtiges Werkzeug bei der Umsetzung der neuen Regelungen.

Besonderer Dank gilt folgenden Mitgliedern des Arbeitskreises Datenschutz, die mit ihrer Expertise und wertvollen praktischen Erfahrung ganz maßgeblich zur Entstehung des Leitfadens beigetragen haben:

- Sebastian Brüggemann, IBM Deutschland GmbH
- Rudolf Bertold Gerhard, DATEV eG
- Heiko Gossen, migosens GmbH
- Rudi Kramer, DATEV eG
- Ilona Lindemann, gkv informatik GbR
- Stephan Rehfeld, DQS GmbH und scope & focus Service-Gesellschaft mbH
- Anna Täschner, ePrivacy GmbH
- Vito Tornambé, Deutsche Post
- Marion Weimer-Hablitzel, Deutsche Post AG

Die Grafiken und Übersichten wurden von Herrn Rehfeld, Herrn Gossen und Herrn Gerhard erstellt.

Der Arbeitskreis Datenschutz besteht aus Experten der Bitkom-Mitgliedsfirmen und befasst sich mit aktuellen Themen und datenschutzspezifischen Aspekten der Informations- und Kommunikationstechnik. Ein Profil des Arbeitskreises befindet sich am Ende des Leitfadens.

Als weitere Publikationen des Arbeitskreises Datenschutz sind erhältlich:

- Grafik Datenschutzkonforme Datenverarbeitung nach der EU-Datenschutz-Grundverordnung. Stand April 2017 (Siehe Seite 2).

- FAQ – Was muss ich wissen zur EU-Datenschutz Grundverordnung? Stand September 2016. Download möglich auf Bitkom Webseite: ↗ **https://www.bitkom.org/Bitkom/Publikationen/FAQ-zur-Datenschutzgrundverordnung.html**

- Mustervertragsanlage Auftragsverarbeitung und begleitende Hinweise. Stand April 2017. Download möglich auf Bitkom Webseite: ↗ **https://www.bitkom.org/Bitkom/Publikationen/Mustervertragsanlage.html**

- Übermittlung personenbezogener Daten – Inland, EU-Länder, Drittländer. Stand 2016.* Download möglich auf Bitkom Webseite: ↗ **https://www.bitkom.org/Bitkom/Publikationen/Uebermittlung-personenbezogener-Daten-Inland-EU-Laender-Drittlaender-2.html**

- Das Verarbeitungsverzeichnis (Version 4.0). Stand Mai 2017. Download möglich auf Bitkom Webseite: ↗ **https://www.bitkom.org/Bitkom/Publikationen/Das-Verarbeitungsverzeichnis.html**

Berlin, Mai 2017

*Diese Publikation wird derzeit an die Anforderungen der Datenschutz-Grundverordnung angepasst.

1 Einleitung

1 Einleitung

Jede Datenverarbeitung im Unternehmen muss datenschutzkonform sein und jedes Unternehmen muss diese Konformität gemäß seiner Rechenschaftspflicht nachweisen können. Das in diesem Leitfaden behandelte Thema Risikomanagement/Datenschutz-Folgenabschätzung bildet eine Komponente im Gesamtkonzept der DS-GVO zur datenschutzkonformen Datenverarbeitung.

In der betrieblichen Praxis des Datenschutzbeauftragten war bisher § 9 BDSG in Verbindung mit der Anlage 1 zu § 9 Satz 1 BDSG die Grundlage für die Bewertung der technischen und organisatorischen Maßnahmen. Ferner sah § 4d BDSG unter bestimmten Voraussetzungen die Durchführung einer Vorabkontrolle vor. Beide Verpflichtungen finden sich in veränderter Form und unter teilweise geänderten Begriffen in der DS-GVO wieder. In Art. 32 DS-GVO wird nunmehr die »Sicherheit der Verarbeitung« und in Art. 35 DS-GVO die Datenschutz-Folgenabschätzung beschrieben. Beide Artikel beschreiben Verpflichtungen des Verantwortlichen, wobei Art. 32 gleichermaßen für den Auftragsverarbeiter gilt.

Im Vergleich zur bisherigen Rechtslage unter dem BDSG ändert sich die Systematik zur Bewertung von technischen und organisatorischen Maßnahmen. Gemäß Art. 32 DS-GVO ist nunmehr bei der Bewertung auf die Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen abzustellen. In vielen Unternehmen wurden zwar auch in der Vergangenheit bereits die zu implementierenden Maßnahmen unter Risikogesichtspunkten – oft in Einklang mit einem Informationssicherheitsmanagementsystem – bewertet. Jedoch herrschten auch Unsicherheiten, ob damit den gesetzlichen Anforderungen immer Genüge getan wurde, da § 9 BDSG von Erforderlichkeit, Angemessenheit und Geeignetheit sprach. Mit Blick auf Art. 32 DS-GVO wird hier nun eine Methodik zugrunde gelegt, die vielen bereits aus der klassischen Risikoanalyse und -bewertung bekannt sein dürfte.

Ähnlich der bisherigen Rechtslage müssen alle Verfahren und Systeme, die personenbezogene Daten verarbeiten, einer Risikoanalyse unterzogen werden. Dabei kann – ähnlich wie bisher in vielen Unternehmen bereits etabliert – zwischen einer »Basis-Sicherheit«, die grundsätzlich für alle Verfahren greift, und verfahrensspezifischen Maßnahmen unterschieden werden. Somit reduziert sich der Dokumentationsaufwand je Verfahren auf die Ermittlung und Beschreibung des Deltas zum Gesamt-Sicherheitskonzept.

Die Datenschutz-Folgenabschätzung (Art. 35 DS-GVO) ist das Pendant zur bisherigen Vorabkontrolle. Im Gegensatz zu § 4d BDSG ist nun nicht mehr der betriebliche Datenschutzbeauftragte zur Durchführung der Vorabkontrolle verpflichtet, sondern der Verantwortliche selbst. Waren bisher die Ausnahmen, wann eine solche Vorabkontrolle entfallen kann, im BDSG festgeschrieben, obliegt es in Zukunft den Aufsichtsbehörden in Listen aufzuführen, wann eine Datenschutz-Folgenabschätzung (DSFA) zwingend durchzuführen ist und wann diese nicht erforderlich ist. Dazwischen wird es vermutlich eine Vielzahl von Verfahren geben, die sich auf keiner der Listen wiederfinden und in denen dann nach den Voraussetzungen von Art. 35 Abs. 1 geprüft werden muss, ob eine DSFA (im engl. auch oft PIA von Privacy Impact Assessment abgekürzt) durchzuführen ist. Ähnlich der heutigen Situation ist aber davon auszugehen, dass nicht für jedes Verfahren eine DSFA durchgeführt werden muss, sondern dies eher die Ausnahme darstellt.

Daher sollten im Unternehmen entsprechende Prozesse sicherstellen, dass für alle Verfahren eine Bewertung der Risiken durchgeführt wird und in Abhängigkeit des Ergebnisses

- zusätzliche Maßnahmen nach Art. 32 DS-GVO geplant und umgesetzt werden und/oder
- eine DSFA durchgeführt wird.

Es ist zu beachten, dass die Bewertung der Sicherheit der Verarbeitung eine Untermenge der Datenschutz-Folgenabschätzung ist:

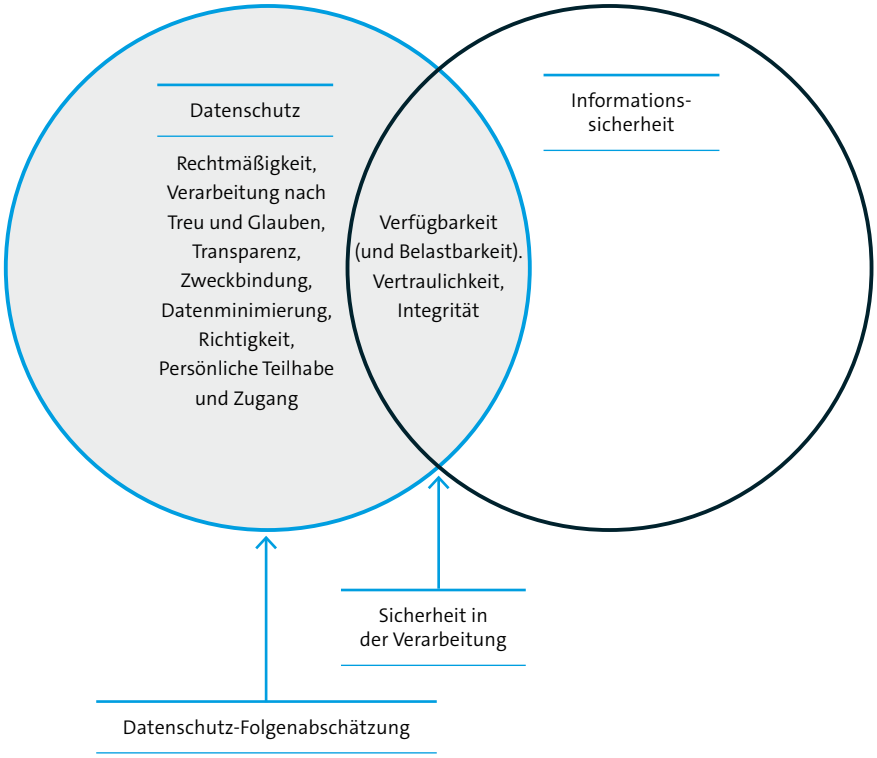


Abbildung 1: Schnittmenge Datenschutz und Informationssicherheit

Art. 32 und Art. 35 DS-GVO bauen aufeinander auf, was sich auch in der Konzeption dieses Leitfadens widerspiegelt. Die Bewertung der Sicherheit der Verarbeitung muss bei der Verarbeitung personenbezogener Daten grundsätzlich durchgeführt werden. Die Ergebnisse der Bewertung wiederum sind Bestandteil einer möglicherweise durchzuführenden Datenschutz-Folgenabschätzung.

Die folgenden Kapitel beschreiben die grundsätzlichen Anforderungen und geben Anregungen, wie diese im Unternehmen umgesetzt werden können. Dabei bleibt zu beachten, dass je nach Unternehmenssituation und Gegenstand der Verarbeitungen detailliertere oder auch weniger detaillierte Betrachtungen der Risiken erforderlich sein können. Auch kann die Form der Implementierung der Prozesse stark variieren.

2 Risikobasierter Ansatz

2 Risikobasierter Ansatz

Risiko in der DS-GVO

Obwohl der europäische Gesetzgeber immer wieder auf den Begriff des Risikos für die Rechte und Freiheiten der Betroffenen verweist, wird der Risikobegriff der DS-GVO nicht definiert. In Erwägungsgrund 75 werden lediglich die nachteiligen Folgen der Verletzung der Rechte der Freiheiten natürlicher Personen beschrieben: »Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere […], die zu einem physischen, materiellen oder immateriellen Schaden führen könnte […], erheblichen wirtschaftlichen oder gesellschaftlichen Nachteilen führen kann, wenn die betroffenen Personen um ihre Rechte und Freiheiten gebracht, […]«.

Die Art. 29-Datenschutzgruppe hat im April 2017 eine Leitlinie zur Datenschutz-Folgenabschätzung und zur Bestimmung, ob eine Verarbeitung im Sinne der Verordnung 2016/679 »wahrscheinlich mit einem hohen Risiko behaftet« sein wird, veröffentlicht und zur Kommentierung bereit gestellt (Working Paper 248).[1] Das Papier beschäftigt sich mit der Frage, wann eine Datenschutz-Folgenabschätzung durchzuführen ist und was die Bestandteile einer solchen sein sollten. Aber auch die Leitlinie definiert den Risikobegriff nicht näher.

Datenschutzrisiko im internationalen Kontext

Im europäischen Ausland und international haben sich die Aufsichtsbehörden und die ISO bereits seit Jahren mit dem Datenschutz-Risikomanagement und auch der Datenschutz-Folgenabschätzung (Privacy Impact Assessment – PIA) beschäftigt und Vorschläge zur Umsetzung erarbeitet und veröffentlicht, auf die auch in der Guideline der Art. 29-Datenschutzgruppe verwiesen wird:

Europa

- Großbritannien – ico. (2014)
  ↗ **https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf**
- Frankreich – CNIL (2015) ↗ **https://www.cnil.fr/fr/node/15798**
- Spanien – EIPD, (AGPD) (2014) ↗ **https://www.agpd.es/portalwebAGPD/canaldocumentacion/publicaciones/common/Guias/Guia_EIPD.pdf**
- Deutschland – Standard Datenschutzmodell, V 1.0 – Trial Version (2016)
  ↗ **https://www.datenschutzzentrum.de/uploads/SDM-Methodology_V1_EN1.pdf**

1 Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is »likely to result in a high risk« for the purposes of Regulation 2016/679 ↗ http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083.

Nordamerika

- Canada – OPC ↗ **https://www.priv.gc.ca/information/pia-efvp/index_e.asp**

Neuseeland

- OPC ↗ **https://www.privacy.or**

ISO

- ISO/IEC FDIS 29134 – Informationstechnik – Sicherheitsverfahren – Datenschutz-Folgenabschätzung

Die ISO stellt zusätzlich einen Katalog mit Begriffsbestimmungen zur Risikoanalyse zur Verfügung:

ISO/Guide 73:2009(en) Risk management — Vocabulary
↗ **https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en**

Ganz im Sinne eines EU-weit vereinheitlichten Datenschutzes soll auch in diesem Leitfaden auf die bereits bestehenden Arbeitsergebnisse von europäischen Aufsichtsbehörden zurückgegriffen werden und für die betriebliche Praxis unter den Maßgaben des DS-GVO erläutert. An verschiedenen Stellen werden ferner Brücken zu anderen Standards geschlagen, allen voran zum Risikomanagement nach ISO/IEC 27005:2011. Hierdurch soll eine integrierte Vorgehensweise zwischen Datenschutz und Informationssicherheit unterstützt werden. Für den Anwender ist hier auf die Arbeiten der französischen Aufsichtsbehörde (CNIL) hinzuweisen, die insb. im Bereich der Risikomethodologie ausführliche Vorarbeiten geleistet hat. Auch das Beispiel in diesem Leitfaden basiert auf der Methodologie der CNIL.

Anwender international aufgestellter Unternehmen sollten sich zur Umsetzung eines Privacy Impact Assessments mit dem Standard ISO/IEC FDIS 29134:2017[2] auseinandersetzen. In der ISO/IEC FDIS 29134:2017 wird ein Geschäftsprozessmodell für eine vollständige Datenschutz-Folgenabschätzung gegeben. Der Ansatz der ISO/IEC FDIS 29134:2017 ist kompatibel mit den Arbeiten der CNIL.

In den genannten Standards der französischen Aufsichtsbehörde und auch der International Organization for Standardization (ISO) wird nicht auf die Einbettung der Datenschutz-Folgenabschätzung in bestehende Managementsysteme oder auch eines alleinstehenden Datenschutz-Risikomanagementsystems eingegangen. Auch hier verweisen wir auf internationale Best-Practices. Praktische Hilfestellung gibt das Risikomanagementrahmenwerk der ISO 31000:2011.

2 Aktuell liegt dieser Standard als FDIS vor und ist kurz vor der internationalen Verabschiedung.

3 Voraussetzung zur Umsetzung der Art. 32 und 35 DS-GVO: das Verarbeitungsverzeichnis

3 Voraussetzung zur Umsetzung der Art. 32 und 35 DS-GVO: das Verarbeitungsverzeichnis

Obwohl ein Verarbeitungsverzeichnis laut DS-GVO erst ab 250 Mitarbeitern geführt werden muss, ist es als Ordnungskriterium unverzichtbar. Nach Auffassung der Autoren ist eine Strukturierung von Unternehmen anhand von definierten Verarbeitungstätigkeiten oder Verfahren sinnvoll, um die Verpflichtungen der DS-GVO in bearbeitbare Portionen zu zerlegen und nachvollziehbar zu dokumentieren.

Dieser Leitfaden baut in weiten Teilen darauf auf, dass im Unternehmen ein Verarbeitungsverzeichnis bzw. ein »Verzeichnis von Verarbeitungstätigkeiten« vorhanden ist oder zumindest eine Strukturierung oder Gruppierung von Verarbeitungstätigkeiten anhand von Prozessen, Geschäftsvorfällen oder Verarbeitungstätigkeiten stattgefunden hat. Wie eine solche Strukturierung sinnvoll erfolgen kann, wird im **↗ Leitfaden »Verarbeitungsverzeichnis«** beschrieben, auf den an dieser Stelle verwiesen wird.

> Ein Verarbeitungsverzeichnis ist die Grundlage zur Umsetzung des Art.32 und der Art.35 und 36 DS-GVO. Ohne dieses Hilfsmittel wird fast jede Datenschutz-Risikobeurteilung an der betrieblichen Komplexität scheitern.

Die mögliche Umsetzung der Art.32 und der Art. 35 und 36 sollen anhand des Geschäftsprozesses der Fakturierung illustriert werden. Hierzu empfiehlt es sich das Verfahren zu beschreiben:

Beispiel zu den allgemeinen Verfahrensangaben

Name des Verfahrens	Fakturierung
Zweck der Verarbeitung personenbezogener Daten	Erstellung von Angeboten und Rechnungen, Schnittstelle zur FiBu
Interessierte Parteien	Interessenten, Kunden, verantwortliche Stelle
Verantwortliche Stelle	Mustermann Marketing GmbH Eckstr. 5 60437 Frankfurt

Es ist zu beachten, dass die oben genannten Angaben zum Verfahren um die interessierten Parteien ergänzt sind. Datenschutz ist Grundrechtsschutz. Eine Beurteilung der Datenschutzfolgen kann also nur aus Sicht des Betroffenen erfolgen. Unabhängig davon empfiehlt es sich aber auch den Sichtwinkel der anderen interessierten Parteien einzunehmen, bzw. sofern diese bereits im Rahmen eines Risikomanagements betrachtet wurden, diese ggfs. zu zusammenzuführen. Hierdurch können in der Regel Synergien geschaffen werden.

Beispiel zur Dokumentation der Betroffenen, Daten oder Datenkategorien und Aufbewahrungsfristen

Betroffener	Kreditor, Debitor	Mitarbeiter
Kategorien personenbezogener Daten	Name, Firma, Adressdaten, Rechnungsdaten, Kontodaten	Protokolldaten
Personenbezogene Daten		User-ID, Tätigkeit / Aktion, Datum, Uhrzeit
Empfänger der personenbezogenen Daten	Intern: Sachbearbeiter, Geschäftsleitung, Vorgesetzte	Intern: Geschäftsleitung, Leiter Rechnungswesen
Zugriff auf personenbezogene Daten	Auftragnehmer: Wartungstechniker, Datenträgervernichter	Auftragnehmer: Wartungstechniker, Datenträgervernichter
Aufbewahrungsfrist	Angebote, abgelehnt: sofort Angebote, angenommen: 6 Jahre Rechnungen: 10 Jahre Steuerrelevante E-Mails: 10 Jahre	Protokolle: Vernichtung nach Aufgabenerfüllung, 3 Tage

Hinweis

Hier handelt es sich nur um einen Teil der Gesamtverfahrensdokumentation, die im Leitfaden Verarbeitungsverzeichnis des Bitkom näher dargestellt ist.

4 Sicherheit der Verarbeitung (Art. 32 DS-GVO)

4 Sicherheit der Verarbeitung (Art. 32 DS-GVO)

Bei der Verarbeitung personenbezogener Daten müssen der Verantwortliche und der Auftragsverarbeiter für die personenbezogenen Daten von natürlichen Personen ein angemessenes Schutzniveau umsetzen und die Wirksamkeit der getroffenen Maßnahmen nachweisen. Im Folgenden wird beschrieben, wie das angemessene Schutzniveau identifiziert und im Rahmen eines Managementsystems umgesetzt und gehalten werden kann.

4.1 Angemessene Sicherheitsmaßnahmen

In Art. 32 DS-GVO werden die Anforderungen an die Sicherheit der Verarbeitung definiert. Im Gegensatz zur Rechtslage bis Mai 2018 ist die Systematik zur Ermittlung geeigneter technischer und organisatorischer Maßnahmen nun explizit auf eine Bewertung anhand der ermittelten Risiken ausgerichtet. Eine Bewertung und Ableitung von Maßnahmen anhand von Risiken ist in vielen Unternehmen keine neue Methode, bspw. haben viele Unternehmen bereits ein Risikomanagement für Informationssicherheitsrisiken. Jedoch unterscheidet sich der Ansatz in der DS-GVO etwas von der reinen Betrachtung aus der Perspektive der Informationssicherheit.

Art. 32 Abs. 1 verlangt vom Verantwortlichen und vom Auftragsverarbeiter, dass zum Schutz personenbezogener Daten angemessene Sicherheitsmaßnahmen ergriffen werden müssen:

> »Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;«

Die Risikoorientierung bei der Auswahl von Informationssicherheitsmaßnahmen ist nicht neu, im Bundesdatenschutzgesetz (BDSG) wurde sie in § 9 Satz 2 als Verhältnismäßigkeit der technisch-organisatorischen Maßnahmen bezeichnet.

> »Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.«

Die nunmehr sehr klare Beschreibung der anzuwendenden Methode (Risikoorientierung) legt einen Vergleich mit internationalen Standards für Managementsysteme nahe. Im Datenschutz und der Informationssicherheit nutzen wir zur Beurteilung der Sicherheit von personenbezogenen Daten und der Sicherheit von Informationen die identischen Prinzipien, bewerten aber aus unterschiedlichen Perspektiven:

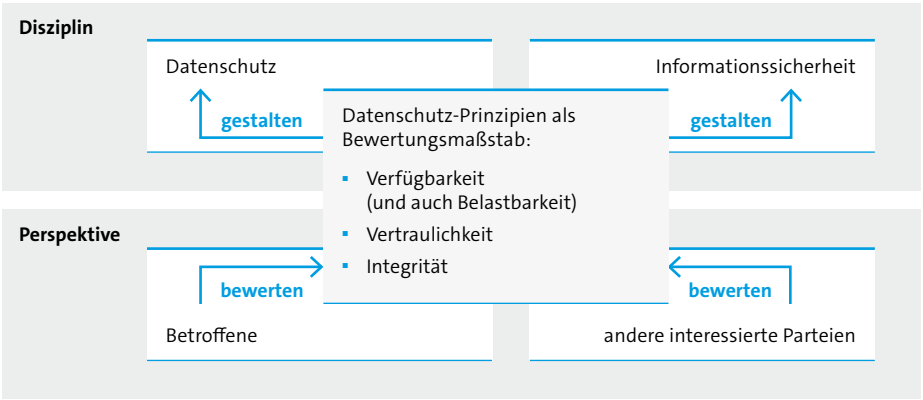


Abbildung 2: Perspektive der Informationssicherheit und des Datenschutzes

Wegen des unterschiedlichen Blickwinkels können die Ergebnisse aus der Informationssicherheit für den technischen Datenschutz nicht einfach übernommen werden, sofern die Risiken für die Freiheiten und Rechte der Betroffenen nicht bereits in der vorhandenen Methodik ausreichend berücksichtigt wurden. Die Ergebnisse der Datenschutz- und der Informationssicherheits-Risikobewertung können zufällig identisch, müssen es aber nicht zwangsläufig sein.

Beispiel Bewerberdatenbank

Ein Unternehmen setzt ein Online-Bewerbungsportal ein, an dem Bewerber sich registrieren und ihre Bewerberdaten einpflegen und aktualisieren können. Das Authentisierungsverfahren ist jedoch schwach, da der Benutzername der E-Mailadresse des Bewerbers entspricht und keine Anforderungen an die Länge und Komplexität des Passworts existieren.

Eine reine Schadens-Betrachtung aus Unternehmenssicht wird das Risiko eines Vertraulichkeitsverlusts (bspw. durch einen gehackten Bewerber-Account) ggfs. als gering einstufen, da für das Unternehmen kein unmittelbarer Schaden entsteht. Mit Blick auf die Verpflichtung aus Art. 32 DS-GVO wird nun aber auch der potentielle Schaden für den Betroffenen mit zu berücksichtigen sein, bspw. ein wirtschaftlicher Schaden der ihm droht, da der Umstand seiner Bewerbung einschl. aller Bewerbungsunterlagen nun öffentlich bekannt wird. Dies kann somit durchaus zu einem veränderten Ergebnis der Risikobewertung führen und somit auch weitere Maßnahmen der Risikobehandlung erforderlich machen.

4.2 Umsetzung des Schutzniveaus mit Hilfe eines Managementsystems

Der Europäische Gesetzgeber beschreibt in Art. 32 Abs. 1 lit. d) der Verordnung die Anforderungen an die Überwachung der technischen und organisatorischen Maßnahmen, die für (Informationssicherheits-) Managementsysteme (ISMS) bereits seit Jahren praktiziert werden: »ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung«.

Dieser recht unscheinbare Satz verpflichtet Unternehmen nun, entsprechende Prozesse ein- und regelmäßig durchzuführen. Aber auch hier bieten sich wieder sinnvolle Synergien mit dem Informationssicherheits-Management an.

1. Als Motor des Management-Systems wird der PDCA-Zyklus eingesetzt.
2. Es werden die Phasen des Risiko-Assessments, der Erstellung und Umsetzung eines Risikobehandlungsplanes, interne Audits, Managementbewertung und Ergreifen von Korrekturmaßnahmen vorgeschrieben.

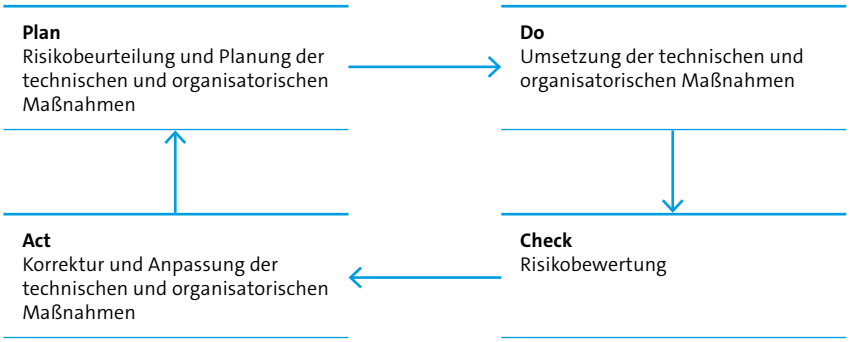


Abbildung 3: PDCA Zyklus

Aufgrund der systematischen Nähe zu dem internationalen Standard DIN ISO/IEC 27001:2015, der die Anforderungen an ein Informationssicherheitsmanagementsystem beschreibt, sowie der thematischen Nähe der Sicherheitsanforderungen an die Verarbeitung personenbezogener Daten zu den grundlegenden Sicherheitsanforderungen eines Unternehmens an die Verarbeitung sämtlicher Informationen, bietet sich eine prozessuale und methodische Verschmelzung der beiden Themenkomplexe an. Dies schafft nicht nur erhebliche Synergien bei der Bewertung und Umsetzung von Maßnahmen, es erhöht auch die Akzeptanz der Anforderungen im Unternehmen.

Gegenüberstellung der Anforderungen DIN ISO/IEC 27001:2015 und DS-GVO

Phase in einem ISMS	Art. 32 Abs. 1, 2 DS-GVO
Risikobeurteilung Es sind geeignete technische und organisatorische Maßnahmen zu treffen Einbeziehung: ▪ Stand der Technik ▪ Implementierungskosten ▪ Art, Umfang, Umstände, Zwecke der Verarbeitung Beurteilungsmaßstab (Schutzziele): ▪ Vertraulichkeit ▪ Integrität ▪ Verfügbarkeit	»Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten;« (Art. 32 Abs. 1 S. 1 DS-GVO) »Bei der Beurteilung des angemessenen Schutzniveaus sind insbesondere die Risiken zu berücksichtigen, die mit der Verarbeitung – insbesondere durch Vernichtung, Verlust oder Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder unbefugte Offenlegung von beziehungsweise unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden – verbunden sind.« (Art.32 Abs. 2 DS-GVO)
Es soll ein Maßnahmenkatalog erstellt werden, der mindestens erfüllt: ▪ Pseudonymisierung ▪ Verschlüsselung ▪ Vertraulichkeit, ▪ Integrität ▪ Verfügbarkeit ▪ schnelles BCM	»diese Maßnahmen schließen unter anderem Folgendes ein: a) die Pseudonymisierung und Verschlüsselung personenbezogener Daten; b) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen; c) die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;« (Art.32 Ab. 1 S. 2 lit. a) – c) DS-GVO)
internen Audits und Managementbewertung und Verfahren zur Korrektur/Anpassung von ergriffenen Maßnahmen.	»diese Maßnahmen schließen unter anderem Folgendes ein: a) ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.« (Art. 32 Abs. 1 S. 2 lit. d) DS-GVO)

4.3 Methoden der ISO 27001 als Best-Practice

Der Nachweis über die Einhaltung eines angemessenen Schutzniveaus lässt sich durch verschiedene Dokumentationen erbringen, die üblicherweise mit einem ISMS nach ISO 27001 einhergehen:

- Übersicht der Werte (personenbezogene Daten/Informationen und alles, womit diese verarbeitet werden oder hierfür erforderlich ist) – dies kann aus Datenschutzsicht bspw. die Verarbeitungsübersicht/das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DS-GVO darstellen/beinhalten (siehe ↗ **Leitfaden »Verarbeitungsverzeichnis«**)
- Technik zur Risikobewertung festlegen
- Risikomanagementprozess
- Risikoidentifikation, Risikoanalyse und Risikobewertung,
- Maßnahmenplan,
- Risiko-Behandlungsplan
- internes Auditprogramm und Auditberichte (einschl. der Nachhaltung von Korrekturmaßnahmen)
- Managementreview bzw. Bericht an die Unternehmensführung
- Weitere Dokumentationen wie Gesprächs-Protokolle aus Gremien-Sitzungen, Wirksamkeitsprüfungen, interne Richtlinien und Vorgaben, Schulungsnachweise etc.

Die im Folgenden dargestellte Vorgehensweise stellt eine Möglichkeit dar, wie ein Risikomanagementprozess in der Praxis aussehen kann.

4.4 Vorüberlegungen zur Umsetzung der »Sicherheit der Verarbeitung«

Organisationen sollten bis Mai 2018 ein Datenschutz-Risiko-Management eingeführt und für die einzelnen Geschäftsprozesse durchlaufen haben.

Zur Vorbereitung sollten zwei wichtige Überlegungen angestellt und entschieden werden:

- Woran richtet man die Risikobewertung aus?
- Wie werden Risiken beurteilt (Technik der Risikobewertung)?

Ersteres ist wichtig, um die Risiken nach einem bestimmten System erfassen und zuordnen zu können. In der Informationssicherheit werden die Risiken i.d.R. an den (Informations-) Werten (Assets)- vgl. bspw. DIN ISO/IEC 27001:2015) ausgerichtet, wobei diese sehr unterschiedlich defi-

niert werden können. Nimmt man eine rein datenschutzrechtlich orientierte Risikoermittlung vor, bietet sich eine Bewertung der Risiken für personenbezogene Daten gruppiert nach Verfahren an. In diesem Leitfaden werden Verfahren mit Geschäftsprozessen gleichgesetzt. Abhängig von der erforderlichen Detaillierung können Verfahren ganze Geschäftsprozesse oder Teilprozesse sein.

Bei einer integrierten Betrachtung ist zumindest eine Referenzierung zu den zugehörigen Verfahren sinnvoll. Weiterhin können Gruppen von Verfahren/Assets zusammengefasst werden bzw. ein zweistufiges Modell sinnvoll sein. In einem zweistufigen Modell erfasst und bewertet man erstmal die übergreifenden Datenschutzrisiken für die gesamte Verarbeitung und legt ein Basis-Sicherheitsniveau fest. Im zweiten Schritt prüft man dann je Verfahren/Asset, ob besondere Datenschutzrisiken bestehen und somit für einzelne Verfahren höhere Anforderungen bestehen bzw. für ein Verfahren weitere Maßnahmen erforderlich sind.

Neben dieser grundsätzlichen Strukturierung ist es wichtig eine Technik zur Risikobewertung zu definieren. Diese stellt üblicherweise nicht nur sicher, dass die Bedrohungen und Risiken nach einer gewissen Systematik betrachtet/ermittelt werden, sie sorgt auch für einen Bewertungsmaßstab. Dieser ist wiederum nicht nur für die Personen hilfreich, die die Bewertung erstmalig durchführen müssen, sondern schafft auch eine gewisse Nachvollziehbarkeit und Reproduzierbarkeit. Erst damit werden die ermittelten Risiken einschließlich der abgeleiteten Maßnahmen rechenschaftsfähig (Art. 5 Abs. 1 lit. f). i.V.m. Abs. 2 DS-GVO).

4.4.1 Der Datenschutz-Risikoprozess

Risikoprozesse sind prinzipiell sehr ähnlich gestaltet. Ein Datenschutz-Risikoprozess kann wie folgt aussehen:

- »Erstellung des Kontextes« oder auch »Anwendungsbereich festlegen«
- Risiken identifizieren
- Risiken analysieren
- Risiken bewerten
- Risiken bewältigen
- Risiken überwachen

Diese sechs Schritte des Risikomanagements können in der Praxis vom Umfang und der Methode sehr unterschiedlich umgesetzt werden. Zum Beispiel schreibt der Gesetzgeber in der DS-GVO keine Methode zur Risikoanalyse zwingend vor. So können zur Bestimmung der Maßnahmen zur Einhaltung eines angemessenen Schutzniveaus quantitative, qualitative Methoden oder auch Mischformen eingesetzt werden. Auch wenn in diesem Leitfaden nur eine Methode zur Risikoanalyse angewendet wird, bedeutet dies nicht, dass andere Methoden der Risikoanalyse vom Gesetzgeber nicht zugelassen sind.

4.4.2 Methode zur Risikoanalyse

Bei einer klassischen Risikoanalyse im Bereich der Informationssicherheit werden die Risiken aus der Sicht eines möglichen Schadens für das jeweilige Unternehmen vorgenommen. Eine Erweiterung um Risikobetrachtung gemäß DS-GVO eines bestehenden Risikoprozesses ist möglich, allerdings muss eine Bewertung der Höhe eines Datenschutzrisikos aus Sicht des Betroffenen erfolgen. Daher wurde der Verfahrensbeschreibung bereits eine weitere Perspektive interessierter Parteien hinzugefügt. Eine Erweiterung des internen und externen Kontextes ist erforderlich, damit auch die relevanten Risikokriterien zur Bestimmung der Risikohöhe angewendet werden.

Die Wahrscheinlichkeit in der Informationssicherheit wird häufig als eine Funktion der Bedrohungen des Systems, der ausnutzbaren Schwachstellen und der Konsequenzen der Ausnutzung dieser Schwachstellen dargestellt. Es wird in dieser Funktion also auf Systemschwächen abgestellt.

Davon zu unterscheiden ist die Bewertung des Niveaus von Datenschutzrisiken. Das Niveau von Datenschutzrisiken kann berechnet werden als:

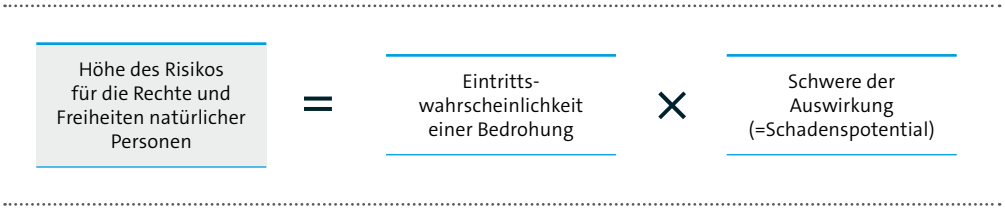


Abbildung 4: Risikohöhe

Obwohl es primär die natürlichen Personen zu schützen gilt, die durch den Schutz ihrer Daten (personenbezogene Daten) geschützt werden sollen, ist dies nur teilweise durch Informationssicherheitsmaßnahmen möglich. Stattdessen können zunächst nur die sogenannten unterstützenden Werte, also Hard-, Software oder Netzwerkkomponenten geschützt werden.

Personenbezogene Daten = primäre Werte

Kategorien von unterstützenden Werten können sein:[3]

- Hard- und Software von Benutzern
- Hardware
- Software
- Datenübertragungskanäle
- Individuen
- Papier-Dokumente
- Übertragungswege für Papier-Dokumente

3 ISO/IEC FDIS 29134:2017, Annex B.

Risikoquellen (Menschen oder auch Natur) führen Aktionen gegen unterstützende Werte aus. Diese Aktionen wiederum können zu Datenschutzverletzungen führen. Das konkrete Szenario wird als Bedrohung bezeichnet.

Beispiel:
Szenario: Ein Mitarbeiter (Risikoquelle) nutzt Hardware, auf der personenbezogene Daten verarbeitet werden (unterstützender Wert) entgegen der bestimmten Nutzung (Aktion). Dadurch gehen personenbezogene Daten verloren (Datenschutzrisiko).

Konkrete Bedrohung: Ein Mitarbeiter nutzt Unternehmenshardware für persönliche Zwecke

4.5 Umsetzung der »Sicherheit der Verarbeitung«

4.5.1 Erster Schritt: Einbindung des obersten Managements

Die Einbindung des obersten Managements (bspw. Geschäftsführung, Vorstand) ist unabdingbar. Neben den Ergebnissen der Risikobeurteilung sollte auch die Risikobehandlung (insbesondere die Risikoakzeptanz) mit der obersten Leitung abgestimmt sein bzw. bestätigt werden. Dies dient auch regelmäßig der Entlastung der übrigen Mitarbeiter. Aber auch die Ergebnisse der internen Audits sollten dem Management regelmäßig berichtet werden.

Zur Umsetzung der Rechenschaftspflichten gemäß Art. 5 DS-GVO empfehlen sich im Weiteren regelmäßig Gesprächsprotokolle aus Gremien-Sitzungen, Wirksamkeitsprüfungen, interne Richtlinien und Vorgaben sowie Schulungsnachweise systematisch und zentral zu dokumentieren.

4.5.2 Zweiter Schritt: Festlegung der Verantwortlichkeiten

Um eine Datenschutz-Risikobeurteilung umsetzen zu können, muss ein entsprechendes Projektteam von der Leitung der Organisation mit den erforderlichen Kompetenzen und Ressourcen ausgestattet werden. Nur wenn die Organisationsleitung sich zur Umsetzung einer Datenschutz-Risikobeurteilung bekennt, kann die Einführung erfolgreich verlaufen.

Operativ kann dies bspw. durch die Verabschiedung einer Richtlinie Risikomanagement erfolgen, die definiert

- wer ist für die Durchführung der Datenschutz-Risikobeurteilung (Sicherheit der Verarbeitung und Datenschutz-Folgenabschätzung) verantwortlich,

- wer liefert Informationen und bewertet die Datenschutzrisiken,
- wie wird der Verantwortliche für Datenschutzrisiken ermittelt,
- wie oft wird der Geschäftsprozess durchgeführt,
- wie sieht die Technik zur Risikobewertung aus,
- welche anwendbaren Behandlungsoptionen gibt es und
- was passiert mit den Ergebnissen der Analyse der Sicherheit der Verarbeitung und der Datenschutz-Folgenabschätzung.

4.5.3 Dritter Schritt: Internen und externen Kontext festlegen

Bei der Betrachtung der Risiken für die beteiligten Kategorien von Betroffenen sind vor der Risikobeurteilung relevante Datenschutzanforderungen (sog. interner und externer Kontext) zu identifizieren und bei der Risikobewertung zu berücksichtigen.

Datenschutzanforderungen können zum Beispiel erwachsen aus:[4]

- Anforderungen aus internationalem oder nationalem Gesetz
- Gerichtsentscheidungen
- Verordnungen
- Vertragliche Vereinbarungen (zum Beispiel Auftragsverarbeitungen)
- Geschäftsanforderungen (zum Beispiel Codes of Conduct, Industrie-Standards)
- Internes Kontrollsystem (IKS)

Abbildung 5: Datenschutzanforderungen aus ISO/IEC 29100:2011

4 Weitere Hinweise: ISO/IEC 29100:2011, Seite 11.

4.5.4 Vierter Schritt: Anwendungsbereich der Analyse der »Sicherheit der Verarbeitung« festlegen (scoping)

In einem ersten Schritt muss bestimmt werden, für welchen Anwendungsbereich eine Risikobeurteilung gilt.

Gegenstände einer Risikobeurteilung können prinzipiell sein:

- Geschäftsprozesse
- einmalige Aktionen oder Vorhaben der verantwortlichen Stelle oder
- die EDV-Infrastruktur (Software, Hardware oder Netzwerk).

Hier bietet sich an, als grundlegende Einteilung auf ein etwaig bereits vorhandenes Verarbeitungsverzeichnis zurückzugreifen. Die Granularität des Verarbeitungsverzeichnisses bestimmt sich nach praktischen Aspekten, zum Beispiel den Anforderungen von Auftraggebern im Rahmen von Auftragsverarbeitungen (siehe **↗ Leitfaden »Verarbeitungsverzeichnis«**). In der weiteren Betrachtung wird beispielhaft die Ausrichtung an einem Verfahren vorgenommen.

4.5.5 Fünfter Schritt: Identifikation der Datenschutzrisiken

Zu betrachtende Datenschutzziele

In Art. 32 DS-GVO werden lediglich drei (vier) Datenschutzziele betrachtet:

- Verfügbarkeit (Belastbarkeit),
- Vertraulichkeit und,
- Integrität

Im Rahmen einer datenschutzrechtlichen Risikobeurteilung wird in der Sicherheit der Verarbeitung nur betrachtet, welche Risiken eine Verletzung dieser Datenschutzziele für die Betroffenen nach sich zieht.

Der Verantwortliche oder der Auftragsverarbeiter muss die Datenschutzrisiken identifizieren, die bei der Datenverarbeitung in dem Verfahren drohen. Zur Identifizierung von Risiken sollten in den folgenden Schritten Risikoquellen, Werte (auch Informationen, personenbezogene Daten, Systeme etc.), Bedrohungen und Schwachstellen, sowie mögliche Auswirkungen und Datenschutz-Risiken identifiziert werden. Auch hierbei sind Betrachtungen von Gruppen bzw. die Zusammenfassung von ähnlichen Werten sinnvoll. Eine mögliche Herangehensweise ist, anhand von Werten die zutreffenden Datenschutzrisiken abzuleiten und daraus die möglichen Bedrohungen zu betrachten. Diese Betrachtung kann z. B. in Interview-Form mit relevanten Verantwortlichen durchgeführt werden, als auch in Form von Workshops oder einem Brainstorming.

4.5.6 Sechster Schritt: Risikoanalyse

Zuerst werden die bestehenden Maßnahmen zur Vermeidung der Verletzung der Vertraulichkeit, Verfügbarkeit oder Integrität identifiziert und dokumentiert.

Ob und inwieweit man für ein Unternehmen bereits eine Betrachtung eines Basis-Sicherheitsniveaus (im Sinne eines zweistufigen Modells) oder ein Verfahren isoliert betrachtet, ist für die grundsätzliche Methode unerheblich.

Beispiel zweistufige Risikobetrachtung:

Ein produzierendes, mittelständiges Unternehmen betreibt seine IT vollständig selbst auf internen Servern. Das Unternehmen ist ausschließlich im B2B-Umfeld tätig und neben den geschäftlichen Kontaktdaten der Kunden und Interessenten beschränkt sich die Verarbeitung personenbezogener Daten auf Mitarbeiterdaten. Nach einem Maximums-Prinzip erfolgt daher für die bekannten Verfahren anhand der Datenarten, Betroffenenkategorien und Datenmengen eine Risikobeurteilung für die gesamte IT- und Geschäftsumgebung. Für die bekannten Verfahren erfolgt daher anhand der personenbezogenen Daten und/oder Kategorien personenbezogener Daten und den dazugehörigen Betroffenen oder Kategorien von Betroffenen eine Risikobeurteilung für die verantwortliche Stelle. Bei der Risikobewertung ist für jedes Datenschutzziel aus der Informationssicherheit das Maximalprinzip anzuwenden.

Nun wird im Rahmen der Risikobewertung festgestellt, dass das betriebliche Wiedereingliederungsmanagement nach § 84 Abs. 2 SGB IX weitaus sensiblere Datenkategorien (Gesundheitsdaten der Mitarbeiter) verarbeitet und daher die Basis-Risikobeurteilung nicht ausreicht. Daher werden nun in einer zweiten Stufe die besonderen Risiken für die Betroffenen für dieses Verfahren betrachtet und beurteilt, ob weitere Maßnahmen erforderlich sind.

Weitere Auslöser für eine gesonderte Betrachtung könnten bspw. die Nutzung von Cloud-Services für einzelne Verfahren, der Zugriff durch Dritte auf Daten, Einbindung von Dienstleistern in Drittstaaten usw. sein.

Bedrohungen und Risikoquellen

In diesem Schritt werden die Bedrohungen und die dazugehörigen Risikoquellen (Auslöser einer Bedrohung) bestimmt.

Typen von Risikoquellen können interne, externe oder auch sonstige Quellen (Feuer, Wasser, Naturkatastrophen) sein. Zur Bewertung einer Risikoquelle kann es hilfreich sein, die Motivation von Externen oder Internen zu kennen.

Folgende Aufzeichnungen sollten geführt werden:

- Risikoquelle (Typ)
- Motivation

Im Weiteren werden nun Bedrohungen identifiziert und den Risikoquellen zugeordnet. Diese Informationen werden in einer Liste geführt.

Beispiel für die Identifikation und Dokumentation von Risikoquellen

Risikoquellen (Typ)			Relevante Risikoquellen	Beschreibung der Potenz der Risikoquellen
Menschliche Risikoquellen	intern	unbeabsichtigt	Mitarbeiter, Vorgesetzte	Relevante Risikoquellen verwenden keine Ressourcen auf versehentliche Aktionen.
		vorsätzlich		Relevante Risikoquellen verwenden minimale Ressourcen auf vorsätzliche Aktionen (z. B. bei Kündigung oder Abmahnungen).
	extern	unbeabsichtigt	Wartungspersonal, Mitbewerber, Hacker	Relevante Risikoquellen verwenden keine Ressourcen auf versehentliche Aktionen.
		vorsätzlich		
Nichtmenschliche Risikoquellen	intern		Wasserschaden durch Rohrbruch, Feuer	Wasserschaden durch Rohrbruch und Feuer traten in den letzten 15 Jahren Betriebstätigkeit nicht auf.
	extern		Stromausfall, Ausfall der Internet-Leitung	Ausfall der Internet-Leitung und Stromausfall treten regelmäßig auf, die Betriebsunterbrechungen sind aber bisher nicht relevant gewesen.

Auswirkungen bei Verletzung der drei Datenschutzziele

Die folgenden drei Auswirkungen sollen nun genauer betrachtet werden:

- Illegaler Zugriff auf personenbezogene Daten
- Ungewollte Modifikation von personenbezogenen Daten
- Verlust von personenbezogenen Daten

Nun sollen den Ereignissen mögliche Auswirkungen bei Eintritt und die entsprechenden Risikoquellen zugeordnet werden.

Beispiel für die Dokumentation und Bewertung von Ereignissen

Ereignis (potentielle Datenschutzvorfälle)	Risikoquelle	Folge des Eintritts des (unerwünschten) Ereignisses	Mögliche Auswirkungen für die interessierten Parteien
Unbefugter Zugriff auf personenbezogene Daten (Vertraulichkeit)	Mitarbeiter, Vorgesetzter, Wartungspersonal	▪ Keine ▪ Weiterverteilung ▪ Nutzung der personen-bezogenen Daten	Offenbarung von Zahlungsdaten (Bankdaten) von Kreditoren und daraus resultierende monetäre Schäden bei Missbrauch (Schadensersatz).
Unerwünschte Verände-rung von personenbezo-genen Daten (Integrität)	Mitarbeiter, Vorgesetzter, Wartungspersonal	▪ Fehlfunktion im Verfahren	Liquiditätsprobleme der Organisation
Verlust personenbezoge-ner Daten (Verfügbarkeit)	Mitarbeiter, Vorge-setzter, Wartungs-personal, Schadcode, Wasserschaden, Feuer	▪ Fehlfunktion im Verfahren ▪ Störung im Ver-fahren	Liquiditätsprobleme der Organisation

Identifikation relevanter Bedrohungen

Die relevanten Risikoquellen wurden bereits identifiziert. Auf unterstützende Werte können nun die folgenden Aktionen wirken:

- Unangemessener Gebrauch
- Überwachung
- Überlastung
- Manipulation
- Beschädigung
- Veränderung
- Verlust

Eine Übersicht der daraus resultierenden Bedrohungen im Datenschutz können dem Anhang B der ISO/IEC FDIS 29134:2017 oder der »Knowledge base: Typology of threats« der CNIL[5] entnommen werden.

5 CNIL, PIA Manual 2 – Privacy Impact Assessment (PIA) – Tools (templates and knowledge bases), 2015, S.18 ff.

Einschätzung der Schwere der Auswirkung

Die Auswirkungen bei der Realisierung eines Risikos werden zum Beispiel zunächst in vier Risiko-Niveaus eingestuft:

1. Vernachlässigbar
2. Eingeschränkt
3. Signifikant
4. Maximal

»Die Risiken für die Rechte und Freiheiten natürlicher Personen – mit unterschiedlicher Eintrittswahrscheinlichkeit und Schwere – können aus einer Verarbeitung personenbezogener Daten hervorgehen, die zu einem

- physischen,
- materiellen oder
- immateriellen

Schaden führen«[6].

Für jedes Risiko-Niveau können nun je Schadenart Kriterien und Beispiele definiert werden, die eine Einstufung ermöglichen und bei einer erneuten Durchführung einer Risikobeurteilung zum identischen Ergebnis führen.

Damit die Ergebnisse der Risikobeurteilung wiederholbar sind, bietet es sich an, eine Einstufungstabelle zur Einschätzung der Schwere von Auswirkungen zu erstellen und im Unternehmen immer wieder zu verwenden. Ein Beispiel einer solchen Einstufungstabelle kann im Anhang »Einstufungstabelle« eingesehen werden. Dieser Vorschlag für eine Einstufungstabelle stammte von der CNIL.[7]

Diese Kategorien können ggfs. mit vorhandenen Kategorien und deren Kriterien abgestimmt und angepasst werden. Hier hat der Gesetzgeber den Unternehmen ausreichend Freiheiten gelassen, um die Methode der Unternehmenssituation angemessen selber festlegen zu können. Die Wahl von vier Stufen für die Bewertung der Auswirkung und der Eintrittswahrscheinlichkeit ist oft vorzufinden, kann aber in Abhängigkeit der Geschäftsfeldes eines Unternehmens, der Komplexität der Prozesse oder Systeme und vieler weiterer Faktoren auch anders gewählt werden.

6 Erwägungsgrund 75.

7 CNIL, PIA Manual 2 - Privacy Impact Assessment (PIA) – Tools (templates and knowledge bases), 2015, S.13 ff.

Beispiele zur Einschätzung der Auswirkungen aus Sicht verschiedener interessierter Parteien

Erster Business Case: Geschäftsprozess »Produktion«

Szenario: Ein Unternehmen betreibt eine Produktion eines Wirtschaftsgutes. Im Produktionsprozess fallen wenige personenbezogene Daten an. Es werden in der Produktion Protokolle angefertigt, damit nachvollzogen werden kann, welcher Mitarbeiter zu welchem Zeitpunkt in der Produktion beschäftigt war.

Bewertung: Zum Beispiel ein Verlust dieser Protokolle hat aus Sicht des Betroffenen eine »vernachlässigbare« Auswirkung auf seine Rechte und Freiheiten.

Zweiter Business Case: Geschäftsprozess »internes Audit«

Szenario: Um ein internes Audit durchführen zu können, muss ein interner Auditor ein Mindestmaß an personenbezogenen Daten aufnehmen, zum Beispiel Beteiligte, Verantwortlichkeiten/Rollen.

Bewertung: Bei der Offenbarung eines Protokolls/Berichts eines internen Audits ist dies aus Sicht des Betroffenen als eine »vernachlässigbare« Auswirkung auf seine Rechte und Freiheiten zu bewerten (Datenschutz-Risiko). Aus der Sicht der interessierten Partei Unternehmen kann die Offenbarung eines Berichts eines internen Audits aber ein hohes Risiko darstellen, da eventuell Firmengeheimnisse offenbart werden (monetäres Risiko im ISMS).

Dritter Business Case: Partnervermittlung für Prominente

Szenario: Eine Partnervermittlung erhebt von Prominenten Stammdaten (Adress- und Kontaktdaten), um Personen vermitteln und Rechnungen schreiben zu können.

Bewertung: Bei der Offenbarung der Prominenten-Stammdaten wird dies aus Sicht der Betroffenen »signifikant« sein oder sogar als »maximal« bewertet. Obwohl das Datenschutzgesetz Adressdaten nicht als besonders sensibel einstuft, werden Prominente ein besonderes Interesse an der Geheimhaltung ihrer Adressdaten haben. Bei Politikern oder anderen staatlichen Funktionsträgern kann die Geheimhaltung der Adresse sogar lebenswichtig sein. Zum Vergleich: Eine reine Bewertung aus Unternehmenssicht könnte zu einer viel geringeren Risikoeinschätzung kommen und die Anforderungen der DS-GVO somit nicht adäquat abbilden.

Einschätzung der Eintrittswahrscheinlichkeiten

Die Eintrittswahrscheinlichkeit berücksichtigt viele unterschiedliche Aspekte. Neben den gegebenen Umständen (bspw. Lage eines Raumes in Bezug auf das Risiko eines Wasserschadens) spielen auch Unternehmenserfahrungen (Anzahl vergleichbarer Vorfälle in der Vergangenheit) und allgemeine Statistiken eine Rolle.

Bei einer qualitativen Risikobeurteilung kann die Eintrittswahrscheinlichkeit in verschiedene Stufen eingeteilt werden. Der Gesetzgeber gibt keine Auskunft über die Anzahl der Stufen und die Bewertung der Stufen. Ein potentielles Raster zur Beurteilung der Eintrittswahrscheinlichkeit kann z. B. so aussehen:[8]

1. Vernachlässigbar: für die ausgewählte Risikoquelle scheint es nicht sehr wahrscheinlich zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät und einen Zugangscode gesichert ist).
2. Eingeschränkt: für die ausgewählte Risikoquelle scheint es schwierig zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Raum, der durch ein Ausweislesegerät gesichert ist).
3. Signifikant: für die ausgewählte Risikoquelle scheint es möglich zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einem Büro, welches nur zugänglich ist, nachdem man einen Empfang passiert hat).
4. Maximal: für die ausgewählte Risikoquelle scheint es einfach zu sein, eine Schwachstelle eines unterstützenden Wertes auszunutzen, um eine Bedrohung eintreten zu lassen (zum Beispiel: Diebstahl von Papierdokumenten aus einer öffentlich zugänglichen Lobby).

4.5.7 Siebter Schritt: Risikobewertung

Aus dem Produkt der Auswirkung und der Eintrittswahrscheinlichkeit können dann die folgenden Risikoklassen gebildet werden:

Risikoklasse	Wert
hohes Risiko	12; 16
Risiko	3; 4 ; 6; 8; 9
geringes Risiko	1; 2

In der DS-GVO werden lediglich die Risikostufen »hohes Risiko« und »Risiko« adressiert, es können aber durchaus weitere Risikostufen gebildet werden, sofern dem Anwender daraus ein Vorteil erwächst (z. B. Erkenntnisgewinn).

Die Einstufung von personenbezogenen Daten in eine Risikoklasse hat Auswirkung auf den weiteren Umgang mit diesen personenbezogenen Daten, z. B.

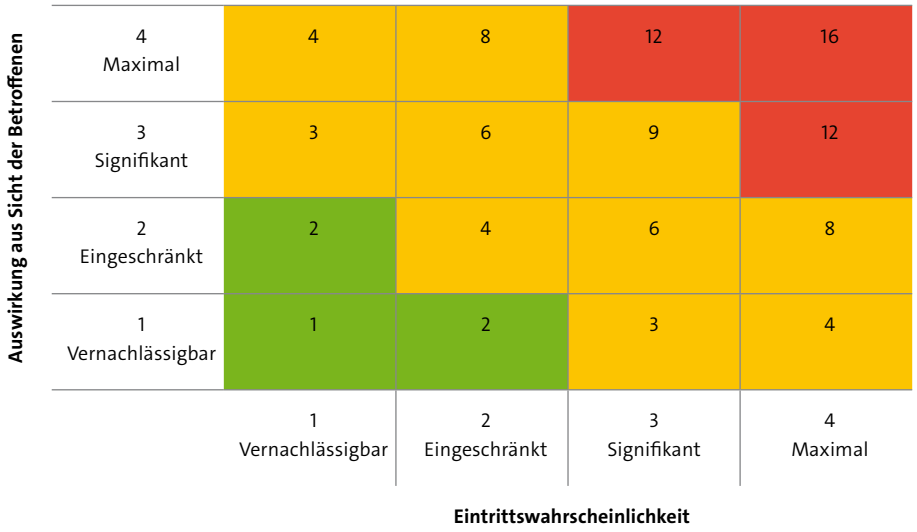
8 Entnommen aus ISO/IEC FDIS 29134:2017.

- Werden personenbezogene Daten in die Risikoklasse hohes Risiko eingeordnet, ist auf jeden Fall zu prüfen, ob eine Datenschutz-Folgenabschätzung durchzuführen ist.
- Wird der Schutz personenbezogener Daten verletzt, die in die Risikoklasse »Risiko« eingeordnet worden sind, so ist dies der zuständigen Aufsichtsbehörde zu melden.
- Wird der Schutz personenbezogener Daten verletzt, die in die Risikoklasse »hohes Risiko« eingeordnet worden sind, so ist dies zusätzlich auch den Betroffenen zu melden.
- Es kann zum Wegfall der Ausnahmen von der Führung einer Verarbeitungsübersicht gem. Art. 30 DS-GVO kommen.

Risikomatrix zur Darstellung des Schutzniveaus für das jeweilige Datenschutzrisiko

Eine Darstellung des Risikos als Produkt aus Eintrittswahrscheinlichkeit und Auswirkung ist in einer Risikomatrix möglich.

Beispiel Risiko-Matrix mit vier Stufen[9]



In die Matrix können nun die berechneten Datenschutz-Risiken eingetragen werden (Verletzung der Vertraulichkeit, Verfügbarkeit und Integrität).

9 Risikomatrix im Papier des Bayerischen Landesamts für Datenschutzaufsicht unter ↗https://www.lda.bayern.de/media/baylda_ds-gvo_18_privacy_impact_assessment.pdf

4.5.8 Achter Schritt: Bewältigung der Datenschutzrisiken

Insgesamt gibt es vier verschiedene Möglichkeiten, mit Risiken zu verfahren:

- Risikominimierung durch das Ergreifen von Maßnahmen
- Risikovermeidung (bspw. durch Beendigung der Verarbeitung bestimmter Daten oder Datenkategorien)
- Risikotransfer auf Dritte
- Risikoakzeptanz

Nicht immer kann jede Möglichkeit zur Risikobehandlung angewendet werden. Zum Beispiel ist im Datenschutz ein Risikotransfer auf Dritte häufig schwierig umzusetzen. Auch wird die Risikoakzeptanz, sofern es um Schäden des Betroffenen geht, nicht ohne weiteres anwendbar sein.

Ergreifen von Maßnahmen

Der europäische Gesetzgeber betrachtet in Art. 32 Abs. 1 DS-GVO lediglich die Option der Risikominderung durch das Ergreifen von (Datenschutz-) Maßnahmen.

Bei einer Risikobehandlung verlangt der europäische Gesetzgeber, dass mindestens die Umsetzung der folgenden Maßnahmen geprüft werden soll:

- Pseudonymisierung und Verschlüsselung personenbezogener Daten;
- Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen;
- Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;
- Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Zusätzlich fordert Art. 32 Abs. 4 von Verantwortlichem und Auftragsverarbeiter

- Zugriffsbeschränkung,
- Need-to-know-Prinzip.

Sofern Risiken durch die Einleitung von Maßnahmen verringert werden sollen, sollte eine entsprechende Maßnahmenliste geführt werden, die dokumentiert

- welche Maßnahme ist geplant
- wer ist für die Umsetzung verantwortlich
- bis wann ist geplant, die Umsetzung abzuschließen.

Darüber hinaus kann man sich bei der Maßnahmenplanung an diversen Maßnahmenkatalogen orientieren.

Maßnahmenkataloge in der Informationssicherheit und im Datenschutz

Sofern Maßnahmen zur Risikominimierung getroffen werden sollen, bietet es sich an auf akzeptierte Maßnahmenkataloge zurückzugreifen. Während viele Standards dem Anwender umfangreiche Maßnahmenkataloge zur Minimierung des Risikos mitgeben, ist die Anwendung eines bestimmten Katalogs nicht gesetzlich vorgeschrieben. Der Verantwortliche kann selber einen Maßnahmenkatalog wählen, sofern die Aspekte des Art. 32 Abs. 1 S. 2 lit a) – c) DS-GVO beachtet werden.

In der Informationssicherheit werden bspw. die folgenden Maßnahmenkataloge eingesetzt:

- ISO/IEC FDIS 29151:2016: Leitfaden für den Schutz personenbezogener Daten
- DIN ISO/IEC 27001:2015: Anhang A und DIN ISO/IEC 27002:2016 als Leitfaden zur Auslegung der Maßnahmen. Zusätzlich kann auf sektorspezifische Ergänzungen der DIN ISO/IEC 27002:2016 zurückgegriffen werden
- Maßnahmenkataloge der IT-Grundschutz-Kataloge

Für diese Kataloge gibt es Mapping-Tabellen für Überleitungsrechnungen und sie sind damit untereinander kompatibel.[10] Im Datenschutz gibt es im BDSG lediglich die Anlage zu § 9 Satz 1 BDSG. Konkrete Maßnahmen zur Umsetzung der Kontrollziele werden von der Literatur vorgeschlagen. Auch gibt es Zuordnungstabellen, um Informationssicherheitsmaßnahmen den Kontrollzielen des BDSG zuzuordnen.[11]

Angesichts existenzbedrohender Bußgeldrisiken empfiehlt es sich, im Unternehmen einen allgemein anerkannten Maßnahmenkatalog zu verwenden.

10 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Hilfsmittel/Doku/Vergleich_ISO27001_GS.pdf?__blob=publicationFile

11 http://www.bfdi.bund.de/SharedDocs/Publikationen/Arbeitshilfen/ErgaenzendeDoks/MassnahmeGS-Kat.pdf?__blob=publicationFile

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Neben dem Einsatz von

- generischen Maßnahmenkatalogen oder
- vorhandenen genehmigten Verhaltensregeln

sollten beim Technikeinsatz generell parallel auch die Grundsätze des Datenschutz durch Technikgestaltung (Data Protection by Design) und Datenschutz durch datenschutzfreundliche Voreinstellungen (Data Protection by Default) beachtet und umgesetzt werden, sofern möglich.

Genehmigte Verhaltensregeln und Zertifizierungen

Der Gesetzgeber hat allerdings auch vor Augen, dass Kleinstunternehmen und KMUs mit der Umsetzung der genannten Standards regelmäßig überfordert sein werden. Daher wird in Art. 32 Abs. 3 DS-GVO explizit darauf hingewiesen, dass Organisationen einen Nachweis mit der in Art. 32 geforderten Informationssicherheit über die Einhaltung genehmigter Verhaltensregeln (Art. 40, 41 DS-GVO) führen können, die von Verbänden oder anderen Organisationen erarbeitet worden sind. Ebenso kann die Erfüllung der Anforderungen zum Datenschutz durch Technikgestaltung (Art. 25 DS-GVO) durch Zertifizierung gemäß Art. 42 nachgewiesen werden.

Vorteile der Einhaltung von genehmigten Verhaltensregeln und einer Zertifizierung für den Verantwortlichen können sein, dass der Verantwortliche durch den Einsatz genehmigter Verhaltensregeln bei der Umsetzung der DS-GVO unterstützt wird. Eine erfolgreiche und aktuelle Zertifizierung gemäß Art. 42 soll bei der Verhängung eines Bußgeldes durch die zuständige Aufsichtsbehörde beachtet werden.

Prüfungen durch die zuständige Aufsichtsbehörde werden durch eine gültige Zertifizierung gemäß Art. 39 natürlich nicht verhindert Die Befugnisse der zuständigen Aufsichtsbehörde werden durch eine gültige Zertifizierung ebenfalls nicht eingeschränkt.

4.5.9 Neunter Schritt: Überwachung und Überprüfung

Der Gesetzgeber verpflichtet den Verantwortlichen einen Prozess für interne Audits der Sicherheit der Verarbeitung zu etablieren und durchzuführen. Dabei ist die Wirksamkeit getroffener technischer und organisatorischer Maßnahmen festzustellen.

Mit Blick auf die Rechenschaftspflichten empfiehlt sich auch hier eine ausführliche Dokumentation der Planung (Auditprogramm) als auch der durchgeführten Kontrollen (Auditberichte).

Sollten in Audits Abweichungen festgestellt werden, sollte die Nachhaltung der Behebung ebenfalls systematisiert und dokumentiert werden.

4.6 Fazit

Damit die Sicherheit in der Verarbeitung gemäß Artikel 32 DS-GVO von Unternehmen effizient umgesetzt werden kann, sind in der Datenschutzpraxis drei Punkte wünschenswert:

1. EU-weit sollten einheitliche Vorgehensmodelle zur Analyse und Umsetzung der »Sicherheit in der Verarbeitung« zur Anwendung kommen. Sonderwege oder experimentelle Verfahren zur Risikobestimmung sollten nicht eingesetzt werden.

2. Anforderung an Vorgehensmodelle zur Risikobestimmung ist, dass diese Verfahren gut dokumentiert sind, damit sie auch von der Masse der KMUs eingesetzt werden kann.

3. Bei der Risikobehandlung durch Maßnahmen sollten gut dokumentierte und erprobte Maßnahmenkataloge angewendet werden, damit der Anwender eine ausreichende Unterstützung durch die Literatur erfährt.

Es sei hier noch einmal klar darauf hingewiesen, dass ein Datenschutzrisiko und ein Risiko in der Informationssicherheit nicht kongruent sind. Aus diesem Grund wird die Sicherheit in der Verarbeitung gemäß Artikel 32 DS-GVO auch nicht durch den einfachen Einsatz eines ISMS zum Beispiel nach ISO/IEC 27001 erreicht. Nichtsdestotrotz ist eine Integration beider Risikomanagement-Systeme bis zu einem gewissen Punkt möglich.

5 Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)

5 Datenschutz-Folgenabschätzung (Art. 35 DS-GVO)

Eine Datenschutz-Folgenabschätzung erweitert die vorangegangene Risiko-Sicht der Bestimmung der »Sicherheit in der Verarbeitung« um eine Sicht auf die Rechte und Freiheiten natürlicher Personen und um eine Compliance-Sicht. Diese betrifft die Erfüllung gesetzlicher Verpflichtungen. Hierzu gehören auch Verpflichtungen, die der Betroffene selbst oder über Verbände vom Verantwortlichen einfordern kann. Zusätzlich wird der Dokumentationsgrad erhöht und – endlich – empfiehlt der europäische Gesetzgeber auch den Betroffenen zu involvieren.

5.1 Prüfung der Pflicht zur Durchführung einer DSFA

Aufsichtsbehörden können eine Liste mit Verarbeitungen erstellen, die generell nicht einer Datenschutz-Folgenabschätzung unterliegen (Whitelisting) und derjenigen, die generell einer Datenschutz-Folgenabschätzung unterliegen (Blacklisting).

Der Verantwortliche hat in gewissen Fällen die Pflicht, eine Datenschutz-Folgenabschätzung durchzuführen. Die Klassifizierung, ob ein hohes Risiko für die Rechte und Freiheiten eines Betroffenen vorliegt, orientiert sich an der Schwere des Grundrechtseingriffs für den Betroffenen. Die DS-GVO fordert vom Verantwortlichen, dass er das Datenschutz-Risiko anhand objektiver Bewertungen beurteilt.

Der europäische Gesetzgeber sieht insbesondere neue Technologien als Auslöser der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung.

Unabhängig von der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung kann diese als Ergänzung der Risikobeurteilung gem. Art. 32 DS-GVO freiwillig durchgeführt werden.

Als Erleichterung können mehrere ähnliche Verarbeitungsvorgänge mit ähnlich hohen Risiken zusammen in einer einzigen Abschätzung vorgenommen werden.

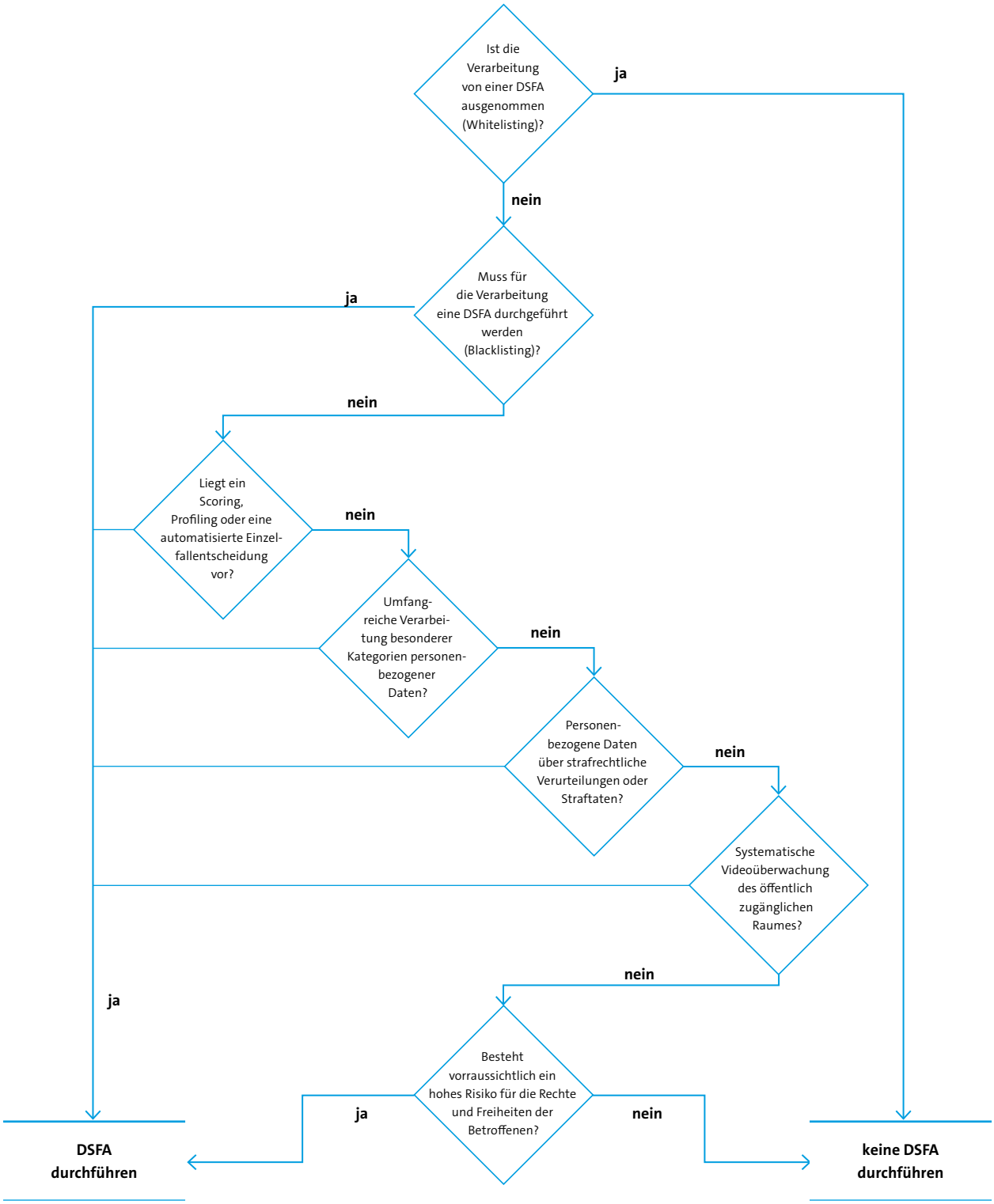


Abbildung 6: Orientierungshilfe Datenschutz-Folgenabschätzung

5.2 Die Rolle des Datenschutzbeauftragten in der DSFA

Ein etwaig bestellter Datenschutzbeauftragter steht dem Verantwortlichen lediglich mit Rat zur Seite und überwacht ihre Durchführung gemäß Art. 35 (Art. 35 Abs. 2 und Art. 39 Abs. 1 c) DS-GVO). Er hat nicht die Aufgabe, die Datenschutz-Folgenabschätzung anzustoßen, durchzuführen oder ein Ergebnis zu beurteilen. So ist es beispielsweise bei einer wesentlichen Änderung an der Unternehmens-EDV durchaus sinnvoll, dass der Change-Manager weiterhin Eigentümer (im Sinne von »Owner«) des Projekts bleibt.

5.3 Beschreibung der Zwecke der Verarbeitung

Eine Beschreibung der Zwecke der Verarbeitung erfolgte bereits im Verarbeitungsverzeichnis, daher sollte auf die bereits erarbeiteten Ergebnisse zurückgegriffen werden (siehe auch Beispiel »Fakturierung« aus dem Kapitel »Verarbeitungsverzeichnis«).

Abhängig von der Genauigkeit der gegebenen Beschreibung wird es sehr wahrscheinlich notwendig sein, die von dem Verantwortlichen verfolgten berechtigten Interessen darzulegen.

Ferner muss durch den Verantwortlichen eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck vorgenommen werden.

5.4 Systematische Beschreibung der geplanten Verarbeitungsvorgänge

Im Gegensatz zur Sicherheit in der Verarbeitung muss bei einer Datenschutz-Folgenabschätzung das Verfahren genauer beschrieben werden. Für jede Phase der Verarbeitung sollen die folgenden Aspekte erhoben und dokumentiert werden:

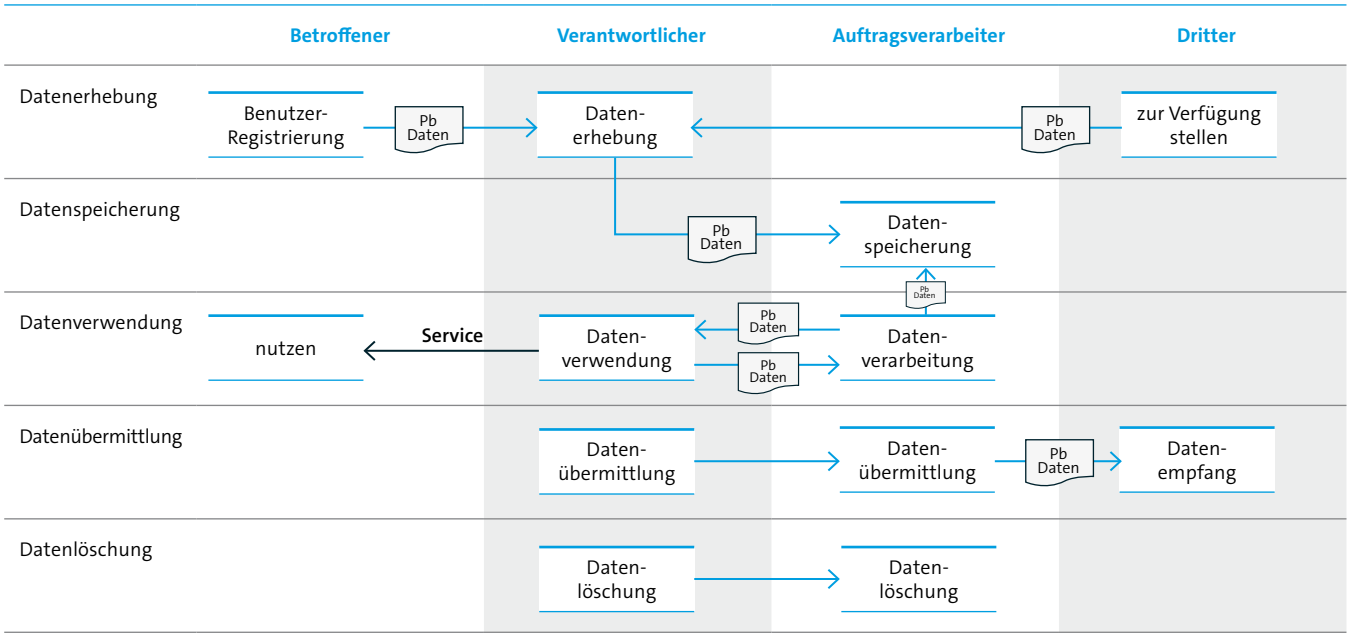
- Beschreibung der Prozessschritte
- Eingesetzte Informationssysteme
- Weitere unterstützende Werte, die eingesetzt werden

Die Beschreibung kann je nach Verarbeitungsphase im Lebenszyklus von Daten / Informationen in einer Tabelle verbal erfolgen (siehe als Beispiel die folgende Grafik) oder als Datenfluss-Diagramm graphisch (siehe als Beispiel die darauffolgende Grafik aus der ISO/IEC FDIS 29134:2017). Andere Beschreibungsmethoden sind natürlich auch möglich.

Beispiel für eine Beschreibung eines Verfahrens (Fakturierung)

Phase des Geschäftsprozesses	Detaillierte Beschreibung der Phase	Informationssysteme, die für die Prozessphase relevant ist	Weitere unterstützende Werte, die für die Prozessphase relevant sind
Erhebung personenbezogener Daten	Die Fachabteilungen beauftragen das Rechnungswesen mit der Angebotserstellung und dem Angebotsversand. Die Stammdaten von Interessenten und Kreditoren werden erfasst, sofern dies noch nicht geschehen ist. Die Rechnungsdaten werden erfasst.	Hardware: Arbeitsplatz-PCs, Applikationsserver (E-Mail und Fakturierungssoftware), Fileserver Software: E-Mail-Server, E-Mail-Clients Fakturierungssoftware (Server) Fakturierungssoftware (Clients)	Mitarbeiter Rechnungswesen, Wartungspersonal
Verarbeiten personenbezogener Daten	Im Rechnungswesen werden Angebote und Rechnungen elektronisch erstellt und ausgedruckt. Rechnungsdaten werden auf Anforderung korrigiert und erneut versendet. Stammdaten von Kreditoren werden aktualisiert.	Hardware: Arbeitsplatz-PCs, Applikationsserver (E-Mail und Fakturierungssoftware), Fileserver Software: E-Mail-Server, E-Mail-Clients Fakturierungssoftware (Server) Fakturierungssoftware (Clients)	Ausdrucke Mitarbeiter Rechnungswesen, Wartungspersonal
Übermittlung personenbezogener Daten	Ausgedruckte Angebote und Rechnungen werden an Interessenten und Kreditoren per Post versendet. Monatlicher Übertrag der Rechnungsdaten an die FiBu.	Hardware: Arbeitsplatz-PCs, Applikationsserver (Fakturierungs software), Fileserver, Drucker Software: Fakturierungssoftware (Server) Fakturierungssoftware (Clients)	Ausdrucke, Postweg zur Übermittlung Mitarbeiter Rechnungswesen, Wartungspersonal
Aufbewahrung personenbezogener Daten	Kopien von versendeten Angeboten und Rechnungen werden ausgedruckt im Archivraum aufbewahrt. Von den Daten der Fakturierungssoftware werden Sicherungsbänder über den Aufbewahrungszeitraum von 10 Jahren aufbewahrt.	Hardware: Arbeitsplatz-PCs, Applikationsserver (E-Mail und Fakturierungssoftware), Fileserver, Sicherungsbänder Software: E-Mail-Server, E-Mail-Clients Fakturierungs-software (Server) Fakturierungs-software (Clients) Sicherungs-Software	Ausdrucke Mitarbeiter Rechnungswesen, Wartungspersonal
Vernichtung personenbezogener Daten	Datenträger werden vernichtet, wenn der Datenträger seine maximale Lebensdauer, abzüglich eines Sicherheitsabschlages, erreicht hat oder wenn die maximale Aufbewahrungsdauer der personenbezogenen Daten auf dem Datenträger erreicht worden ist.	Hardware: Arbeitsplatz-PCs, Applikationsserver (E-Mail und Fakturierungssoftware), Fileserver Sicherungsbänder Software: E-Mail-Server, E-Mail-Clients	Mitarbeiter Rechnungswesen, Datenträgervernichter

Das Ergebnis der genauen Beschreibung einer Verarbeitung kann aber auch ein Datenfluss-Diagramm sein:[11]



5.5 Bewertung der Risiken für die Rechte und Freiheiten der Betroffenen

Die DS-GVO verfolgt eine Anzahl an Datenschutzprinzipien, von denen die überwiegende Zahl in Art. 5 DS-GVO genannt wird:

Datenschutzprinzipien[12]	Datenschutz-Risiko: Verletzung von Rechten und Freiheiten natürlicher Personen	Compliance-Risiko: Verstöße gegen die Daten-schutz-Grundverordnung	Informationssicherheits-Risiko: Verletzung der Prinzipien der Informationssicherheit
1. Rechtmäßigkeit und Verarbeitung nach Treu und Glauben	Art. 5 Abs.1 lit. a)	Art. 6 Abs. 1 a) Einwilligung Art. 6 Abs. 1 b) Vertrag mit dem Betroffenen Art. 6 Abs. 1 c) rechtliche Verpflichtung Art. 6 Abs. 1 d) lebenswichtige Interessen natürlicher Personen Art. 6 Abs. 1 e) öffentliche Aufgaben Art. 6 Abs. 1 f) berechtigte Interessen Verantwortlicher oder Dritter Art. 21 Widerspruchsrecht Art. 22 Recht auf Ausschluss automatisierter Entscheidungen	

Datenschutzprinzipien[12]	Datenschutz-Risiko: Verletzung von Rechten und Freiheiten natürlicher Personen	Compliance-Risiko: Verstöße gegen die Daten-schutz-Grundverordnung	Informationssicherheits-Risiko: Verletzung der Prinzipien der Informationssicherheit
2. Transparenz	Art. 5 Abs. 1 lit. a)	Art. 12 Modalitäten für die Rechteausübung Art. 13 Information bei Erhebung beim Betroffenen Art. 14 Information bei Erhebung nicht beim Betroffenen Art. 15 Auskunftsrecht	
3. Zweckbindung	Art 5 Abs. 1) b)	Art. 6 Abs. 4 Zweckänderung Art. 13 Abs. 3 und Art. 14 Abs. 4 Information bei Zweckänderung	
4. Datenminimierung	Art. 5 Abs. 1 lit. c)	Art. 25 Datenschutz durch Technik-gestaltung und datenschutz-freundlichen Voreinstellungen Art. 17 Recht auf Löschung	
5. Richtigkeit	Art. 5 Abs. 1 lit. d)	Art. 16 Recht auf Berichtigung	
6. Speicherbegrenzung	Art. 5 Abs.1 lit. e)	Art. 17 Recht auf Löschung Art. 18 Recht auf Einschränkung	
7. Integrität und Vertraulichkeit	Art. 5 Abs. 1 lit. f)	Art. 34 Benachrichtigung bei Verletzung des Schutzes personen-bezogener Daten	Art. 32 Abs. 1 lit. b) Vertraulichkeit und Integrität auf Dauer sicherstellen
8. Verfügbarkeit (Belastbarkeit)			Art. 32 Abs. 1 lit. b) Verfügbarkeit und Belastbarkeit auf Dauer sicherstellen Art. 32 Abs. 1 lit. c) Zugang zu Daten nach Zwischenfall rasch wiederher-stellen
9. Persönliche Teilhabe und Zugang		Art. 16 Recht auf Berichtigung Art. 17 Recht auf Löschung Art. 18 Recht auf Einschränkung der Verarbeitung Art. 19 Mitteilungspflicht im Zusammenhang mit der Berichti-gung oder Löschung personenbezo-gener Daten oder der Einschrän-kung der Verarbeitung Art. 20 Recht auf Datenübertragbarkeit	
10. Rechenschaftspflicht	Art. 5 Abs. 2 Nachweis der Einhal-tung der Datenschutz-Grundsätze	Art. 30 Verarbeitungsverzeichnis Art. 32 Sicherheit in der Verarbeitung Art. 35 Datenschutz-Folgenabschät-zung Art. 36 Vorherige Konsultation	

12 ISO/IEC FDIS 29134:2017, Seite 40.

13 Die Datenschutzprinzipien werden im Anhang erläutert.

Der Verantwortliche muss beschreiben, welche Datenschutzrisiken den Betroffenen bei der Verletzung der Datenschutzprinzipien drohen.

Die Informationssicherheitsrisiko-Sicht wurde bereits im Kapitel »Sicherheit in der Verarbeitung« erarbeitet und muss für die Datenschutz-Folgenabschätzung lediglich übernommen werden.

Beispiel: Videoüberwachung im Eingangsbereich eines Unternehmens
Zutritt zum Unternehmen können Mitarbeiter über mehrere Eingänge erhalten. Der Zugang der Mitarbeiter erfolgt durch eine Schleuse, die Authentifizierung der Mitarbeiter erfolgt über Chipkarten. Nur der Haupteingang ist durch den Werksschutz besetzt. Der Werksschutz kann mit Hilfe von Videokameras die Nebeneingänge einsehen (nur verlängertes Auge!), die Gesichter von Personen können auf den Bildschirmen identifiziert werden. Eine Aufschaltung erfolgt auf Anforderung von Mitarbeitern (Probleme mit der Schleuse) oder zufällig durch den Werksschutz, um zu prüfen, ob Schleusen umgangen werden.

Prüfungsbeginn

Um überhaupt ein datenschutzrechtliches Prüfverfahren in Gang zu setzen, muss positiv geprüft werden, ob personenbezogene Daten erhoben, verarbeitet oder genutzt werden.

Dadurch, dass Gesichter identifiziert werden können, werden personenbezogene Daten erhoben.

Compliance-Sicht

In der Compliance-Sicht müssen diverse Datenschutz-Prinzipien geprüft werden. Eine Prüfung umfasst den gesamten Lebenszyklus von personenbezogenen Daten, sofern die Verarbeitungsphasen relevant sind:

Exkurs: Phasen der Verarbeitung:

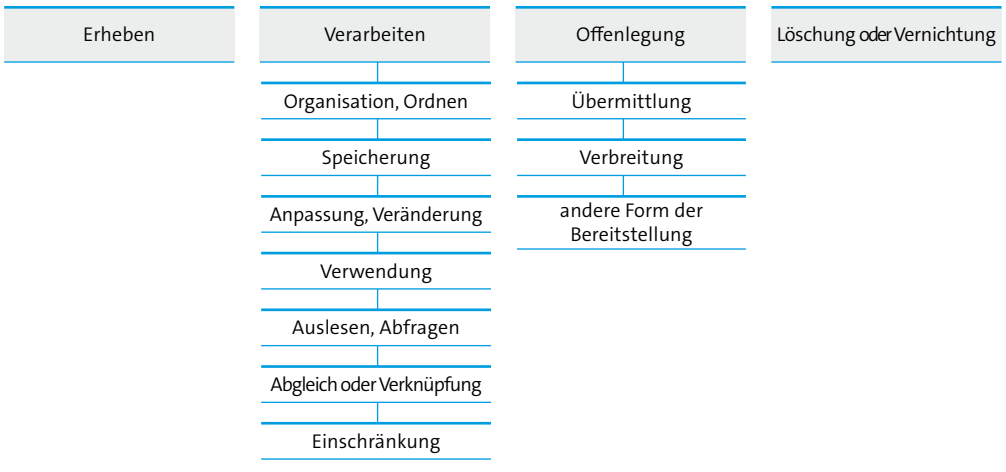


Abbildung 7: Phasen der Verarbeitung

Prüfung der Datenschutzprinzipien

Compliance-Sicht	
1 Rechtmäßigkeit der Datenverarbeitung und Verarbeitung nach Treu und Glauben Eine Videoüberwachung der Nebeneingänge ohne Aufzeichnung ist gemäß Artikel 6 Absatz 1 Buchstabe f) zulässig.	**10 Rechenschaftspflicht** Die Datenschutzmaßnahmen werden vom Verantwortlichen durchgesetzt, die ergriffenen Datenschutzmaßnahmen sind risikoadäquat, es gibt Verfahren zum Umgang mit Datenschutzvorfällen und Meldewege (bis zur AB) die Datenschutzmaßnahmen werden regelmäßig überwacht, Datenschutzverantwortlichkeiten werden vom Verantwortlichen festgelegt, der Datenschutz ist ins unternehmensweite Governance-System eingearbeitet.
2 Transparenz Ergriffene Maßnahme: Es erfolgt eine Auszeichnung der Videoüberwachung unter Beachtung der Anforderungen des Artikel 13 DS-GVO.	
3 Zweckbindung Die Videoüberwachung darf nur zum Zweck der Unterstützung der Mitarbeiter oder der stichprobenartigen Kontrolle einer möglichen Umgehung der Schleusen durch den eigenen Werksschutz eingesetzt werden. Alternativ zu der Videoüberwachung (verlängertes Auge) müssten an jedem Nebenausgang Personen des Werkschutzes postiert werden, was bei dem aktuellen Risiko für die Rechte und Freiheiten des Betroffenen unverhältnismäßig im Vergleich zu den Kosten steht. Alternativ zu der Videoüberwachung (verlängertes Auge) müssten an jedem Nebenausgang Personen des Werkschutzes postiert werden, was bei dem aktuellen Risiko für die Rechte und Freiheiten des Betroffenen unverhältnismäßig im Vergleich zu den Kosten steht. (»Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1« Artikel 35, Absatz 7, Buchstabe c).	
4 Datenminimierung Ergriffene Maßnahmen: Die Kamera ist so eingestellt, dass nur der relevante Schleusenbereich von den Videokameras erfasst wird (Passepartout oder Verpixelung).	
5 Richtigkeit Ergriffene Maßnahmen: Da keine personenbezogenen Daten verarbeitet oder offengelegt werden, muss kein Lösch- oder Korrekturkonzept erarbeitet werden.	
6 Speicherbegrenzung Ergriffene Maßnahmen: Da keine personenbezogenen Daten verarbeitet oder offengelegt werden, muss kein Löschkonzept erarbeitet werden.	
9 Persönliche Teilhabe und Zugang Ergriffene Maßnahmen: Betroffene können sich bei allgemeinen Auskünften direkt an den Verantwortlichen für die Videoüberwachung beim Werksschutz oder den Datenschutzbeauftragten wenden.	

Fazit

1. Die Datenschutzprinzipien in der Compliance-Sicht werden erfüllt,
2. eine Datenschutz-Risikoanalyse weist kein hohes Risiko für die Rechte und Freiheiten der Betroffenen aus, unter Einbeziehung der beschriebenen Maßnahmen.

5.6 Die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen (Risikobehandlungsplan)

Der Verantwortliche muss beschreiben, welche Maßnahmen er ergreifen wird, um eine Verletzung der Datenschutz-Prinzipien zu vermeiden. Auch hier ist zwischen der Compliance- und der Informationssicherheitsrisiko-Sicht zu unterscheiden.

Insbesondere fordert die DS-GVO in Art. 35 Abs. 7 d) die Festlegung von Abhilfemaßnahmen (einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren), durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird. Dabei ist den Rechten der betroffenen Personen und sonstiger Betroffener Rechnung zu tragen.

	Es sind für die Verarbeitung **keine genehmigten Verhaltensregeln vorhanden**		Es sind für die Verarbeitung **genehmigten Verhaltensregeln vorhanden**
	Vorschläge für Maßnahmenkataloge (zu modifizieren auf die Anforderungen der DS-GVO)	zu beachten beim Technikeinsatz:	Sofern die Organisation sich vorhandenen genehmigten Verhaltensregeln unterwerfen will
Compliance-Sicht	Möglicher Maßnahmenkatalog der CNIL: CNIL, Measures for the privacy risk treatment, 2012 Möglicher Maßnahmenkatalog aus der ISO-Welt Für Verantwortliche: ISO/IEC DIS 29151, Annex A Für Auftragsverarbeiter: ISO/IEC 27018, Annex A	Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen, Art. 25 DS-GVO	Anwendungen der genehmigten Verhaltensregeln
Risiko-Sicht	Möglicher Maßnahmenkatalog der CNIL: CNIL, Measures for the privacy risk treatment, 2012 Möglicher Maßnahmenkatalog aus der ISO-Welt Für Verantwortliche: ISO/IEC DIS 29151 Für Auftragsverarbeiter: ISO/IEC 27018 mit den Erläuterungen der ISO/IEC 27002		

Beschließt die Organisation zur Behandlung von Datenschutzrisiken Maßnahmen zu ergreifen, so bietet es sich aus Gründen der Rechenschaftspflicht an, die Maßnahmen zur Minimierung der Datenschutzrisiken tabellarisch in eine Maßnahmenliste aufzunehmen und jeder Maßnahme einen Verantwortlichen zur Umsetzung und ein Zieldatum zuzuweisen. Im Risikomanagement wird eine solche Liste auch Risikobehandlungsplan genannt.

Genehmigte Verhaltensregeln sind nicht vorhanden

Die Compliance-Sicht umfasst gesetzlich vorgeschriebene Maßnahmen. Diese Maßnahmen müssen umgesetzt werden.

> **Beispiel**: Ein Verfahren kann nur rechtmäßig sein oder gegen Recht verstoßen; ein bisschen Rechtmäßigkeit ist nicht möglich.

Maßnahmen zur Einhaltung der Datenschutzprinzipien sind z. B. in der ISO/IEC FDIS 29151:2016 Annex A, der DIN ISO/IEC 27018:2014 Annex A (für Auftragsverarbeiter) oder auch in den Papieren der CNIL enthalten.

Die Risiko-Sicht umfasst Maßnahmen, die sich aus einer Risikobeurteilung ergaben.

> **Beispiel**: Der Zutritt zu einem Gebäude kann durch sehr unterschiedliche Maßnahmen verhindert werden: Türschloss, Alarmanlage, Werkschutz etc.

Hier kann zur Bestimmung von Maßnahmen auf ISO-Kataloge (ISO/IEC FDIS 29151:2016, ISO/IEC 27018:2014, DIN ISO/IEC 27002:2016) oder auch auf die Bausteine der IT-Grundschutz-Kataloge zurückgegriffen werden.

Genehmigte Verhaltensregeln sind vorhanden

Sofern für den zu beurteilenden Sachverhalt genehmigte Verhaltensregeln vorhanden sind, sollten diese bei einer Maßnahmenauswahl eingesetzt werden, bevor auf allgemeine Maßnahmenkataloge zurückgegriffen wird.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Bei Technikeinsatz ist grundsätzlich darauf zu achten, dass die Grundsätze des Datenschutzes durch Technikgestaltung (Data Protection by Default) und der datenschutzfreundlichen Voreinstellungen (Data Protection by Design) beachtet werden.

5.7 Rolle der interessierten Parteien

Während bei der Analyse der Sicherheit der Verarbeitung eine Risikobewertung aus der Perspektive des Betroffenen erfolgt, ist eine Beteiligung der interessierten Parteien bei einer Datenschutz-Folgenabschätzung explizit vorgesehen, aber nicht vorgeschrieben (»gegebenenfalls«).

Auch wenn eine Beteiligung interessierter Parteien unter Umständen zu hohen Kosten führen kann, ist sie in Betracht zu ziehen, da diese Beteiligung zum Beispiel durch die Schaffung von Akzeptanz durch Transparenz auch im ureigenen Interesse des Verantwortlichen liegen kann. Auch darf nicht vergessen werden, dass der Risikoappetit der Betroffenen aus Unternehmenssicht meist nicht korrekt bewertet wird.

5.8 DSFA-Bericht

Ein Bericht für eine Datenschutz-Folgenabschätzung muss gemäß Artikel 35 Absatz 7 mindestens die folgenden Angaben enthalten:

- eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, gegebenenfalls einschließlich der von dem Verantwortlichen verfolgten berechtigten Interessen;
- eine Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck;
- eine Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen gemäß Absatz 1 und
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht wird, dass diese Verordnung eingehalten wird, wobei den Rechten und berechtigten Interessen der betroffenen Personen und sonstiger Betroffener Rechnung getragen wird.

Sofern eine Konsultation der Aufsichtsbehörde notwendig ist, muss ein DSFA-Bericht um die folgenden Angaben ergänzt werden (Artikel 36 Absatz 3):

- gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, insbesondere bei einer Verarbeitung innerhalb einer Gruppe von Unternehmen;
- die Zwecke und die Mittel der beabsichtigten Verarbeitung;
- die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß dieser Verordnung vorgesehenen Maßnahmen und Garantien;
- gegebenenfalls die Kontaktdaten des Datenschutzbeauftragten;
- die Datenschutz-Folgenabschätzung gemäß Artikel 35 und
- alle sonstigen von der Aufsichtsbehörde angeforderten Informationen.

Eine mögliche Mustergliederung für einen Datenschutz-Folgenabschätzungs-Report, die die Anforderungen des Artikels 35 Absatz 7 DS-GVO erfüllt, kann wie folgt aussehen:

Datenschutz-Folgenabschätzung

1 Einleitung

2 Anwendungsbereich Datenschutz-Folgenabschätzung
- 2.1 Systematische Beschreibung der Verarbeitung Zwecke
- 2.2 Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge in Bezug auf den Zweck
- 2.3 Zwecke und die Mittel der beabsichtigten Verarbeitung
- 2.4 Involvierte Parteien:
  - 2.4.1 Verantwortlicher
  - 2.4.2 Gemeinsam Verantwortliche
  - 2.4.3 Auftragsverarbeiter
  - 2.4.4 Kontaktdaten des Datenschutzbeauftragten

3 Datenschutz-Anforderungen

4 Datenschutz-Risikobetrachtung
- 4.1 Datenschutz-Risikoidentifikation
- 4.2 Datenschutz-Risikoanalyse
- 4.3 Datenschutz-Risikobewertung

5 Geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt wird und Nachweis

6 Ergebnis der Datenschutz-Folgenabschätzung und möglich Pflicht zum Durchlaufen des Konsultationsverfahrens

5.9 Konsultationsverfahren

Besteht nach dem Ergreifen von Maßnahmen zur Reduzierung des Risikos für die Rechte und Freiheiten des Betroffenen weiterhin ein hohes Risiko (»sofern der Verantwortliche keine Maßnahmen zur Eindämmung des Risikos trifft« und Erwägungsgrund 94 »ist der Verantwortliche der Auffassung, dass das Risiko nicht durch in Bezug auf verfügbare Technologien und Implementierungskosten vertretbare Mittel eingedämmt werden kann«), so hat der Verantwortliche vor der Inbetriebnahme der Verarbeitung (»geplante Verarbeitung«) die Aufsichtsbehörde zu konsultieren. Der Verantwortliche stellt der Aufsichtsbehörde bei einer Konsultation die in Kapitel 5.8 beschriebenen Informationen zur Verfügung.

Die Aufsichtsbehörde prüft nun im Konsultationsverfahren, ob die zu untersuchende Verarbeitung im Einklang mit der Datenschutz-Grundverordnung steht. Sollte dies nicht der Fall sein, wird der Verantwortliche innerhalb von 14 Wochen (maximal 8 Wochen und eine mögliche Verlängerung um sechs Wochen) darüber informiert. Im Falle der Konformität der Verarbeitung sieht die Verordnung keine Benachrichtigungspflicht durch die Aufsichtsbehörde vor .

Anhang

Kriterien für »hohes Risiko« von Art. 29-Datenschutzgruppe (WP 248)

Auf S. 7-10 des WP 248 nennt die Art. 29-Datenschutzgruppe Kriterien, die bei der Frage nach der Notwendigkeit einer DSFA berücksichtigt werden sollten. Dabei geht sie davon aus, dass es umso wahrscheinlicher ist, dass ein hohes Risiko für die Rechte und Freiheiten der Betroffenen gegeben ist, je mehr dieser Kriterien gleichzeitig erfüllt sind.

1. Evaluierung oder Scoring, inklusive Profilbildung und Vorhersagen
2. Automatisierte Entscheidungen mit rechtlicher oder ähnlich beeinträchtigender Wirkung
3. Systematische Beobachtung
4. Sensible Daten
5. In großem Umfang verarbeitete Daten
6. Datensätze, die abgeglichen oder kombiniert wurden
7. Daten, die verletzliche Datensubjekte betreffen
8. Innovative Nutzung oder Verwendung von technologischen und organisatorischen Lösungen
9. Datenübermittlung in Drittstaaten außerhalb der EU
10. Datenverarbeitungen, die den Betroffenen davon abhalten, ein Recht geltend zu machen oder einen Dienst oder Vertrag zu nutzen

Einstufungstabelle

Beispielhaft wird hier der Vorschlag der CNIL als Einstufungstabelle zur Schätzung der Schwere der Auswirkung angewendet.[14]

Risiko-Niveau	1. Vernachlässigbar	2. Eingeschränkt	3. Signifikant	4. Maximal
Generische Beschreibung der Auswirkung (direkt oder indirekt)	▪ Betroffene erleiden eventuell Unannehmlichkeiten, welche sie aber mit einigen Problemen überwinden können.	▪ Betroffene erleiden eventuell signifikante Unannehmlichkeiten, welche sie aber mit einigen Schwierigkeiten überwinden können.	▪ Betroffene erleiden eventuell signifikante Konsequenzen, die sie nur mit ernsthaften Schwierigkeiten überwinden können.	▪ Betroffene erleiden eventuell signifikante oder sogar unumkehrbare Konsequenzen, die sie nicht überwinden können.

14 CNIL, Privacy Impact Assessment (PIA – Tools (templates and knowledge bases), 2015, Seite 13 ff.

Risiko-Niveau	1. Vernachlässigbar	2. Eingeschränkt	3. Signifikant	4. Maximal
Beispiele für physische Auswirkungen	▪ Mangel an adäquater Betreuung für eine abhängige Person (Minderjährige, Person unter Vormundschaft) ▪ Vorübergehende Kopfschmerzen	▪ Leichte körperliche Beschwerden (z. B. leichte Krankheiten aufgrund unberücksichtigter medizinischer Kontraindikationen) ▪ Minderschwere körperliche Schäden aufgrund mangelnder Gesundheitsfürsorge (z. B. bei Behinderungen) Rufschädigung, die zu physischer oder psychischer Gegenreaktion führt	▪ Schwere körperliche Beschwerden, die langfristigen Schaden verursachen (z. B. Verschlechterung der Gesundheit aufgrund unsachgemäßer Versorgung oder Missachtung von Kontraindikationen) ▪ Veränderung der körperlichen Unversehrtheit z. B. nach einem Angriff, einem Unfall zu Hause oder auf der Arbeit usw.	▪ Langzeiterkrankung oder dauerhafte körperliche Beschwerden (z. B. wegen der Missachtung von Kontraindikationen) ▪ Tod (z. B. Mord, Selbstmord, tödlicher Unfall) ▪ Dauerhafte Beeinträchtigung der körperlichen Unversehrtheit
Beispiele für materielle Auswirkungen	▪ Zeitverlust bei der Wiederholung von Formalitäten oder Warten, bis sie erfüllt sind ▪ Empfang unerwünschter E-Mails (z. B. Spam) ▪ Wiederverwendung von auf Websites veröffentlichten Daten zum Zweck der zielgerichteten Werbung (Information zu sozialen Netzwerken, Wiederverwendung für Papierpost) ▪ Gezielte Werbung für übliche Konsumgüter	▪ Unvorhergesehene Zahlungsverpflichtungen (z. B. fälschlich erhobene Gebühren), zusätzliche Kosten (z. B. Bankgebühren, Prozesskosten), Zahlungsausfälle ▪ Verweigerung von staatlichen Leistungen oder privatwirtschaftlichen Leistungen ▪ Verlust an privatem Komfort (Stornierung von Freizeitaktivitäten, Einkäufen, Urlauben, oder die Kündigung eines online Benutzerkontos)Entgangene Karrierechancen ▪ Gesperrte Benutzerkonten (z. B. Spiele, staatliche Einrichtungen) ▪ Unbestellte und gezielte Mails, die mit hinreichender Wahrscheinlichkeit rufschädigende Wirkung entfalten ▪ Kostenerhöhungen (z. B. erhöhte Versicherungsprämien) ▪ Veraltete Daten ohne Update (z. B. vormalige Arbeitsstelle) Verarbeitung unrichtiger Daten, die beispielsweise zu Kontostörungen führen kann (z. B. Bank, Kunden, gemeinnützige Organisationen) ▪ Gezielte Internetwerbung gerichtet auf persönliche Informationen, welche die betroffene Person geheim halten wollte (z. B. Werbung für schwangere Frauen, Suchttherapien) ▪ Unrichtiges oder unangebrachtes Profiling	▪ Nicht kompensierter Missbrauch von Geld ▪ Nicht-temporäre finanzielle Schwierigkeiten (z. B. Kreditvergabe) ▪ Entgang nicht wiederkehrender Möglichkeiten (z. B. Kreditvergabe, Zulassung zum Studium, Praktikum, Arbeitsstelle, Prüfungszulassung) ▪ Verbot der Führung von Bankkonten ▪ Beschädigung von Eigentum ▪ Verlust der Wohnung ▪ Verlust des Arbeitsplatzes ▪ Trennung oder Scheidung ▪ Finanzieller Verlust infolge eines Betrugs (z. B. nach einem versuchten Phishing) ▪ Kontosperrung im Ausland ▪ Verlust von Kundendaten	▪ Finanzielles Risiko ▪ Erhebliche Schulden ▪ Unfähigkeit zu arbeiten ▪ Unfähigkeit umzuziehen ▪ Verlust von Beweismitteln im Zusammenhang mit Rechtsstreitigkeiten ▪ Verlust des Zugriffs auf lebenswichtige Infrastrukturen (Wasser, Elektrizität)

Risiko-Niveau	1. Vernachlässigbar	2. Eingeschränkt	3. Signifikant	4. Maximal
Beispiele für moralische Auswirkungen	▪ Leichte Verärgerung, ausgelöst durch erhaltene oder erfragte Informationen ▪ Angst, die Kontrolle über die eigenen Daten zu verlieren ▪ Gefühl der Verletzung der Privatsphäre ohne wirklichen oder objektiven Schaden (z. B. kommerzielle Eingriffe) ▪ Zeitverlust bei der Konfiguration der Daten ▪ Mangel an Respekt für die Freiheit der Online-Bewegung aufgrund der Verweigerung des Zugangs zu einer kommerziellen Website (z. B. Alkohol wegen des falschen Alters)	▪ Verweigerung zukünftig Informationssysteme zu nutzen (z. B. nach Whistleblowing, in sozialen Netzwerken) ▪ Minderschwere aber objektiv bestehende psychologische Leiden (z. B. Verleumdungen, Rufschädigungen) ▪ Probleme im Umgang mit privaten oder beruflichen Kontakten (z. B. Rufschädigung, keine Wiedererkennung) Verletzung der Privatsphäre ohne bleibende Schäden ▪ Einschüchterung in sozialen Netzwerken	▪ Schwere psychische Beschwerden (z. B. Depression, Entwicklung einer Phobie) ▪ Gefühl der Verletzung der Privatsphäre mit irreversiblen Schaden ▪ Gefühl der Verwundbarkeit nach einer Vorladung vor Gericht ▪ Gefühl der Verletzung von Grundrechten (z. B. Diskriminierung oder Einschränkung der Meinungsfreiheit) ▪ Opfer einer Erpressung ▪ Cyber-Mobbing und Belästigung	▪ Langfristige oder dauerhafte psychische Beschwerden ▪ Strafrechtliche Verurteilung ▪ Entführung ▪ Verlust familiärer Bindungen ▪ Unfähigkeit Rechtsschutz zu erlangen ▪ Veränderung des Aufenthaltsrechts und/oder Verlust der Geschäftsfähigkeit (Vormundschaft)

Datenschutzprinzipien

Compliance-Sicht

1 Rechtmäßigkeit der Datenverarbeitung und Verarbeitung nach Treu und Glauben
(Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (»Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz«); Artikel 5 Absatz 1 Buchstabe a).)

Erwägungsgrund 39: Jede Verarbeitung personenbezogener Daten sollte rechtmäßig und nach Treu und Glauben erfolgen.

2 Transparenz
(Personenbezogene Daten müssen auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden (»Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz«); Artikel 5 Absatz 1 Buchstabe a).)

Erwägungsgrund 39: Für natürliche Personen sollte Transparenz dahingehend bestehen, dass sie betreffende personenbezogene Daten erhoben, verwendet, eingesehen oder anderweitig verarbeitet werden und in welchem Umfang die personenbezogenen Daten verarbeitet werden und künftig noch verarbeitet werden. Der Grundsatz der Transparenz setzt voraus, dass alle Informationen und Mitteilungen zur Verarbeitung dieser personenbezogenen Daten leicht zugänglich und verständlich und in klarer und einfacher Sprache abgefasst sind. Dieser Grundsatz betrifft insbesondere die Informationen über die Identität des Verantwortlichen und die Zwecke der Verarbeitung und sonstige Informationen, die eine faire und transparente Verarbeitung im Hinblick auf die betroffenen natürlichen Personen gewährleisten, sowie deren Recht, eine Bestätigung und Auskunft darüber zu erhalten, welche sie betreffende personenbezogene Daten verarbeitet werden. Natürliche Personen sollten über die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten informiert und darüber aufgeklärt werden, wie sie ihre diesbezüglichen Rechte geltend machen können.

Ergriffene Maßnahme: Es erfolgt eine Auszeichnung der Videoüberwachung unter Beachtung der Anforderungen des Artikel 13 DS-GVO.

10 Rechenschaftspflicht
Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (»Rechenschaftspflicht«).

3 Zweckbindung
(Personenbezogene Daten müssen für festgelegte, eindeutige und legitime Zwecke erhoben werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden; eine Weiterverarbeitung für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke gilt gemäß Artikel 89 Absatz 1 nicht als unvereinbar mit den ursprünglichen Zwecken (»Zweckbindung«); Artikel 5 Absatz 1 Buchstabe b).)

Erwägungsgrund 39: Insbesondere sollten die bestimmten Zwecke, zu denen die personenbezogenen Daten verarbeitet werden, eindeutig und rechtmäßig sein und zum Zeitpunkt der Erhebung der personenbezogenen Daten feststehen. [...] Personenbezogene Daten sollten nur verarbeitet werden dürfen, wenn der Zweck der Verarbeitung nicht in zumutbarer Weise durch andere Mittel erreicht werden kann.

4 Datenminimierung
(Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein (»Datenminimierung«); Artikel 5 Absatz 1 Buchstabe c).)

Erwägungsgrund 39: Die personenbezogenen Daten sollten für die Zwecke, zu denen sie verarbeitet werden, angemessen und erheblich sowie auf das für die Zwecke ihrer Verarbeitung notwendige Maß beschränkt sein.

5 Speicherbegrenzung
(Personenbezogene Daten müssen in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden (»Speicherbegrenzung«); Artikel 5 Absatz 1 Buchstabe e).)

Erwägungsgrund 39: Dies erfordert insbesondere, dass die Speicherfrist für personenbezogene Daten auf das unbedingt erforderliche Mindestmaß beschränkt bleibt. [...] Um sicherzustellen, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden, sollte der Verantwortliche Fristen für ihre Löschung oder regelmäßige Überprüfung vorsehen.

6 Richtigkeit
(Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden (»Richtigkeit«); Artikel 5 Absatz 1 Buchstabe d).).

Erwägungsgrund 39: Es sollten alle vertretbaren Schritte unternommen werden, damit unrichtige personenbezogene Daten gelöscht oder berichtigt werden.

7 Persönliche Teilhabe und Zugang

10 Rechenschaftspflicht
Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (»Rechenschaftspflicht«).

Risiko-Sicht

8 Integrität und Vertraulichkeit
(Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen (»Integrität und Vertraulichkeit«);

Erwägungsgrund 39: Personenbezogene Daten sollten so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen diese verarbeitet werden, benutzen können.

9 Verfügbarkeit (Belastbarkeit);
Artikel 32 Absatz 2

Der Verantwortliche ist für die Einhaltung des Absatzes 1 verantwortlich und muss dessen Einhaltung nachweisen können (»Rechenschaftspflicht«).

Maßnahmenkatalog der CNIL

Die CNIL gibt eine Übersicht an Datenschutz-Maßnahmen.[15] Die einzelnen Maßnahmen werden im PIA Manual 3 der CNIL erläutert. Da dieser Maßnahmenkatalog vor der Verabschiedung der DS-GVO erstellt worden ist, müssen die gesetzlich geforderten Maßnahmen um die Datenschutz-Anforderungen der CNIL ergänzt werden. Die anderen Maßnahmenblöcke können so übernommen werden.

1. Rechtliche Kontrolle (zwingend)	
Verarbeitungszweck: bestimmter, eindeutiger und berechtigter Zweck der Verarbeitung	Daten
Minimierung: Strenge Begrenzung des Umfangs der personenbezogenen Daten auf das für die Erfüllung des Zwecks Erforderliche	Daten
Qualität: Gewährleistung der Qualität personenbezogener Daten	Daten
Aufbewahrungsdauer: Zeitraum, der für die Zweckerreichung erforderlich ist, es sei denn, es besteht eine andere Rechtspflicht zur längeren Speicherung	Daten
Information: Erfüllung der Informationspflichten gegenüber natürlichen Personen	Daten
Einwilligung: Einholung der Einwilligung der natürlichen Person oder das Eingreifen eines gesetzlichen Erlaubnistatbestandes für die Datenverarbeitung	Daten
Widerspruchsrecht: Gewährleistung des Rechts auf Widerspruch gegen die Datenverarbeitung	Daten
Auskunftsrecht: Gewährleistung des Rechts natürlicher Personen Auskunft über die Datenverarbeitung zu verlangen	Daten
Recht auf Berichtigung: Gewährleistung des Rechts natürlicher Personen ihre Daten berichtigen und löschen zu lassen	Daten
Drittstaatenübermittlung: Einhaltung der gesetzlichen Bestimmungen für die Übermittlung von Daten an Stellen außerhalb der europäischen Union	Daten
Vorabkontrolle: Bestimmung und Einhaltung von Formalien vor Beginn der Datenverarbeitung	Daten

2. Organisatorische Kontrolle	
Organisation	organisationsübergreifend
Richtlinien (Management von Regeln)	organisationsübergreifend
Risiko-Management	organisationsübergreifend
Projekt-Management	organisationsübergreifend
Management von Vorfällen und Datenschutzverletzungen	Auswirkung
Management von Mitarbeitern	Risikoquelle

15 CNIL, PIA Manual 2 - Privacy Impact Assessment (PIA) – Tools (templates and knowledge bases), 2015, Seite 7 ff.

Beziehungen zu Dritten	Risikoquelle
Wartung	Risikoquelle
Aufsicht (Audits, Dashboards, etc.)	organisationsübergreifend
Kennzeichnung von Dokumenten	Risikoquelle
Archivierung	organisationsübergreifend

3. Logische Sicherheitsmaßnahmen

Anonymisierung	Daten
Verschlüsselung	Risikoquelle
Integritäts-Checks	Auswirkung
Backups	Auswirkung
Datenpartitionierung	Risikoquelle
Logische Zugriffskontrolle	Risikoquelle
Nachvollziehbarkeit	Risikoquelle
Abläufe	Unterstützender Wert
Überwachung (Einstellungen, Konfigurationssteuerung, echt-zeit Überwachung)	Unterstützender Wert
Arbeitsplatzorganisation	Unterstützender Wert
Schutz vor schädlichem Code (Viren, Spyware, Software-Bomben)	Risikoquelle
Schutz der Kanäle (Netzwerk)	Unterstützender Wert

4.Physische Sicherheitsmaßnahmen

Vermeidung von Risikoquellen (Gefährliche Produkte, gefährliche geographische Ortslagen etc.)	Risikoquelle
Physische Zugangskontrolle	Risikoquelle
Hardwareschutz	Unterstützender Wert
Sicherheit im Umgang mit Papierdokumenten	Unterstützender Wert
Sicherheit bei der Weitergabe	Unterstützender Wert
Schutz vor natürlichen Risikoquellen (Feuer, Wasser etc.)	Risikoquelle

Maßnahmenkatalog aus der ISO/IEC DIS 29151

Die ISO/IEC FDIS 29151:2016 schlägt dem Anwender einen erweiterten Maßnahmenkatalog vor.[16]

A.1 Generelle Regeln für die Verarbeitung und den Schutz personenbezogener Daten

A.2 Einwilligung und Wahlmöglichkeit
- A.2.1 Einwilligung
- A.2.2 Wahlmöglichkeit

A.3 Zulässigkeit des Zwecks und Zweckbestimmung
- A.3.1 Zulässigkeit des Zwecks
- A.3.2 Zweckbestimmung

A.4 Erhebungsbeschränkung
- A.4.1 Erhebungsbeschränkung

A.5 Datenvermeidung und Datensparsamkeit
- A.5.1 Datenvermeidung und Datensparsamkeit

A.6 Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung
- A.6.1 Beschränkung bei der Nutzung, Aufbewahrung und Offenlegung
- A.6.2 Sicheres Löschen temporärer Dateien
- A.6.3 Informationspflichten
- A.6.4 Aufzeichnung der Offenlegung von pbD
- A.6.5 Offenlegung der im Unterauftrag ausgeführten Verarbeitung von pbD

A.7 Genauigkeit und Qualität
- A.7.1 Datenqualität

A.8 Offenheit, Transparenz und Benachrichtigung
- A.8.1 Benachrichtigung
- A.8.2 Offenheit und Transparenz

A.9 Persönliche Teilnahme und Zugang
- A.9.1 Hauptzugang
- A.9.2 Abhilfemaßnahmen und Mitwirkung
- A.9.3 Beschwerde-Management

16 Da die ISO/IEC FDIS 29151:2016 lediglich in einer englischen Fassung vorliegt, wurde hier auf die Übersetzung der ISO/IEC 27018:2014 zurückgegriffen. Lag keine Übersetzung vor, wurde vom Autor oder der Bitkom-Geschäftsstelle eine Übersetzung angefertigt.

A.10 Verantwortlichkeit

- A.10.1 Governance
- A.10.2 Datenschutz-Folgenabschätzung
- A.10.3 Datenschutzbestimmungen für Subunternehmer und Auftragsdatenverarbeiter
- A.10.4 Überwachung und Überprüfung des Datenschutzes
- A.10.5 Sensibilisierung und Training im Umgang mit personenbezogenen Daten
- A.10.6 Berichtssystem

A.11 Informationssicherheit

A.12 Einhaltung der Datenschutzpflichten

- A.12.1 Compliance
- A.12.2 Einschränkungen des grenzüberschreitenden Datentransfers in bestimmten Rechtsordnungen Die Struktur des Maßnahmenkataloges für die Maßnahmen der Informationssicherheit richtet sich nach der Struktur des Anhang A der DIN ISO/IEC 27001:2015 und wird hier nochmal wiedergegeben. Allerdings ist zu beachten, dass die Maßnahmen des Anhang A der DIN ISO/IEC 27001:2015 in der ISO/IEC FDIS 29151:2016[17] um spezifische Handlungsinhalte des Datenschutzes ergänzt werden, so wird z. B. bei der Maßnahme »5.1.1 Richtlinien für die Informationssicherheit« auch auf eine Datenschutz-Leitlinie eingegangen.

5 Informationssicherheitsrichtlinien

- 5.1 Managementausrichtung zur Informationssicherheit
  - 5.1.1 Richtlinien für die Informationssicherheit
  - 5.1.2 Überprüfung der Richtlinien für die Informationssicherheit

6 Organisation der Informationssicherheit

- 6.1 Interne Organisation
  - 6.1.1 Mit der Informationssicherheit verbundene Aufgaben und Verantwortlichkeiten
  - 6.1.2 Funktionstrennung
  - 6.1.3 Kontakt zu Behörden
  - 6.1.4 Kontakt zu speziellen Interessengruppen
  - 6.1.5 Informationssicherheit im Projektmanagement
- 6.2 Mobilgeräte und von zuhause Arbeiten (»Teleworking«)

7 Personalsicherheit

- 7.1 Vor Beginn eines Anstellungsverhältnisses
- 7.2 Während des Anstellungsverhältnisses
  - 7.2.1 Managementverantwortlichkeiten
  - 7.2.2 Sensibilisierung, Ausbildung und Schulung zur Informationssicherheit
  - 7.2.3 Disziplinarverfahren
- 7.3 Beendigung und Änderung des Anstellungsverhältnisses

17 Da die ISO/IEC FDIS 29151:2016 lediglich in einer englischen Fassung vorliegt, wurde hier auf die Übersetzung der ISO/IEC 27018:2014 zurückgegriffen.

8 Verwaltung der Werte

9 Zugangsprüfung

- 9.1 Geschäftliche Anforderungen in Bezug auf die Zugangsprüfung
- 9.2 Benutzerzugangsverwaltung
  - 9.2.1 Registrierung und Deregistrierung von Benutzern
  - 9.2.2 Zuteilung von Benutzerzugängen
  - 9.2.3 Verwaltung privilegierter Zugangsrechte
  - 9.2.4 Verwaltung geheimer Authentifizierungsdaten von Benutzern
  - 9.2.5 Überprüfung von Benutzerzugangsrechten
  - 9.2.6 Entzug oder Anpassung von Zugangsrechten
- 9.3 Benutzerverantwortlichkeiten
  - 9.3.1 Gebrauch geheimer Authentifizierungsdaten
- 9.4 Zugangssteuerung für Systeme und Anwendungen
  - 9.4.1 Informationszugangsbeschränkung
  - 9.4.2 Sichere Anmeldeverfahren
  - 9.4.3 System zur Verwaltung von Kennwörtern
  - 9.4.4 Gebrauch von Hilfsprogrammen mit privilegierten Rechten
  - 9.4.5 Zugangssteuerung für Quellcode von Programmen

10 Kryptographie

- 10.1 Kryptographische Maßnahmen
  - 10.1.1 Richtlinie zum Gebrauch von kryptographischen Maßnahmen
  - 10.1.2 Schlüsselverwaltung

11 Physische und umgebungsbezogene Sicherheit

- 11.1 Sicherheitsbereiche
- 11.2 Geräte und Betriebsmittel
  - 11.2.1 Platzierung und Schutz von Geräten und Betriebsmitteln
  - 11.2.2 Versorgungseinrichtungen
  - 11.2.3 Sicherheit der Verkabelung
  - 11.2.4 Instandhaltung von Geräten und Betriebsmitteln
  - 11.2.5 Entfernen von Werten
  - 11.2.6 Sicherheit von Geräten, Betriebsmitteln und Werten außerhalb der Räumlichkeiten
  - 11.2.7 Sichere Entsorgung oder Wiederverwendung von Geräten und Betriebsmitteln19
  - 11.2.8 Unbeaufsichtigte Benutzergeräte
  - 11.2.9 Richtlinie für eine aufgeräumte Arbeitsumgebung und Bildschirmsperren

12 Betriebssicherheit

- 12.1 Betriebsabläufe und -verantwortlichkeiten
  - 12.1.1 Dokumentierte Bedienabläufe
  - 12.1.2 Änderungssteuerung
  - 12.1.3 Kapazitätssteuerung
  - 12.1.4 Trennung von Entwicklungs-, Test- und Betriebsumgebungen

- 12.2 Schutz vor Schadsoftware
- 12.3 Datensicherung
  - 12.3.1 Sicherung von Informationen
- 12.4 Protokollierung und Überwachung
  - 12.4.1 Ereignisprotokollierung
  - 12.4.2 Schutz der Protokollinformation
  - 12.4.3 Administratoren- und Bedienerprotokolle
  - 12.4.4 Uhrensynchronisation
- 12.5 Steuerung von Software im Betrieb
- 12.6 Handhabung technischer Schwachstellen
- 12.7 Audit von Informationssystemen

13 Kommunikationssicherheit

- 13.1 Netzwerksicherheitsmanagement
- 13.2 Informationsübertragung
  - 13.2.1 Richtlinien und Verfahren zur Informationsübertragung
  - 13.2.2 Vereinbarungen zur Informationsübertragung
  - 13.2.3 Elektronische Nachrichtenübermittlung
  - 13.2.4 Vertraulichkeits- oder Geheimhaltungsvereinbarungen

14 Anschaffung, Entwicklung und Instandhaltung von Systemen

15 Lieferantenbeziehungen

16 Handhabung von Informationssicherheitsvorfällen

- 16.1 Handhabung von Informationssicherheitsvorfällen und Verbesserungen
  - 16.1.1 Verantwortlichkeiten und Verfahren
  - 16.1.2 Meldung von Informationssicherheitsereignissen
  - 16.1.3 Meldung von Schwächen in der Informationssicherheit
  - 16.1.4 Beurteilung von und Entscheidung über Informationssicherheitsereignisse(n)
  - 16.1.5 Reaktion auf Informationssicherheitsvorfälle
  - 16.1.6 Erkenntnisse aus Informationssicherheitsvorfällen
  - 16.1.7 Sammeln von Beweismaterial

17 Informationssicherheitsaspekte des Managements zur Aufrechterhaltung des Geschäfts im Krisenfall

18 Regelkonformität

- 18.1 Einhaltung von rechtlichen und vertraglichen Anforderungen
- 18.2 Überprüfungen der Informationssicherheit
- 18.2.1 Unabhängige Überprüfung der Informationssicherheit
  - 18.2.2 Einhaltung von Sicherheitsrichtlinien und -standards
  - 18.2.3 Überprüfung der Einhaltung von technischen Vorgaben

Begriffe

Begriff	Bedeutung	Quelle
Betroffener	»betroffene Person« im Sinne der DS-GVO: natürliche Person, auf die sich Daten und Informationen beziehen, die einer Verarbeitung unterliegen.	Art. 4 Abs. 1 DS-GVO
Compliance	Übereinstimmung mit gesetzlichen Vorschriften, insbesondere der DS-GVO	
Compliance-Risiko	Risiko des Verantwortlichen, dass er gesetzliche Vorschriften, insbesondere der DS-GVO verletzt	
Datenschutzrisiko	Risiko natürlicher Personen, dass ihre Rechte und Freiheiten verletzt werden	
DSFA	Datenschutz-Folgenabschätzung	
DS-GVO	Datenschutz-Grundverordnung	
Interessierte Parteien	Person oder Organisation, die an Entscheidungen oder Tätigkeiten beteiligt oder davon betroffen ist. Der Begriff umfasst Betroffene, Management von Verantwortlichen und Auftragsverarbeitern, Aufsichtsbehörden, Kunden, auch Verbände oder Vereinigungen. (Engl. Stakeholder)	ISO/IEC FDIS 29134:2017 Erwägungsgrund 99 DS-GVO
Pb Daten	Personenbezogene Daten	
Verantwortlicher	natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;	Art. 4 Abs. 1 DS-GVO
Verarbeitung	Vorgang oder Vorgangsreihe im Zusammenhang mit personenbezogenen Daten, die mit oder ohne Hilfe automatisierter Verfahren ausgeführt werden	Art. 4 Abs. 2 DS-GVO

Literaturverzeichnis

DIN ISO 31000:2011, Risikomanagement – Grundsätze und Leitlinien, 2011.

DIN ISO/IEC 27001:2015, Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen (ISO/IEC 27001:2013 + Cor. 1:2014), 2015.

DIN ISO/IEC 27002:2016, Informationstechnologie – IT-Sicherheitsverfahren – Leitfaden für Informationssicherheits-Maßnahmen (ISO/IEC 27002:2013 + Cor. 1:2014 + Cor. 2:2015), 2016.

ISO Guide 73:2009-11, Risk management – Vocabulary, 2009.
↗ https://www.iso.org/obp/ui/#iso:std:iso:guide:73:ed-1:v1:en

ISO/IEC 27005:2011, Information technology – Security techniques – Information security risk management, 2011.

ISO/IEC 27018:2014, Information technology – Security techniques – Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors, 2014.

ISO/IEC 29100:2011, Information technology — Security techniques — Privacy framework, 2011.

ISO/IEC FDIS 29134:2017, Information technology – Security techniques – Guidelines for privacy impact assessment, 2017.

ISO/IEC FDIS 29151:2016, Information technology – Security techniques – Code of practice for personally identifiable information protection.

CNIL, PIA Manual 1 – Privacy Impact Assessment (PIA) – Methodology (how to carry out a PIA), 2015. ↗ https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf

CNIL, PIA Manual 2 – Privacy Impact Assessment (PIA) – Tools (templates and knowledge bases), 2015. ↗ https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-2-Tools.pdf

CNIL, PIA Manual 2 – Measures fort he privacy risk treatment– Good Practices, 2012.
↗ https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-3-GoodPractices.pdf

Art. 29-Datenschutzgruppe, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is »likely to result in a high risk« for the purposes of Regulation 2016/679. ↗ http://ec.europa.eu/newsroom/document.cfm?doc_id=44137

Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder, Das Standard-Datenschutzmodell – Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele.
↗ https://datenschutzzentrum.de/uploads/SDM-Methode_V_1_0.pdf

Bitkom vertritt mehr als 2.400 Unternehmen der digitalen Wirtschaft, davon gut 1.600 Direktmitglieder. Sie erzielen mit 700.000 Beschäftigten jährlich Inlandsumsätze von 140 Milliarden Euro und stehen für Exporte von weiteren 50 Milliarden Euro. Zu den Mitgliedern zählen 1.000 Mittelständler, 300 Start-ups und nahezu alle Global Player. Sie bieten Software, IT-Services, Telekommunikations- oder Internetdienste an, stellen Hardware oder Consumer Electronics her, sind im Bereich der digitalen Medien oder der Netzwirtschaft tätig oder in anderer Weise Teil der digitalen Wirtschaft. 78 Prozent der Unternehmen haben ihren Hauptsitz in Deutschland, 9 Prozent kommen aus Europa, 9 Prozent aus den USA und 4 Prozent aus anderen Regionen. Bitkom setzt sich insbesondere für eine innovative Wirtschaftspolitik, eine Modernisierung des Bildungssystems und eine zukunftsorientierte Netzpolitik ein.

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10
10117 Berlin
T 030 27576-0
F 030 27576-400
bitkom@bitkom.org
www.bitkom.org

bitkom