



DATA **PRIVACY**

DATA PROTECTION MANUAL

Handbuch zum Datenschutzmanagementsystem
des Rheinmetall Konzerns für den Rechtsraum der EU/EWR

Version 2 | 01. November 2021

INHALTSVERZEICHNIS

A	ALLGEMEINER TEIL	5
1	Ziel und Zweck	5
2	Herausgeber	5
3	Geltungsbereich	5
4	Schnittstelle	6
5	Mitgeltende Unterlagen	6
6	Verfahrensbegleitende Dokumente	7
7	Änderungsdienst	7
8	Gültigkeit	7
9	Hinweise zum Lesen des Dokuments	7
B	BESONDERER TEIL DATENSCHUTZMANAGEMENTSYSTEM	8
1	Allgemeines	8
1.1	Einleitung	8
1.2	Rollen	9
1.3	Begriffe A – Z	9
1.4	Abkürzungen	11
2	Allgemeine Vorgaben zum Datenschutzmanagement	12
2.1	Datenschutzmanagementsystem	12
2.2	Verantwortlichkeiten und Gestaltungsmöglichkeiten der Zuständigkeiten	12
2.3	Aspekte des Datenschutzmanagementsystems	12
2.4	Verarbeitung, Asset und Verarbeitungstätigkeit	12
2.5	Allgemeines zur Data Privacy Organization	13
2.6	Delegation und Zentralisierungsfähigkeit von datenschutzrelevanten Prozessen	13
3	Datenschutz-Governance und -Organisation im Rheinmetall Konzern	17
3.1	Datenschutz Governance	17
3.2	Verantwortlichkeiten und Zuständigkeiten	17
3.3	Steuerung des Datenschutzes im Rheinmetall Konzern	28
3.4	Regelmäßige Überprüfung und Fortschreibung des DSMS	29
4	Gestaltung datenschutzkonformer Prozesse	30
4.1	Einleitung	30
4.2	Besonderheiten im Konzern	30
4.3	Auslöser des Prozesses „datenschutzkonforme Verarbeitung“	31
4.4	Zuständigkeit bei Datenverarbeitungen und Projekten	35
4.5	Rechtmäßigkeit der Verarbeitung	36
4.6	Informationspflichten	41

4.7	Datenübermittlung an Drittländer oder an internationale Organisationen (EU)	43
4.8	Löschung, Sperrung, Anonymisierung und Berichtigung von Daten	47
4.9	„Privacy by Design“ und „Privacy by Default“	50
4.10	Risiko im Datenschutz	53
4.11	Technische und organisatorische Maßnahmen (TOM)	60
4.12	Datenschutz-Folgenabschätzung (DSFA)	64
5	Verarbeitungstätigkeiten, Assets und verarbeitungsbasierte Risiken	68
5.1	Einleitung	68
5.2	Allgemeine Vorgaben zu den Verarbeitungs- und Asset-Beschreibungen	68
5.3	Vorgaben zum Verzeichnisses von Verarbeitungstätigkeiten (VVT)	71
6	Datenverarbeitungsdienstleister und gemeinsam Verantwortliche	77
6.1	Allgemeine Vorgaben	77
6.2	Beauftragung von Auftragsverarbeitern	77
6.3	Gemeinsame Verantwortliche	80
6.4	Tätigwerden als Auftragsverarbeiter	82
7	Betroffenenrechte	85
7.1	Gestaltung des Prozesses bei Rheinmetall	85
7.2	Auskunftsrecht	90
7.3	Recht auf Berichtigung der Daten	92
7.4	Recht auf Löschung	93
7.5	Einschränkung der Verarbeitung	94
7.6	Datenportabilität	96
7.7	Widerspruch gegen die Verarbeitung	97
8	Datenschutzvorfälle	100
8.1	Einleitung	100
8.2	Meldung an die Aufsichtsbehörde und an die betroffene Person 72 Stunden	100
8.3	Datenschutzverletzung im Rahmen von Auftragsverarbeitungsverhältnissen	102
8.4	Entfallen der Meldepflicht	102
8.5	Dokumentation	103
8.6	Rollen und Verantwortung	103
9	Verpflichtung von Beschäftigten	105
9.1	Einleitung	105
9.2	Beschreibung	105
9.3	Dokumentation	105
9.4	Rollen und Verantwortung	105
10	Schulung und Awareness	107
10.1	Einleitung	107
10.2	Beschreibung	107

10.3	Dokumentation	107
10.4	Rollen und Verantwortung	108
11	Sonstiges und besondere Verarbeitungssituationen	109
11.1	Umgang mit Beschäftigtendaten	109
11.2	Videoüberwachung (Deutschland)	111
11.3	Automatisierte Entscheidungen im Einzelfall (einschließlich Profiling)	115
11.4	Wissenschaftliche oder historische Forschungszwecke und statistische Zwecke	116
11.5	Zusammenarbeit mit der Datenschutz-Aufsichtsbehörde	118
11.6	Vorherige Konsultation	119
11.7	Verhaltensregeln	120
11.8	Webseiten und Social-Media-Auftritte	121
C	DOKUMENTENMANAGEMENT	125

A ALLGEMEINER TEIL

1 Ziel und Zweck

Das Data Protection Manual (hier auch Datenschutzhandbuch) konkretisiert das in der Datenschutz-Leitlinie definierte Datenschutzmanagementsystem (DSMS) des Rheinmetall Konzerns und beschreibt im Detail die Prozesse und organisatorischen Voraussetzungen zur Bearbeitung der Anforderungen des Datenschutzes und der Fortschreibung dieser Regelungen.

Zum primären Adressatenkreis gehören neben der Data Privacy Organization insbesondere die Schnittstellenbereiche (vgl. Ziffer 4) sowie Fachbereiche, die in ihrem Tätigkeitsumfeld verstärkt datenschutzrelevante Aspekte berücksichtigen müssen. Grundsätzlich richtet sich das Handbuch jedoch an alle Beschäftigten und ermöglicht durch seinen thematischen Aufbau eine gezielte Anwendung bei konkreten Fragestellungen.

Das Datenschutz-Handbuch konkretisiert darüber hinaus die Verantwortlichkeiten und Zuständigkeiten der in der Datenschutz-Leitlinie definierten Rollen.

Die Regelungen sollen sowohl betroffene Personen (z. B. Beschäftigte¹ der Rheinmetall oder Beschäftigte von Lieferanten, Dienstleistern und Kunden) bei der Datenverarbeitung durch den Rheinmetall Konzern schützen als auch die Unternehmen des Rheinmetall Konzerns vor Schaden bei Datenschutz-Verstößen bewahren (z. B. Bußgelder, Rufschädigung oder Schadenersatz).

2 Herausgeber

Herausgeber ist der Chief Compliance Officer als Leiter des Zentralbereichs Corporate Compliance der Rheinmetall AG.

Die Veröffentlichung des Datenschutzhandbuches erfolgt in deutscher und englischer Sprache. Über die Notwendigkeit der Veröffentlichung weiterer Sprachversionen wird im Einzelfall durch den Herausgeber entschieden.

3 Geltungsbereich

Inkraftsetzung

100%-Gesellschaften

Handbücher der Rheinmetall AG gelten nach erfolgter Bekanntgabe und Veröffentlichung im Intranet der Rheinmetall² für sämtliche Gesellschaften im Rheinmetall Konzern, bei denen die Rheinmetall AG direkt bzw. indirekt Alleingesellschafterin ist. Sie sind von den zuständigen Organen dieser Gesellschaften in geeigneter Weise so umzusetzen, dass sie für alle Organe und relevanten Mitarbeiter/Beschäftigten der jeweiligen Gesellschaft verbindlich gelten.

Gemeinschaftsunternehmen (Joint Venture)

Bei Gemeinschaftsunternehmen³ ist unter Berücksichtigung der Regelungen in den Gesellschaftervereinbarungen auf entsprechende Vorgaben sachgerecht hinzuwirken. Ist eine Umsetzung dieser Vorgaben im Gemeinschaftsunternehmen nicht möglich, ist Compliance⁴ zu informieren.

Rechtliche Implementierung auf Ebene der Konzerngesellschaft

In Kraft gesetzte Handbücher der Rheinmetall AG sind entsprechend der im Regulation Management Manual

¹ Aus Gründen der leichten Lesbarkeit werden in diesem Dokument sowie in sämtlichen, darauf aufbauenden Regelungen - soweit geschlechtsneutrale Formulierungen nicht verwendet werden können - ausschließlich die männlichen Formulierungen verwendet. Gemeint sind damit jedoch stets Menschen jeglicher geschlechtlichen Identität, sprich männlich, weiblich und divers und soweit in anderen Ländern vorgesehen, entsprechende Differenzierungen für den Begriff „divers“.

² Details siehe Regulation Management Manual, Abschnitt B, Ziffer 2, Prozessschritt 5.

³ Mehrheitsbeteiligung, 50%/50%-Beteiligung sowie Minderheitsbeteiligungen bis zu einer Beteiligungsschwelle von mindestens 25 %.

⁴ Die Division Compliance Officer informieren hierzu Corporate Compliance.

beschriebenen Verfahren⁵, bei der Konzerngesellschaft rechtlich wirksam zu implementieren, um so deren tatsächliche Anwendung in relevanten Gesellschaften sicher zu stellen⁶. Handbücher sollen dabei grundsätzlich unmittelbar Anwendung finden.

Soweit Vorgaben des Handbuchs nicht umgesetzt werden können - insbesondere aufgrund des lokalen Rechts - ist der Herausgeber hierüber unverzüglich und umfassend zu informieren. Sich daraus ableitende Änderungserfordernisse sind zu begründen. Der Herausgeber entscheidet sodann, ob die Vorgaben mit Änderungen umgesetzt werden sollen. Weiterhin hat dieser seinerseits erforderlichenfalls Anpassungen am Handbuch vorzunehmen oder ergänzende Landesregelungen zu erstellen, die eine sachgerechte Umsetzung ermöglichen.

Besondere Umsetzungsaufträge

Das vorliegende Datenschutzhandbuch gilt für alle Unternehmen des Rheinmetall Konzerns im Geltungsbereich der EU Datenschutz-Grundverordnung (DSGVO) und als Orientierung für alle Unternehmen des Rheinmetall Konzerns, bei denen die Datenschutz-Leitlinie in Kraft gesetzt wurde.

Unternehmen des Rheinmetall Konzerns außerhalb des Anwendungsbereiches der DSGVO übernehmen entweder dieses Datenschutzhandbuch nebst Datenschutz-Leitlinie oder beschreiben für sich das Datenschutzmanagement in einem eigenen DSMS in adäquater Form und legen dieses dem Corporate Data Privacy Officer zur Genehmigung vor.

4 Schnittstelle

Die Data Privacy Organization erbringt Leistungen für alle (Matrix-) Organe, Führungskräfte und Mitarbeiter im Rheinmetall Konzern. Mit dieser Querschnittsfunktion hat der Fachbereich somit Schnittstellen in nahezu alle Bereiche des Rheinmetall Konzerns.

Ungeachtet dessen besteht funktional eine enge Beziehung zu den Fachbereichen

- Einkauf / Purchasing
- HR
- IT / IT-Security
- Informationssicherheit
- Security

5 Mitgeltende Unterlagen

Folgende Regelungen sind bei der Anwendung dieses Handbuchs zu berücksichtigen:

- Group Manual | Vorstandsvorgabe
- Datenschutz-Leitlinie des Rheinmetall Konzerns | Vorstandsvorgabe - Compliance / Data Privacy
- Richtlinie Personenbezogene Daten in der Matrixorganisation | HR
- Richtlinie zum Notfall- und Krisenmanagement | Security
- Informationssicherheits Management System / ISMS Manual | IT⁷

⁵ Details siehe Regulation Management Manual, Abschnitt B Ziffer 2, Prozessschritt 6.

⁶ Die Verteilung erfolgt durch den Herausgeber über die Divisionen in die nachgeordneten Gesellschaften sowie direkt an die Shared Service-Gesellschaften. Die Divisionen entscheiden ihrerseits über die weitere Verteilung zur Pflichtimplementierung nach dem Need-to-know-Prinzip.

⁷ Zum Zeitpunkt der Erstellung dieses Manuals in Arbeit.

6 Verfahrensbegleitende Dokumente

Nachfolgende Dokumente stehen zur Anwendung dieses Handbuches zur Verfügung:

Zu erarbeitende Richtlinien für besondere Regelungsbereiche, vertiefende (Verfahrens-/Prozess-/Arbeits-) Anweisungen, Muster und sonstige Hilfestellungen.

7 Änderungsdienst

Die Aktualisierung dieses Datenschutzhandbuchs obliegt ausschließlich dem Herausgeber.

Diese erfolgt alle **drei Jahre** sowie anlassbezogen.

8 Gültigkeit

Dieses Handbuch wird durch den Vorstand der Rheinmetall AG freigegeben und gilt ab dem **01.11.2021**.

Mit Veröffentlichung dieses Handbuches verlieren die Vorversion „Datenschutzhandbuch – Verbindliche Regeln im Datenschutz“ Version 2019 1.1 vom 31.05.2019 sowie die „OA UBD 11 Richtlinie zur Auftragsverarbeitung vom 01.04.2015“ ihre Gültigkeit.

9 Hinweise zum Lesen des Dokuments

Die in dieser Art hervorgehobenen Texte sind von allen Rheinmetall Gesellschaften im Anwendungsbereich des Handbuchs zwingend zu beachten.

Der übrige Text dient der allgemeinen Erläuterung.

B BESONDERER TEIL | DATENSCHUTZMANAGEMENTSYSTEM

1 Allgemeines

1.1 Einleitung

Personenbezogene Daten unterliegen dem Datenschutz. Bei der Verarbeitung personenbezogener Daten sind für die EU/EWR die EU Datenschutz-Grundverordnung (DSGVO) und für Deutschland zusätzlich das Bundesdatenschutzgesetz (BDSG) sowie weitere gesetzliche Vorgaben zu beachten. Darüber hinaus sind für die Durchführung spezieller Aufgaben bereichsspezifische Vorschriften anzuwenden. Hierzu zählen z. B. in Deutschland das Telekommunikationsgesetz (TKG), das Telemediengesetz (TMG) oder die Vorschriften zum Risikomanagement aus dem Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG).

Zudem gibt es weltweit gesetzliche Vorgaben zum Datenschutz. Datenschutz bezeichnet den Schutz des Einzelnen vor Beeinträchtigung seiner Persönlichkeitsrechte beim Umgang mit seinen personenbezogenen Daten.

In der EU sieht die DSGVO erhebliche Bußgelder nicht nur für tatsächliche, materielle Datenschutzverstöße, sondern auch für die Nichteinhaltung formaler Vorgaben aus der DSGVO vor. Dafür enthält die DSGVO eine Nachweispflicht für Unternehmen, die von ihnen verlangt, jederzeit den Nachweis führen zu können, dass die Regelungen aus der DSGVO eingehalten werden. Weitere Sanktionen können sich aus Verletzungen anderer Rechtsvorschriften ergeben.

Die erforderlichen technischen und organisatorischen Sicherheitsmaßnahmen sowie die Abwicklung von Sicherheitsvorfällen sind Bestandteil des Informationssicherheitsmanagementsystems (ISMS) der jeweiligen Unternehmen des Rheinmetall Konzerns sowie der zentralen Vorgaben der Unternehmenssicherheit zum Umgang mit Krisen und werden im Datenschutzhandbuch nicht beschrieben. Unabhängig davon stellt der Datenschutz hohe Anforderung an die Sicherheit von personenbezogenen Daten. Insofern ist das DSMS auf ein effektives ISMS angewiesen, zudem existieren diverse Schnittstellen, die zu beschreiben und zu bedienen sind. Der Datenschutz (die *Data Privacy Organization*) ist an dieser Stelle ein sogenannter Bedarfsträger gegenüber der Informationssicherheit und der Unternehmenssicherheit, d. h. das Gesetz formuliert gewisse Anforderungen an technische und organisatorische Schutzmaßnahmen (Datensicherheit) oder an ein Incident-Management. Diese Anforderungen werden im Datenschutzhandbuch beschrieben und sind bei entsprechenden Prozessen der Informationssicherheit und der Unternehmenssicherheit zu beachten.

Dieses Handbuch stellt in diesem Abschnitt in **Ziffer 2⁸** allgemeine Vorgaben und in **Ziffer 3** die Datenschutz-Governance, die Datenschutz Organisation sowie eine erste Übersicht der Aufgaben und Zuständigkeiten im Rheinmetall Konzern dar. Ab **Ziffer 4** werden die Datenschutz-Kernprozesse und die zentralen Subprozesse sowie der zentrale Prozess zur „*Gestaltung datenschutzkonformer Prozesse*“ beschrieben.

Ziffer 5 erläutert, wie diese Prozesse in Form von Verarbeitungstätigkeiten und Assets datenschutzkonform beschrieben und dokumentiert werden müssen, um die gesetzlichen Dokumentations-, Nachweis- und Rechenschaftspflichten (insbes. nach DSGVO und BDSG) zu erfüllen, aber auch um ein proaktives Datenschutzmanagement zu etablieren.

In **Ziffer 6** werden die Anforderungen an die Ausgliederung von Verarbeitungstätigkeiten auf externe Dienstleister, sogenannte Datenverarbeitungsdienstleister, beschrieben.

Ziffer 7 stellt die Prozesse, die zur Erfüllung der gesetzlich verbrieften Rechte von der Datenverarbeitung betroffener Personen eingehalten werden müssen, dar.

Ziffer 8 beschreibt die Prozesse, die bei Vorliegen eines Datenschutzvorfalls ergänzend zu einem Informationssicherheits-Incident-Management beachtet und eingehalten werden müssen. Üblicherweise beschreibt das ISMS ein Informationssicherheits-Incident-Management und die Informationssicherheit betreibt dieses. Im Rheinmetall Konzern wird zudem ein Vorfall, der potentiell öffentlichkeitswirksam (z. B. negative Presse, Bußgeld, Meldung an Datenschutzaufsichtsbehörde) ist, als Krisenfall definiert und im Zuge des Krisenstabmanagements behandelt. Die Rheinmetall Incident Organization (RIO) wird von der Unternehmenssicherheit betrieben, die Prozesse und Zuständigkeiten hierzu sind in der „Richtlinie zum Notfall- und Krisenmanagement“ beschrieben. Die

⁸ Sofern nicht anderweitig angegeben, beziehen sich alle Angaben auf den Abschnitt B dieses Handbuchs.

in Ziffer 8 beschriebenen datenschutzrechtlichen Anforderungen der Unternehmen des Rheinmetall Konzerns aus der EU an das Incident-Management sind in einer Anlage zu diesem Handbuch berücksichtigt.

Ziffer 9 regelt die Verpflichtung von Beschäftigten zur Einhaltung des Datenschutzes.

Ziffer 10 stellt die Zuständigkeiten bei Schulungen und Awareness-Maßnahmen dar, während in **Ziffer 11** besondere Verarbeitungssituationen, wie z. B. die Videoüberwachung, beschrieben werden.

1.2 Rollen

Innerhalb der Data Privacy Organization bei Rheinmetall sind folgende Rollen festgelegt:

Rollen	Verortung innerhalb der Organisation	View
Corporate Data Privacy Officer	Rheinmetall AG	Management
Data Privacy Officer	Divisionen	Management
Data Privacy Manager	Gesellschaften	Management
Regional Data Privacy Manager	Land/Region	Management
Datenschutzkoordinator	Fachbereich	Legal
Datenschutzbeauftragter	Rheinmetall AG und Gesellschaften (Legale Einheiten)	Legal

Deren ebenen-spezifische bzw. ereignisbezogene Aufgaben sowie weitere relevante Rollen ergeben sich aus den nachfolgenden Ziffern 4 bis 11.

1.3 Begriffe A – Z

Begriff	Erläuterung
Asset (Vereinfachte Darstellung)	Assets sind häufig IT-Systeme/-Anwendungen, die zur Unterstützung von Geschäftsprozessen eingesetzt werden. Digitale Assets: IT-Systeme/-Anwendungen/-Lösungen (z. B. Cisco WebEx, Microsoft Excel, SAP HCM, SharePoint, Gruppenlaufwerk, Lotus Notes, Empower, Server XY-) Analoge Assets: analoge Speichermedien/Aufbewahrungsorte wie z. B. Aktenschränke, Dokumentenarchive, Tresore.
Data Privacy Organization Datenschutz Organisation	Die Data Privacy Organization oder auch Datenschutz Organisation besteht aus dem Corporate Data Privacy Officer, den Data Privacy Officer, den Data Privacy Managern und den Regional Data Privacy Managern.
Datenschutz-Folgenabschätzung	Eine Datenschutz-Folgenabschätzung (DSFA) ist ein spezielles Instrument zur Beschreibung, Bewertung und Eindämmung von Risiken für die Rechte und Freiheiten natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die DSFA ist durchzuführen, wenn die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko zur Folge hat. Sie befasst sich insbesondere mit Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der Verordnung nachgewiesen werden kann. ⁹
Datenschutzrisiko	Ein Risiko im Sinne der DSGVO ist das Bestehen der Möglichkeit des Eintritts eines Ereignisses, das selbst einen Schaden (materiell oder immateriell) darstellt oder zu einem weiteren Schaden für eine oder mehrere natürliche Personen führen kann. Hierbei geht es um die Risiken für die von der Verarbeitung betroffenen Personen, nicht um Risiken für das Unternehmen! <u>Achtung:</u> „Unrechtmäßige Verarbeitungstätigkeiten oder Verarbeitungstätigkeiten, die nicht den Grundsätzen des Art. 5 DSGVO entsprechen, sind in sich Beeinträchtigungen des Grundrechts auf Datenschutz und stellen daher bereits ein Schadensereignis dar.“ ¹⁰

⁹ Hierzu auch Kurzpapier der Datenschutzkonferenz (DSK) Nr. 5.

¹⁰ Hierzu auch Kurzpapier der Datenschutzkonferenz (DSK) Nr. 18.

Begriff	Erläuterung
Ermittelnde Stelle	Die Abteilung, die Ermittlungen gegenüber dem Beschäftigten durchführt. Dies kann z. B. die Personalabteilung, Compliance-Abteilung oder die Informationssicherheit sein.
Federführende Kontaktstelle	Der Fachbereich, der für die jeweilige Betroffenengruppe (z. B. Beschäftigte, Bewerber) allgemein zuständig ist, muss die Bearbeitung von Anträgen dieser Betroffenengruppe als federführende Kontaktstelle vornehmen. Das wären grundsätzlich für Beschäftigte der Personalbereich, für Bewerber die Personalabteilung und Recruiting, für Lieferanten/Dienstleister der Einkauf, für Kunden der Vertrieb und für Adressaten von Werbung oder die Webseitenbesucher das Marketing.
Geschäftsprozess (Vereinfachte Darstellung)	Geschäftsprozesse sind vereinfacht die zusammenhängenden Folgen von Tätigkeiten, die in Unternehmen zur Erreichung bestimmter Unternehmensziele erledigt werden. Hierbei umfassen diese eine klar abgegrenzte, regelhafte Abfolge von Tätigkeiten und Entscheidungen, die aufeinander bezogen sind und schrittweise von eindeutig benannten Akteuren bzw. Instanzen ausgeführt werden, um ein bestimmtes organisatorisches Ziel zu erreichen. Beispiele: Reisekostenabrechnung, Geschäftspartnerprüfung, Beschäftigten-Onboarding, Betrieb einer bestimmten IT-Anwendung, Personalbewertung)
Personenbezogene Daten	Alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person („betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann. (Art. 4 Nr. 1 DSGVO). Beispiele: Allgemeine Personendaten (Name, Alter, Familienstand etc.), Kontaktdaten, physische Merkmale, Kennnummern, Werturteile, Gesundheitsdaten, IT-Daten (Logfiles, User-ID etc.). Auch „technische Daten“ können personenbezogene Daten sein, wenn sie sich auf eine Person zurückführen lassen (z. B. IP-Adresse).
Privacy by Default (auch: Datenschutzfreundliche Voreinstellung)	Datenschutzrechtlicher Grundsatz. Es ist sicherzustellen, dass Verarbeitungstätigkeiten und Assets durch geeignete technische und organisatorische Maßnahmen so voreingestellt werden, dass nur personenbezogene Daten verarbeitet werden, die für den Zweck der Verarbeitung tatsächlich erforderlich sind. Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Durch datenschutzfreundliche Voreinstellung sollen Unternehmen sicherstellen, dass personenbezogene Daten mit dem größtmöglichen Datenschutz (z. B. Datenminimierung, kurze Speicherfristen und begrenzte Zugänglichkeit) verarbeitet werden. Mehr dazu in Ziffer 4.9.2.
Privacy by Design (auch: Datenschutz durch Technikgestaltung)	Datenschutzrechtlicher Grundsatz. Jede Verarbeitung von personenbezogenen Daten muss angemessen technisch und organisatorisch abgesichert sein. Es müssen daher stets geeignete technische und organisatorische Maßnahmen (TOM) getroffen werden, die darauf ausgerichtet sind, die Datenschutzgrundsätze umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO sowie der Datenschutz-Leitlinie zu genügen und die Rechte der betroffenen Personen zu schützen. Unternehmen sind angehalten, zum frühestmöglichen Zeitpunkt der Gestaltung der Verarbeitungstätigkeiten (inkl. Auswahl der Mittel wie z. B. IT-Systeme/-Anwendungen) technische und organisatorische Maßnahmen zu treffen, die darauf ausgelegt sind, die Privatsphäre der von der Datenverarbeitung betroffenen Personen zu schützen und Datenschutzgrundsätze von Beginn an zu garantieren. Solche Maßnahmen können beispielsweise darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, eine starke Verschlüsselung der Daten implementiert wird, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung

Begriff	Erläuterung
	personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern. Mehr dazu siehe Ziffer 4.9.1.
Standarddatenschutzklauseln (auch: Standardvertragsklauseln)	Von der EU-Kommission herausgegebene Standardklauseln für die Legitimierung von Datenübermittlungen in Ländern außerhalb der EU/des EWR (Drittländer). Für Unternehmen im Rheinmetall Konzern innerhalb der EU/des EWR müssen zur Legitimierung eines Drittlandtransfers grundsätzlich die Standarddatenschutzklauseln eingesetzt werden. Gleichwohl sind zur Legitimierung des Drittlandtransfers darüber hinaus regelmäßig weitere technische und organisatorische Maßnahmen erforderlich.
Verarbeitungstätigkeit (Vereinfachte Darstellung)	Vereinfacht: Jeder Geschäftsprozess, in dem personenbezogene Daten vorkommen bzw. verarbeitet werden.

1.4 Abkürzungen

Abkürzung	Erläuterung
AVV	Auftragsverarbeitungsvertrag
DSFA	Datenschutz-Folgenabschätzung
DSGVO	Datenschutz-Grundverordnung (EU)
DSK	Datenschutzkonferenz
DSMS	Datenschutzmanagementsystem
ISMS	Informationssicherheitsmanagementsystem
EU-SVK	EU-Standardvertragsklauseln (auch EU-Standarddatenschutzklauseln)
RIO	Rheinmetall Incident Organization der Unternehmenssicherheit
TOM	Technische und organisatorische Maßnahmen
VVT	Verzeichnis von Verarbeitungstätigkeiten

2 Allgemeine Vorgaben zum Datenschutzmanagement

2.1 Datenschutzmanagementsystem

Mit Datenschutzmanagement werden die Prozesse und Organisation bezeichnet, die notwendig sind, um die Umsetzung der gesetzlichen Anforderungen des Datenschutzes bei der Planung, Einrichtung, dem Betrieb und nach Außerbetriebnahme von automatisierten oder datenschutzrechtlich gleichgestellten Verarbeitungen personenbezogener Daten sicherzustellen.

2.2 Verantwortlichkeiten und Gestaltungsmöglichkeiten der Zuständigkeiten

Die Unternehmen im Rheinmetall Konzern, die personenbezogene Daten verarbeiten oder verarbeiten lassen, tragen die Verantwortung für die datenschutzrechtliche Zulässigkeit und Ordnungsmäßigkeit der genutzten Assets und für die zugrundeliegenden Geschäftsprozesse. Zur effektiven Umsetzung der datenschutzrechtlichen Anforderungen stellt das vorliegende Datenschutzhandbuch auch die Möglichkeiten und Grenzen in Bezug auf die Zuordnung und Delegation von Zuständigkeiten dar.

2.3 Aspekte des Datenschutzmanagementsystems

2.3.1 Betroffene Personengruppen

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten durch Unternehmen des Rheinmetall Konzerns betreffen im Wesentlichen Beschäftigte (z. B. Angestellte und Auszubildende), Kunden bzw. Interessenten der angebotenen Produkte und Dienstleistungen, weitere Personen im Kontext von Vertragsbeziehungen (z. B. Ansprechpartner bei Kunden oder Dienstleistern), Beschäftigte der Geschäftspartner der Unternehmen des Rheinmetall Konzerns sowie Besucher der Webseiten, Social-Media-Auftritte, Standorte und Räumlichkeiten des Rheinmetall Konzerns.

Die *Data Privacy Organization* muss eine aktuelle Liste der potentiell betroffenen Personengruppen pflegen und stellt diese den Unternehmen zur Verfügung.

2.3.2 Zulässigkeit der Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten im Rheinmetall Konzern ist nur zulässig, soweit die Datenschutzgesetze oder eine andere Rechtsvorschrift dies erlauben oder anordnen (z. B. Vorschriften aus dem Handels- oder Steuerrecht). Darüber hinaus wird der Rheinmetall Konzern keine personenbezogenen Daten verarbeiten.

2.3.3 Rechenschaftspflicht und Dokumentationspflicht

Die Datenschutzgesetze (insbes. DSGVO) statuieren regelmäßig eine Rechenschaftspflicht. Erforderlich ist nicht nur die Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten, sondern auch die Fähigkeit, diese Einhaltung nachweisen zu können. Dazu besteht u. a. die Verpflichtung, geeignete technische und organisatorische Maßnahmen (TOM) zu implementieren, um sicherzustellen und den Nachweis dafür erbringen zu können, dass die Verarbeitung personenbezogener Daten datenschutzkonform erfolgt.

Die Dokumentation datenschutzrechtlicher Maßnahmen stellt nicht bloß eine prozessuale bzw. faktische Notwendigkeit dar, sondern wird durch die Datenschutzgesetze (u. a. DSGVO) zu einer ausdrücklichen, gesetzlichen Verpflichtung erhoben und dient zudem der Abwehr von Rechtsansprüchen Dritter gegen die Unternehmen des Rheinmetall Konzerns.

Darüber hinaus ist die Dokumentation der datenschutzrelevanten Prozesse regelmäßig Gegenstand von Auditierungs- und Zertifizierungsmaßnahmen.

2.4 Verarbeitung, Asset und Verarbeitungstätigkeit

Der Ausdruck „Verarbeitung“ bezeichnet jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten. Beispiele sind das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form

der Bereitstellung, der Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung von personenbezogenen Daten.¹¹

Die zu betrachtenden Verarbeitungen sind schrittweise und bedarfsgerecht für die Nachweisbarkeit differenziert zu dokumentieren. Dabei ist eine geeignete Abstraktionsebene (Prozessebene) zu wählen.

Eine grundsätzliche Festlegung für den Verarbeitungsprozess (Verarbeitungstätigkeit, Verarbeitung) im Rheinmetall Konzern ist, dass es sich bei einer Verarbeitung um einen Geschäftsprozess handelt, bei dem auch personenbezogene Daten vorkommen. Der Geschäftsprozess definiert regelmäßig den zugrundeliegenden Zweck einer Verarbeitungstätigkeit.

Unterstützt werden die Verarbeitungstätigkeiten von sogenannte Assets. Assets sind in diesem Kontext insbesondere IT-Tools, IT-Applikationen, IT-Systeme, Server, IT-Lösungen einschließlich webbasierter Anwendungen (digitale Assets). Daneben werden auch analoge Assets wie etwa Dokumentenarchive, Ordner oder Karteisysteme erfasst, die ebenfalls zu beschreiben sind (wie die digitalen Assets, hier allerdings nur in bestimmten Fällen, vgl. Ziffer 5.3).

Zuständig für die Beschreibung der Verarbeitungstätigkeit ist der Geschäftsprozess-Eigentümer (Prozesseigentümer). Er ist zugleich auch der Eigentümer der Verarbeitung (vgl. Ziffer 3.2.4.6).

Zuständig für die Beschreibung eines Assets ist derjenige, der dieses Asset verantwortet bzw. verwaltet (Asset-Eigentümer). Der Asset-Eigentümer und Prozesseigentümer können personenidentisch sein (vgl. Ziffer 3.2.4.7)

Zudem sind Prozess- und Asset-Eigentümer dafür zuständig, Ihre Prozesse und Assets datenschutzkonform zu gestalten und zu betreiben.

Die Data Privacy Organization stellt für die Dokumentation und Beschreibung der Verarbeitungstätigkeiten und Assets geeignete Tools und Templates zur Verfügung und berät Asset-Eigentümer und Prozesseigentümer diesbezüglich. Der zuständige Datenschutzbeauftragte steht bei Beratungsanfragen ebenfalls zur Verfügung (vgl. Ziffer 3.2.2)

2.5 Allgemeines zur Data Privacy Organization

Zum Schutz personenbezogener Daten ergreifen die Unternehmen im Rheinmetall Konzern eine Vielzahl von Maßnahmen. Das vorliegende Datenschutzhandbuch fasst Handlungsvorgaben zu datenschutzrelevanten Prozessen zusammen, sodass sie als Vorgabe zu einer methodischen und formalen Prozessmodellierung verwendet werden können. Hierzu enthält dieses Handbuch auch Kontrollprozesse zu den datenschutzrelevanten Prozessen und Dokumentationsanforderungen an die Ergebnisse der datenschutzrelevanten Prozesse und Kontrollen. Ebenfalls dargestellt werden die erforderlichen Skills und Kompetenzen seitens des Verantwortlichen für die Erfüllung der datenschutzrelevanten Prozesse und eine zugehörige Rollenbeschreibung unter Berücksichtigung des fachlichen Umfeldes.

Die Vorgaben des Handbuchs gelten unmittelbar oder werden falls erforderlich seitens des Verantwortlichen über weitere Handlungsvorgaben in Form von Anweisungen konkretisiert.

2.6 Delegation und Zentralisierungsfähigkeit von datenschutzrelevanten Prozessen

Die Verantwortung für die Einhaltung der Anforderungen aus dem Datenschutz liegt zunächst bei den Vorständen bzw. bei den Geschäftsführern des Verantwortlichen bzw. der Gesellschaft (nachfolgend „Geschäftsführung“). Mithin hat die Geschäftsführung Maßnahmen zu ergreifen, um Verstöße gegen Datenschutzbestimmungen zu verhindern.

Übertragen auf die funktionale Matrixorganisation im Rheinmetall Konzern bedeutet dies, dass diese Verantwortlichkeit ebenso auf die Leitung der Divisionen zutrifft.

Die Geschäftsführung kann die Zuständigkeit für die Umsetzung des Datenschutzes für die einzelnen Verarbeitungen auf Fachbereiche bzw. Funktionsstellen oder auch auf einzelne Personen übertragen. Das kann z. B. Personen etwa als Zuständige für ein abgegrenztes Projekt (Auftraggeber eines Projektes, Projekt-Verantwortlicher,

¹¹ Vgl. die Legaldefinition in Art. 4 Nr. 2 DSGVO.

Projektleiter), als Datenschutz-Koordinator oder als Prozesseigentümer (Eigentümer der Verarbeitung) oder Asset-Eigentümer betreffen.

Die Zuständigkeiten **müssen** klar definiert, kommuniziert und dokumentiert werden.

Wenn möglich, sind datenschutzrelevante Aufgaben, Zuständigkeiten und Prozesse, die zentralisierungsfähig sind, zu zentralisieren, um auf diese Weise benötigte Kompetenzen und Kapazitäten übergreifend nutzen zu können.

2.6.1 Erforderliche Skills und Kompetenzen

Für die organisatorische Zuordnung von Prozessen ist aus Sicht des Datenschutzes insbesondere eine Berücksichtigung folgender Kompetenzen zu beachten:

Skills & Kompetenz	Beschreibung
Fachliches Knowhow zum Prozess	Die Kenntnis der Verarbeitung personenbezogener Daten für eigene Zwecke wird als Kernkompetenz des Fachbereichs vorausgesetzt.
Technisches Knowhow zum Prozess	Die Kenntnis der genutzten technischen Verfahren zur Verarbeitung personenbezogener Daten wird als Kompetenz des Fachbereichs vorausgesetzt, die bei Bedarf in Zusammenarbeit mit den zuständigen IT-Bereichen und des Bereiches Informationssicherheit zu ergänzen ist.
Methodische Kompetenz	Die Kenntnisse zum methodischen Vorgehen zur Bearbeitung der datenschutzrelevanten Prozesse werden durch das Datenschutzhandbuch und weitere begleitende Vorgaben unterstützt. Sie erfordern eine Einarbeitung und zusätzliche Berücksichtigung neben dem jeweils eigenen fachlichen Umfeld und die Fähigkeit, Informationen zu beschaffen, zu strukturieren, zu bearbeiten und wieder zu verwenden und Ergebnisse von Verarbeitungsprozessen richtig zu interpretieren.
Kompetenz zur Risikobewertung	Die Verarbeitung personenbezogener Daten erfordert eine datenschutzrelevante Risikobewertung und dafür die Fähigkeit, Risikobewertungen nach einer vorgegebenen Methodik unter Berücksichtigung der fachlichen Zusammenhänge durchzuführen.
Datenschutzrechtliche Kompetenz	Zur Bearbeitung der datenschutzrelevanten Prozesse unter Berücksichtigung der fachlichen Zusammenhänge sind Kenntnisse der relevanten Datenschutzregelungen erforderlich, die über den erforderlichen Rahmen für das fachliche Tagesgeschäft hinausgehen.

2.6.2 Datenschutzrelevante Kernkompetenzen

Aufbauend auf die in Ziffer 2.6.1 beschriebenen Anforderungen werden die datenschutzrelevanten Kernkompetenzen der in Frage kommenden Funktionen folgendermaßen eingeschätzt:

	Fachbereich	Data Privacy Organization	Datenschutzbeauftragter
Fachliches Knowhow zum Prozess	++	o -> +	o/+
Technisches Knowhow zum Prozess	++	o -> +	o/+
Methodische Kompetenz	o	++	+
Kompetenz zur Risikobewertung	o	++	++
Datenschutzrechtliche Kompetenz	o	+ bis ++	++

Legende:

o: Standardkenntnisse

+: erweiterte Standardkenntnisse

++: umfangreiche Kenntnisse

o -> +: Kenntnisaufbau

o/+ : Im Rahmen von Überwachung, Kontrollen und Beratung Aufbau erweiterter Kenntnisse

2.6.2.1 Fachbereich

Der Fachbereich ist durch seine regelmäßigen Tätigkeiten gut mit fachlichen Fragen aus seinem Verantwortungsbereich vertraut und kennt das Geschäft des Rheinmetall Konzerns. Je nach konkretem Betätigungsfeld des Fachbereichs resultieren hieraus auch gute Kenntnisse der entsprechenden technischen Verfahren.

Wenn die zusätzliche Bearbeitung datenschutzrelevanter Prozesse im Fachbereich weniger häufig stattfindet, sind der Aufbau und das Vorhalten der erforderlichen Kenntnisse hierfür im Fachbereich vergleichsweise aufwändig.

2.6.2.2 Data Privacy Organization / Datenschutz Organisation

Die Data Privacy Organization (hier auch Datenschutz Organisation) setzt sich insbesondere mit der operativen Anwendung des Datenschutzrechts sowie der Weiterentwicklung des DSMS auseinander und besteht aus dem Corporate Data Privacy Officer, den Data Privacy Officern, den Data Privacy Managern¹² und den Regional Data Privacy Managern¹³.

Die Stärke einer zentralen Data Privacy Organization liegt in erster Linie in der gebündelten methodischen Kompetenz, die aufgrund der regelmäßigen Inanspruchnahme mit erweiterten Kenntnissen zu relevanten datenschutzrechtlichen Fragestellungen ergänzt wird. Hierdurch können die Einheitlichkeit der Beachtung der datenschutzrechtlichen Anforderungen innerhalb des Rheinmetall Konzerns sowie die formalen Vorgaben an die Dokumentation der Ergebnisse sichergestellt werden.

In der Zusammenarbeit mit den Fachbereichen können sich die Beschäftigten auch weiterhin auf ihre eigene fachliche Kompetenz konzentrieren, während sie durch die Data Privacy Organization beraten, unterstützt und zielgerichtet geschult werden.

Eine zentrale Data Privacy Organization ist unabhängig gegenüber den jeweiligen Eigeninteressen der Fachbereiche, die etwa für die geforderten Formalismen einer Datenschutz-Folgenabschätzung (DSFA)¹⁴ oder aber auch der Bewertung einer datenschutzrechtlichen Zulässigkeit von Datenverarbeitungen relevant sind.

Eine systematische Fortschreibung und Weiterentwicklung des DSMS sowie der datenschutzrelevanten Prozesse und der dafür erforderlichen Materialien sowie Regelungen ist seitens des Rheinmetall Konzerns mit Verankerung in der Data Privacy Organization leistbar.

Eine ausführliche Darstellung der Aufgaben und der Funktion der Data Privacy Organization im Rheinmetall Konzern erfolgt ab Ziffer 3.2.2.

2.6.2.3 Datenschutzbeauftragter¹⁵

Der Datenschutzbeauftragte verfügt in seiner gesetzlichen Rolle über eine datenschutzrechtliche Kernkompetenz und kann durch die Beratung der Fachbereiche und der Data Privacy Organization die Einheitlichkeit der Anwendung des Datenschutzrechts innerhalb des Rheinmetall Konzerns fördern. Im Rahmen der Kontakte und seiner eigenen Überwachungstätigkeiten werden die Kenntnisse in fachlichen und technischen Verarbeitungen bedarfsweise ausgebaut. Sein Tätigwerden entspricht dem gesetzlichen Leitbild des Datenschutzbeauftragten aus der DSGVO.¹⁶

Während bei der Data Privacy Organization die operative Anwendung des Datenschutzrechts sowie die Weiterentwicklung des DSMS im Vordergrund stehen, werden dem Datenschutzbeauftragten (engl. Data Protection Officer) laut Gesetz überwachende Aufgaben zugeschrieben. Insofern ist eine zentrale Aufgabe des Datenschutz-

¹² Zuvor Datenschutz-Ansprechpartner.

¹³ Zuvor regionaler Datenschutz-Ansprechpartner.

¹⁴ Vgl. Art. 35 DSGVO.

¹⁵ Die Benennung eines Datenschutzbeauftragten unterliegt den Anforderungen aus der DSGVO und in Deutschland aus dem BDSG. Eine Benennungspflicht eines Datenschutzbeauftragten oder einer vergleichbaren Rolle ist durch die Verantwortlichen in den jeweiligen Ländern anhand der nationalen Regelungen zu prüfen.

¹⁶ Vgl. Art. 39 Abs. 1 DSGVO.

beauftragten die Überwachung der Einhaltung der DSGVO, anderer Datenschutzvorschriften sowie der Strategien der Unternehmen des Rheinmetall Konzerns zum Schutz personenbezogener Daten. Mithin überwacht er auch die Tätigkeiten der Data Privacy Organization.

Die Aufgaben und Funktion des Datenschutzbeauftragten werden in Kapitel 3.2.4.8 ausführlicher beschrieben.

3 Datenschutz-Governance und -Organisation im Rheinmetall Konzern

3.1 Datenschutz Governance

Das Group Manual des Rheinmetall Konzerns definiert funktional in einer Matrixorganisation geführte Geschäftsbereiche, die unternehmensübergreifend geführt werden (Management View). Unabhängig von den Anforderungen, die das Group Manual an eine Matrix-Organisation stellt, müssen die Unternehmen im Rheinmetall Konzern jeweils eigenständig den Datenschutz beachten, da die Datenschutzgesetze das Unternehmen, d. h. die einzelnen Unternehmen im Rheinmetall Konzern, adressieren (Legal View).

Diesen Umstand müssen die Datenschutz Organisation und das Datenschutzmanagementsystem der Rheinmetall Group berücksichtigen.

Verantwortlichkeiten und Zuständigkeiten im Datenschutz **müssen** im Rheinmetall Konzern (Management View) und in den Unternehmen im Rheinmetall Konzern (Legal View) eindeutig und widerspruchsfrei festgelegt und dokumentiert werden.

Bei der Verteilung der Zuständigkeiten und Verantwortlichkeiten im Datenschutz **muss** das Prinzip der Funktionstrennung umgesetzt werden, um insbesondere potentielle Interessenkonflikte wirksam ausschließen zu können. Widersprüchliche Verantwortlichkeiten **dürfen nicht** von ein und derselben Person oder Organisationseinheit wahrgenommen werden.

Wenn eine Funktionstrennung nicht oder nur mit unverhältnismäßig hohem Aufwand durchführbar ist, können widersprüchliche Verantwortlichkeiten von ein und derselben Person oder Organisationseinheit wahrgenommen werden.

Werden widersprüchliche Verantwortlichkeiten von ein und derselben Person oder Organisationseinheit wahrgenommen, **muss** die rechtliche Zulässigkeit geprüft und Maßnahmen wie

- Überwachung von Tätigkeiten,
- Kontrollen oder Leitungsaufsicht umgesetzt und
- die nicht durchgeführte Funktionstrennung

in der Dokumentation der Funktionsverteilung besonders hervorgehoben werden.

Um Verantwortlichkeiten im Datenschutz wahrzunehmen, **müssen** die Beschäftigten im erforderlichen Umfang von anderen Tätigkeiten freigestellt werden.

Verantwortliche für den Datenschutz **dürfen** Aufgaben an andere Personen delegieren. Die Verantwortung für die delegierten Aufgaben verbleibt jedoch bei ihnen, sodass sie die Erfüllung und das Ergebnis der delegierten Aufgaben überprüfen **müssen**.

Nachfolgend werden die Rollen und Berichtslinien in Grundzügen beschrieben.

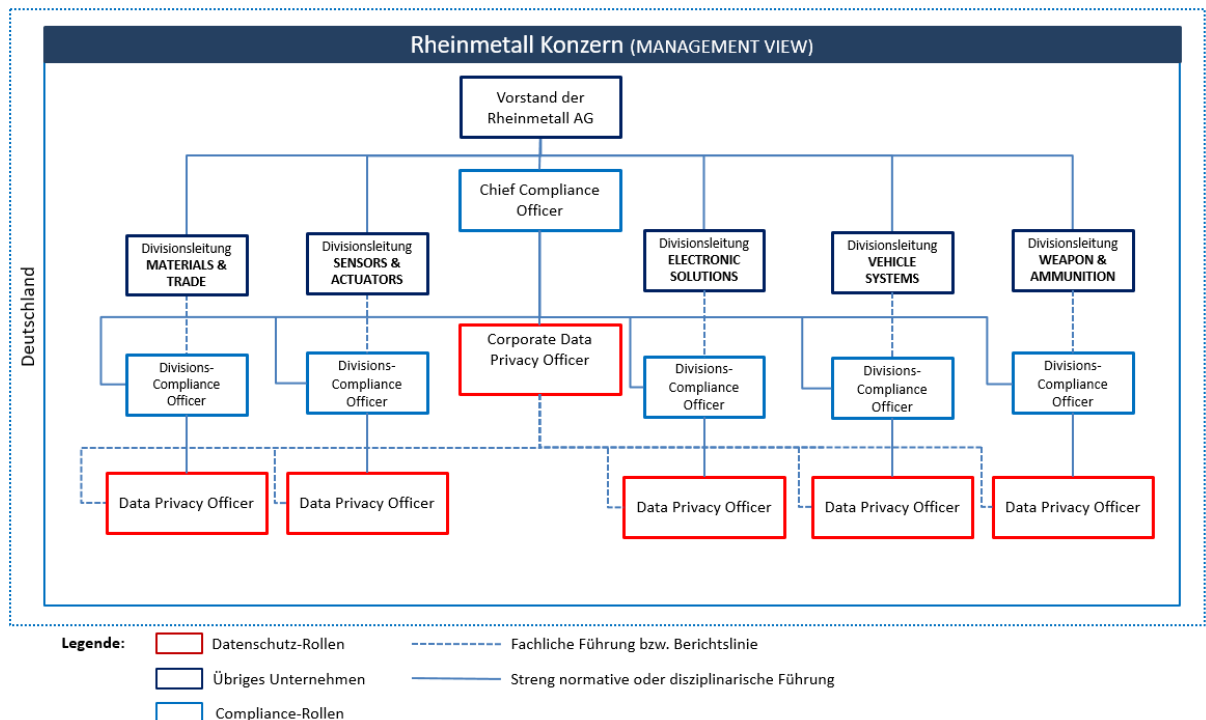
3.2 Verantwortlichkeiten und Zuständigkeiten

3.2.1 Organisation des Datenschutzes bei Rheinmetall¹⁷

In diesem Abschnitt werden in Grundzügen die Rollen beschrieben, die der Datenschutz Organisation in der Matrix des Rheinmetall Konzerns zuzuordnen sind, um den Datenschutz im Rheinmetall Konzern unternehmensübergreifend einheitlich und möglichst ressourcenschonend umzusetzen.

¹⁷ Management View.

3.2.1.1 Datenschutz Organisation in Deutschland | Management View



3.2.1.2 Vorstand und Chief Compliance Officer der Rheinmetall AG

Der Vorstand der Rheinmetall AG ist für die Etablierung und Umsetzung eines konzernweiten Datenschutzmanagementsystems verantwortlich. Zu diesem Zweck hat der Vorstand der Rheinmetall AG die Compliance Organisation und den Chief Compliance Officer der Rheinmetall AG mit der Aufgabe betraut, den Datenschutz konzernweit umzusetzen und ein effektives Datenschutzmanagementsystem zu etablieren.

3.2.2 Data Privacy Organization

3.2.2.1 Corporate Data Privacy Officer

Der *Vorstand* der Rheinmetall AG **muss** auf Konzern-Ebene einen *Corporate Data Privacy Officer* benennen.

Der Corporate Data Privacy Officer ist bei der Rheinmetall AG im Bereich Compliance angesiedelt. Für die Rheinmetall AG übernimmt er zusätzlich die Aufgaben des Data Privacy Managers.

Der Corporate Data Privacy Officer führt die Data Privacy Officer fachlich. Der Corporate Data Privacy Officer berichtet disziplinar an den Chief Compliance Officer.

Wesentliche Aufgaben des Corporate Data Privacy Officers sind:

- Zusammenführen der Anforderungen an das Datenschutzmanagementsystem.
- Einberufen regelmäßiger Treffen der Data Privacy Organization und fachliche Führung der Data Privacy Officer.
- Koordination der Bewertung gruppenweiter Verarbeitungsprozesse sowie IT-Lösungen.
- Koordination der Umsetzung und Durchsetzung des Datenschutzmanagementsystems.
- Weiterentwicklung des Datenschutzmanagementsystems des Rheinmetall Konzerns.
- Regelmäßiger Bericht an den Chief Compliance Officer und an den Vorstand der Rheinmetall AG.
- Abstimmung und Koordination der Zusammenarbeit mit dem Datenschutzbeauftragten.

3.2.2.2 Data Privacy Officer

Aufgrund der Position des Data Privacy Officers auf Divisionsebene soll der Data Privacy Officer die Einheitlichkeit der Umsetzung des Datenschutzmanagementsystems innerhalb des Rheinmetall Konzerns sicherstellen, indem

er die Unternehmen in seinem Verantwortungsbereich hinsichtlich des Datenschutzes fachlich führt und anleitet, entweder über die Data Privacy Manager oder über die Geschäftsführungen. Der Data Privacy Officer ist in der Compliance-Organisation angesiedelt und wird disziplinarisch vom Divisions-Compliance Officer geführt.

Die *Data Privacy Officer* der Divisionen **müssen** von der jeweiligen Divisionsleitung in Abstimmung mit dem *Corporate Data Privacy Officer* benannt werden.

Der Data Privacy Officer führt in Deutschland die Data Privacy Manager in seinem Verantwortungsbereich fachlich hinsichtlich der Anforderungen aus dem Datenschutzmanagementsystem.

Der Data Privacy Officer führt die im Ausland ansässigen Regional Data Privacy Manager und Data Privacy Manager in seinem Verantwortungsbereich fachlich hinsichtlich der Anforderungen aus dem Datenschutzmanagementsystem (siehe nachfolgende Abbildung in Ziffer 3.2).

Der *Data Privacy Officer* **kann** zudem die Aufgaben des *Data Privacy Managers* übernehmen, sofern die erforderlichen Kapazitäten vorhanden sind. Im Rahmen der Benennung sind die in Ziffer 3.2.3.1 aufgeführten Anforderungen zu beachten.

Die *Data Privacy Officer* **müssen** an den *Corporate Data Privacy Officer* berichten. Der Bericht **muss** mindestens zweimonatlich sowie anlassbezogen erfolgen.

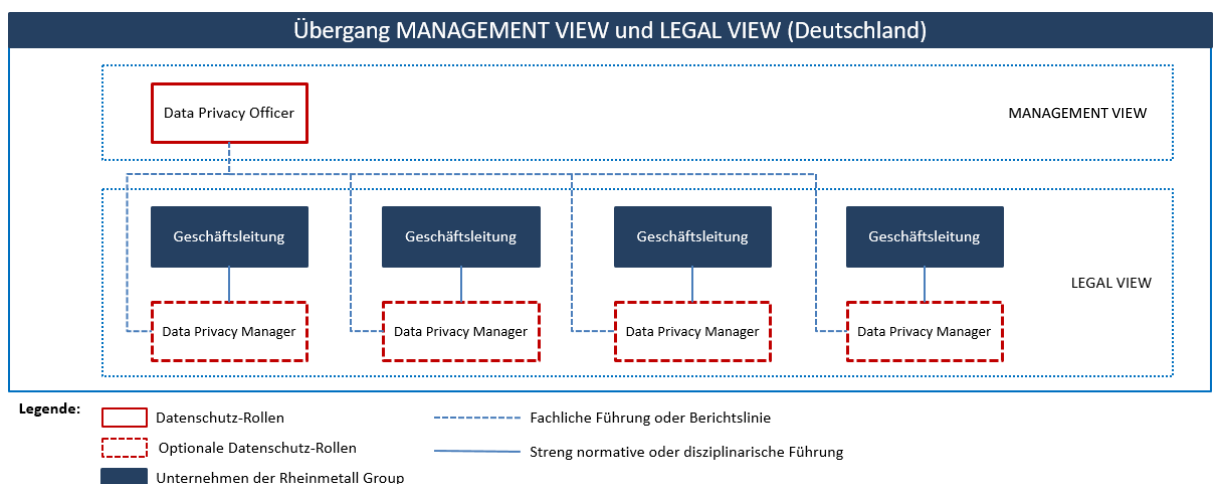
Die *Data Privacy Officer* **dürfen** sich in Fragen des Datenschutzes und Datenschutzmanagementsystems an den *Corporate Data Privacy Officer* wenden.

Wesentliche Aufgaben des Data Privacy Officers sind:

- Die kontinuierliche Verbesserung und Weiterentwicklung des Datenschutzmanagementsystems unter fachlicher Führung des Corporate Data Privacy Officers.
- Die Bewertung gesetzlicher Anforderungen und Umsetzung durch Implementierung und Aufrechterhaltung des konzernweiten Datenschutzmanagementsystems in seinem Verantwortungsbereich.
- Der regelmäßige Bericht an den Corporate Data Privacy Officer und an die für sie zuständigen Divisions-Compliance Officer sowie bei Bedarf an die Divisionsleitung.
- Die Übernahme divisionsübergreifender datenschutzrechtlicher Experten-Themen, gesteuert durch den Corporate Data Privacy Officer.
- Abstimmung und Zusammenarbeit mit dem Datenschutzbeauftragten der Division.

3.2.3 Data Privacy Organization innerhalb und außerhalb Deutschlands¹⁸

3.2.3.1 Data Privacy Manager



¹⁸ Management View und Übergang Legal View.

Die *Geschäftsführungen* der Unternehmen im Rheinmetall Konzern **dürfen** ihre datenschutzbezogenen Aufgaben auf einen *Data Privacy Manager* delegieren. Dieser *Data Privacy Manager* **muss** formal benannt und dessen Aufgaben dokumentiert werden.

Die Benennung des Data Privacy Managers erfolgt grundsätzlich schriftlich durch die Geschäftsführung der durch ihn betreuten Gesellschaften.

Benennt die Geschäftsführung keinen Data Privacy Manager, so muss die Geschäftsführung die Aufgaben des Data Privacy Managers erfüllen und ist insofern Teil der Data Privacy Organization. Der Data Privacy Manager stellt die wesentliche Schnittstelle zwischen der Data Privacy Organization und dem übrigen Unternehmen dar.

Der *Data Privacy Officer* **kann** zugleich *Data Privacy Manager* sein, sofern sichergestellt ist, dass die für seine Aufgaben erforderlichen Kapazitäten vorhanden sind. Sollte der *Data Privacy Officer* zugleich *Data Privacy Manager* eines Unternehmens im Rheinmetall Konzern werden, **muss** die Benennung schriftlich durch die *Geschäftsführung* erfolgen.

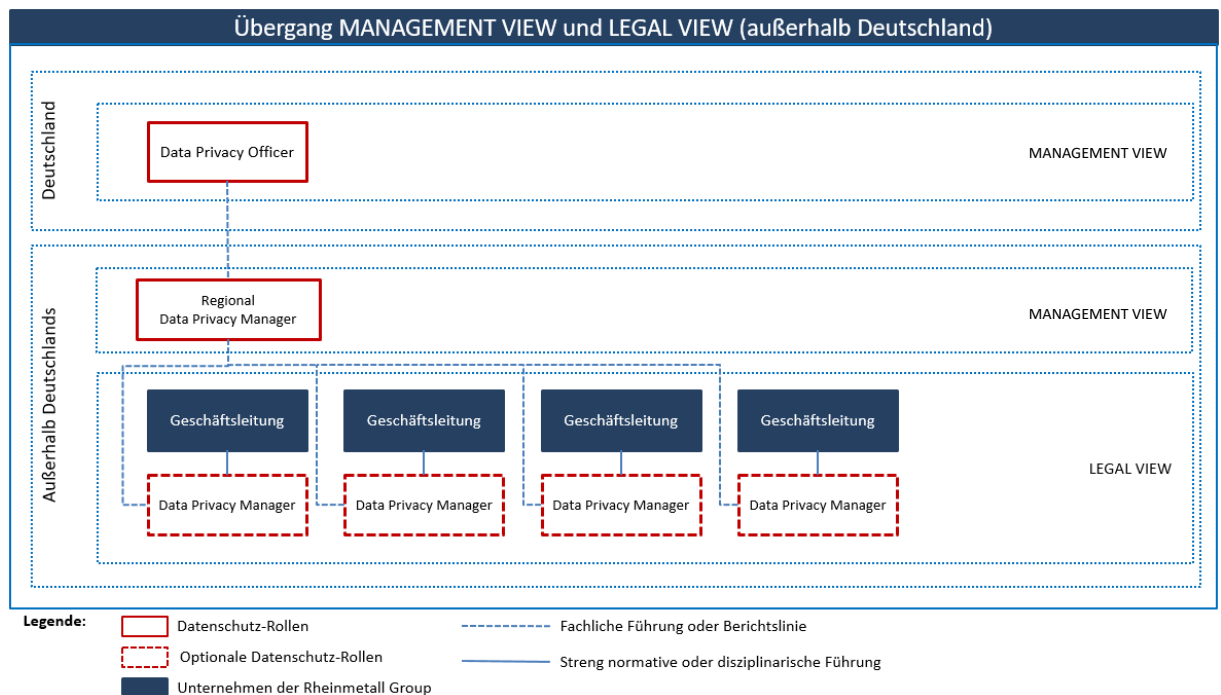
Die *Data Privacy Manager* **dürfen** sich in Fragen des Datenschutzes und Datenschutzmanagementsystems an den *Corporate Data Privacy Officer* und an den für sie zuständigen *Data Privacy Officer* wenden.

Die *Data Privacy Manager* **müssen** an den für sie zuständigen *Data Privacy Officer* berichten. Der Bericht **sollte** monatlich erfolgen.

Wesentliche Aufgaben des Data Privacy Managers sind:

- Schnittstelle zwischen der globalen Data Privacy Organization (Management View) und der lokalen Datenschutz Organisation (Legal View).
- Hinwirken auf die Umsetzung der Vorgaben aus den Datenschutzgesetzen und dem Datenschutzmanagementsystem.
- Hinwirken auf die Einhaltung der Dokumentationspflichten, die Information der betroffenen Personen und die Gewährung von Betroffenenrechten.
- Regelmäßiger Bericht an den Data Privacy Officer und an die für sie zuständigen Compliance Officer.

3.2.3.2 Regional Data Privacy Manager



In jedem Land außerhalb Deutschlands, in dem Unternehmen im Rheinmetall Konzern ihren Sitz haben (sogenannter „Sitzland“), **muss** ein gesellschaftsübergreifender Data Privacy Manager für die Unternehmen in diesem Land, ein sogenannter *Regional Data Privacy Manager*, benannt werden.

Um die landesspezifischen Anforderungen zu ermitteln, **darf** der *Regional Data Privacy Manager* auf die in seinem Verantwortungsbereich ansässigen *Data Privacy Manager* zurückgreifen. Die *Data Privacy Manager* **müssen** den *Regional Data Privacy Manager* unterstützen.

Die *Data Privacy Manager* eines Sitzlandes **müssen** mit dem *Regional Data Privacy Manager* zusammenarbeiten und mindestens einmal im Quartal an ihn berichten.

Der *Regional Data Privacy Manager* hat auf fachlicher Ebene mit der Compliance Organisation zusammenzuarbeiten und benötigt datenschutzrechtliches Fachwissen bezüglich seines Sitzlandes (insbesondere zum lokalen Datenschutzrecht).

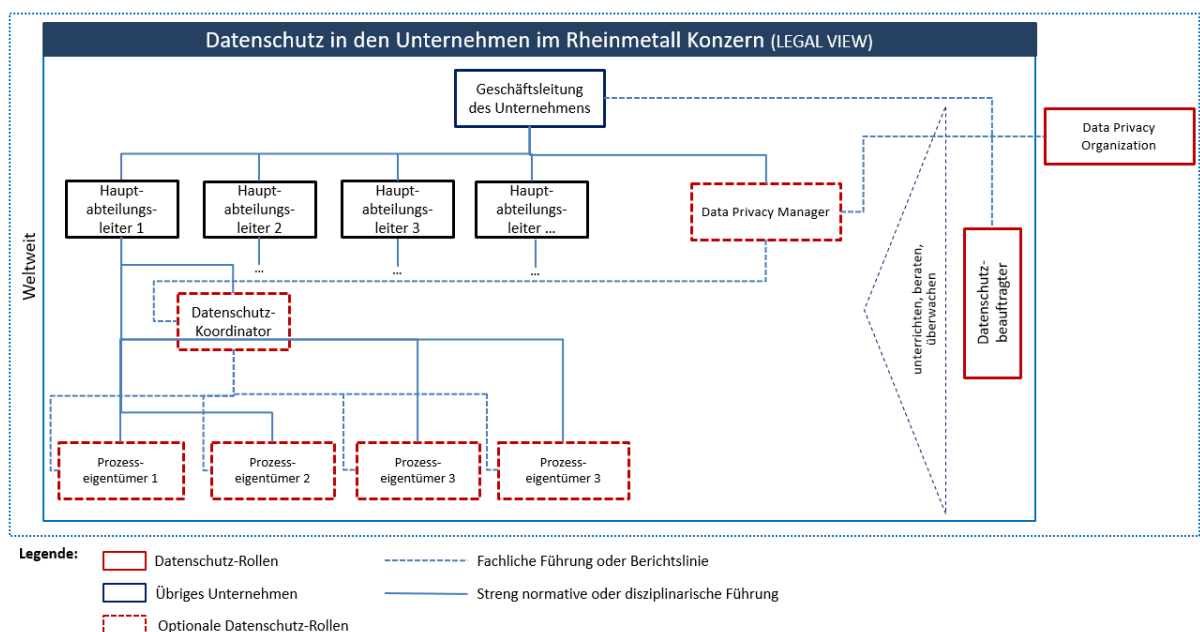
Der *Regional Data Privacy Manager* **muss** hinsichtlich der Umsetzung des Datenschutzmanagementsystems und Datenschutz-Vorfälle an den für ihn zuständigen *Data Privacy Officer* berichten. Der Bericht hinsichtlich der Umsetzung des Datenschutzmanagementsystems **muss** mindestens vierteljährlich und bei Datenschutz-Vorfällen mindestens monatlich erfolgen.

Die *Regional Data Privacy Manager* **dürfen** sich in Fragen des Datenschutzes und Datenschutzmanagementsystems an den *Corporate Data Privacy Officer* und an den für sie zuständigen *Data Privacy Officer* wenden.

Wird kein *Regional Data Privacy Manager* benannt, so werden dessen Aufgaben in Abstimmung mit den Geschäftsführungen im Sitzland von dem für die Region zuständigen *Compliance Officer* zugewiesen.

3.2.4 Verantwortlichkeiten und Zuständigkeiten in den Unternehmen und Fachbereichen¹⁹

In diesem Abschnitt werden in Grundzügen die Aufgaben und die Rollen des Datenschutz-Managements in der Organisation beschrieben, die in den einzelnen Unternehmen im Rheinmetall Konzern auf Ebene des Verantwortlichen wahrgenommen werden können und müssen.



In diesem Zusammenhang werden zunächst die Rollen und Aufgaben beschrieben, die der übrigen Organisation zuzuordnen sind und anschließend die Aufgaben und Funktionen, die eher der Datenschutz Organisation zuzuordnen sind.

¹⁹ Außerhalb der Data Privacy Organization.

3.2.4.1 Unternehmen

Der „Verantwortliche“ ist für die Einhaltung des Datenschutzes verantwortlich. Der Verantwortliche ist dabei die natürliche oder juristische Person (das Unternehmen), welche über die Zwecke und Mittel der Verarbeitung personenbezogener Daten entscheidet. Der Verantwortliche muss die Einhaltung der Datenschutz-Grundsätze dokumentieren und gegenüber der zuständigen Datenschutzaufsichtsbehörde nachweisen können.

Die Unternehmen im Rheinmetall Konzern **müssen** sicherstellen, dass sie die Datenschutz-Grundsätze einhalten und die Einhaltung nachweisen können.

3.2.4.2 Geschäftsführung

Das Unternehmen wird nach außen durch die Geschäftsführung vertreten. Damit trifft die Verantwortung für die Einhaltung des Datenschutzes grundsätzlich die Geschäftsführung der jeweiligen für die Datenverarbeitung verantwortlichen Unternehmen im Rheinmetall Konzern.

Die *Geschäftsführungen* der Unternehmen im Rheinmetall Konzern **müssen** sicherstellen, dass ein Datenschutzmanagementsystem entsprechend den Vorgaben für die Unternehmen im Rheinmetall Konzern eingeführt und umgesetzt wird.

Für die Erfüllung der Anforderungen aus den Datenschutz-Gesetzen und die Umsetzung des Datenschutzmanagementsystems **muss** die *Geschäftsführung* die erforderlichen Ressourcen zur Verfügung stellen.

3.2.4.3 Hauptabteilungsleiter | Main Department Head und andere Führungskräfte

Die *Beschäftigten*, die einen Geschäftsbereich oder eine Hauptabteilung führen („Hauptabteilungsleiter“), **müssen** für ihren Verantwortungsbereich die Einhaltung der datenschutzrechtlichen Anforderungen sicherstellen.

Abteilungsleiter haben die Einhaltung der datenschutzrechtlichen Anforderungen gleichermaßen sicherzustellen. Wenn nachfolgend von Hauptabteilungsleitern geschrieben wird, so gilt dies auch für die Abteilungsleiter.

Die *Hauptabteilungsleiter* **müssen** die Geschäftsprozesse in ihrem Verantwortungsbereich dokumentieren.

Die *Hauptabteilungsleiter* **dürfen** Teile ihrer Aufgaben an *Datenschutz-Koordinatoren* und *Prozesseigentümer* delegieren. Die Verantwortung für die Einhaltung des Datenschutzes verbleibt jedoch bei den Hauptabteilungsleitern.

3.2.4.4 Beschäftigte | Employees

Beschäftigte **müssen** alle sie oder ihre Tätigkeit betreffenden Maßnahmen und Regelungen zum Datenschutz kennen, einhalten und umsetzen, an unternehmensseitig angebotenen Weiterbildungen zum Datenschutz teilnehmen sowie Datenschutz-Vorfälle melden.

Alle *Beschäftigten* **müssen** von den Geschäftsführungen im Rheinmetall Konzern verpflichtet werden, mit der *Data Privacy Organization* zusammenzuarbeiten.

Alle *Beschäftigten* **müssen** die *Data Privacy Organization* bei ihrer Arbeit unterstützen und mögliche Verbesserungen des Datenschutzes oder Schwachstellen an die *Data Privacy Organization* melden.

Alle *Beschäftigten* **dürfen** sich in allen datenschutzrechtlichen Belangen unmittelbar an den für sie zuständigen *Datenschutzbeauftragten* sowie an die *Data Privacy Organization* wenden.

3.2.4.5 Datenschutz-Koordinator

Der *Hauptabteilungsleiter* **darf** für seinen Verantwortungsbereich einen *Datenschutz-Koordinator* benennen. Dieser *Datenschutz-Koordinator* und dessen Aufgaben müssen dokumentiert werden.

Benennt der Hauptabteilungsleiter keinen Datenschutz-Koordinator, so muss der Hauptabteilungsleiter die Aufgaben des Datenschutz-Koordinators erfüllen.

Der *Datenschutz-Koordinator* **darf** sich in Fragen des Datenschutzes und Datenschutzmanagementsystems an die Data Privacy Organization wenden.

Der *Datenschutz-Koordinator* **muss** an den für ihn zuständigen *Data Privacy Manager* berichten. Der Bericht sollte mindestens einmal im Quartal erfolgen.

Wesentliche Aufgaben des Datenschutz-Koordinators sind:

- Übernahme der Koordination von datenschutzrechtlichen Aufgaben seinen Verantwortungsbereich betreffend.
- Koordinator von organisatorischen Maßnahmen seinen Verantwortungsbereich betreffend.
- Koordination der Dokumentation der Prozesseigentümer/Ansprechpartner.
- Terminierung von Abstimmungsterminen zwischen Prozesseigentümern/Ansprechpartner und Data Privacy Manager sowie Data Privacy Officer.
- Koordination der Umsetzung von Aufgaben aus der Data Privacy Organization und aus dem Datenschutzmanagementsystem.

3.2.4.6 Prozesseigentümer bzw. Eigentümer der Verarbeitung

Der *Hauptabteilungsleiter* **darf** für jeden Geschäftsprozess einen *Prozesseigentümer* benennen. Dieser *Prozesseigentümer* **muss** dokumentiert und an die *Data Privacy Organization* gemeldet werden.

Benennt der Hauptabteilungsleiter keinen Prozesseigentümer, so muss der Hauptabteilungsleiter die Aufgaben des Prozesseigentümers erfüllen.

Der *Prozesseigentümer* **muss** eine Überprüfung der Geschäftsprozesse durchführen, um festzustellen, ob im Zusammenhang mit dem Geschäftsprozess personenbezogene Daten oder besondere Kategorien von personenbezogenen Daten erhoben, verarbeitet, genutzt oder übermittelt werden.

Ist dies der Fall, so ist der Prozesseigentümer zugleich auch Eigentümer der Verarbeitung. Nachfolgend steht Prozesseigentümer zugleich für Eigentümer der Verarbeitung, sofern im Geschäftsprozess personenbezogene Daten erhoben, bearbeitet, genutzt oder übermittelt werden.

Der *Prozesseigentümer* **darf** sich in Fragen des Datenschutzes und Datenschutzmanagementsystems an den für ihn zuständigen *Datenschutz-Koordinator* und die *Data Privacy Organization* wenden.

Der *Prozesseigentümer* **muss** dem *Data Privacy Manager* Neueinführungen oder Änderungen von Verarbeitungen personenbezogener Daten rechtzeitig melden.

Der *Prozesseigentümer* **muss** an den für ihn zuständigen *Datenschutz-Koordinator* berichten. Der Bericht sollte anlassbezogen erfolgen.

Wesentliche Aufgaben des Prozesseigentümers sind:

- Beschreibung der Verarbeitungstätigkeiten („Verfahren“).
- Abschätzung und Dokumentation der Datenschutzrisiken, die mit dem Verfahren verbunden sind.
- Technische und Organisatorische Maßnahmen festlegen und dokumentieren.
- Datenschutzinformation der betroffenen Personen über seine Verfahren.
- Sicherstellen, dass bezogen auf seine Verfahren, Betroffenenrechte umgesetzt werden können.
- Unterstützen bei Datenschutzvorfällen seine Verfahren betreffend.

Der *Prozesseigentümer* **darf** Aufgaben (z. B. das Beschreiben von Verarbeitungstätigkeiten) an einen benannten Ansprechpartner delegieren. Die Benennung der Ansprechpartner ist je Verarbeitungstätigkeit zu dokumentieren.

3.2.4.7 Asset-Eigentümer

Der *Hauptabteilungsleiter* **darf** für jedes von ihm verantwortete Asset einen *Asset-Eigentümer* benennen. Dieser *Asset-Eigentümer* **muss** dokumentiert und an die *Data Privacy Organization* gemeldet werden.

Der Asset-Eigentümer ist für das die Verarbeitungstätigkeit unterstützende Asset zuständig. Ein Asset (analog sowie digital, siehe 1.3) kann hierbei mehrere Verarbeitungstätigkeiten unterstützen.

Neben dem *fachlichen* Asset-Eigentümer kann es auch einen *technischen* Asset-Eigentümer geben, falls das jeweilige Asset von einer anderen Fachabteilung bzw. Person technisch betreut bzw. verantwortet wird. Ist dies nicht der Fall, so ist der fachliche Asset-Eigentümer zugleich technischer Asset-Eigentümer.

Der für das Asset (fachlich bzw. technisch) verantwortliche Hauptabteilungsleiter kann einen (fachlichen bzw. technischen) Asset-Eigentümer bestimmen.

Sollte kein (fachlicher) *Asset-Eigentümer* benannt sein, so **muss** der *Hauptabteilungsleiter* der für das Asset zuständigen Abteilung die Aufgaben des *Asset-Eigentümers* übernehmen.

Wesentliche Aufgaben des Asset-Eigentümers sind:

- Umfassende Beschreibung der einzelnen Assets (insbesondere IT-Anwendungen).
- Tüchtig entsprechende Nachforschungen, sofern notwendige Informationen zur Beantwortung bestimmter Fragen zur datenschutzrechtlichen Erfassung des Assets erforderlich sind.
- Tritt (sofern erforderlich) mit dem Dienstleister/Anbieter, der Informations- und/oder IT-Sicherheit in Kontakt.
- Abschätzung und Dokumentation der Datenschutzrisiken, die mit dem Asset verbunden sind.
- Technische und Organisatorische Maßnahmen festlegen und dokumentieren.
- Unterstützt bei der datenschutzfreundlichen Technikgestaltung („Privacy by Design“) und Voreinstellung („Privacy by Default“) des Assets.
- Sicherstellen, dass bezogen auf seine Assets die Betroffenenrechte umgesetzt werden können.
- Unterstützung bei Datenschutzvorfällen seine Assets betreffend.

Der *Asset-Eigentümer* **darf** Aufgaben (z. B. das Beschreiben des Assets) an einen benannten Ansprechpartner delegieren. Die Benennung der Ansprechpartner ist je Asset zu dokumentieren.

3.2.4.8 Datenschutzbeauftragter

Eine wesentliche gesetzliche Aufgabe der Geschäftsführung, die nicht delegiert werden kann, ist die Benennung eines Datenschutzbeauftragten. Sind die gesetzlichen Anforderungen zur Benennungspflicht eines Datenschutzbeauftragten erfüllt, so muss ein Datenschutzbeauftragter benannt werden.

Wenn die gesetzlichen Voraussetzungen erfüllt sind, **müssen** die jeweiligen *Geschäftsführungen* im Rheinmetall Konzern in Abstimmung mit dem *Corporate Data Privacy Officer* einen *Datenschutzbeauftragten* für die betroffenen Unternehmen benennen, der den gesetzlichen Anforderungen genügt.

Die Benennung eines Datenschutzbeauftragten unterliegt den Anforderungen aus der DSGVO und in Deutschland zusätzlich dem BDSG. Der Datenschutzbeauftragte hat gesetzlich definierte Aufgaben zu übernehmen und gesetzlich definierte Anforderungen zu erfüllen. Ein Datenschutzbeauftragter kann auch freiwillig benannt werden, sofern keine gesetzliche Benennungspflicht vorliegt.

Die *Datenschutzbeauftragten* **müssen** an die Geschäftsführungen der Unternehmen berichten, für die sie benannt sind. Zusätzlich **müssen** die *Datenschutzbeauftragten* unter Berücksichtigung ihrer gesetzlichen Unabhängigkeit an den *Corporate Data Privacy Officer* und den für sie zuständigen *Data Privacy Officer* berichten.

Im Rheinmetall Konzern wird angestrebt, einen Konzerndatenschutzbeauftragten zu etablieren.

Der Begriff des „Konzerndatenschutzbeauftragten“ existiert in dieser Form nicht in der DSGVO und ist vielmehr eine Paraphrasierung des „gemeinsamen Datenschutzbeauftragten“ aus der DSGVO²⁰. Danach heißt es, dass eine Unternehmensgruppe einen gemeinsamen Datenschutzbeauftragten ernennen darf, sofern dieser von jeder Niederlassung aus leicht erreicht werden kann. Eine Unternehmensgruppe ist laut DSGVO eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht²¹.

Die Aufgaben des Datenschutzbeauftragten sind gesetzlich geregelt und beziehen sich im Wesentlichen auf das Beraten und das Überwachen aller datenschutzrechtlicher Sachverhalte. Der Datenschutzbeauftragte kann somit

²⁰ Vgl Art. 37 Abs. 2 DSGVO.

²¹ Vgl Art. 4 Nr. 19 DSGVO und § 18 AktG.

nicht zuständig und verantwortlich für die operative Umsetzung des Datenschutzes sein. Für die operative Umsetzung des Datenschutzes ist vielmehr der Verantwortliche zuständig. Jeder Beschäftigte im Rheinmetall Konzern ist für die operative Umsetzung des Datenschutzes in seinem Zuständigkeitsbereich verantwortlich und wird in diesem Unterfangen durch die in diesem Handbuch dargestellte Data Privacy Organization unterstützt.

3.2.4.8.1 Benennung und Stellung eines Datenschutzbeauftragten (Deutschland und EU)

3.2.4.8.1.1. Einleitung

Es ist sicherzustellen, dass - soweit die Voraussetzungen vorliegen - ein Datenschutzbeauftragter benannt und mit einer den gesetzlichen Anforderungen entsprechenden Stellung versehen ist.²²

3.2.4.8.1.2. Pflicht zur Benennung

Der Verantwortliche prüft, ob ein Datenschutzbeauftragter zu benennen ist. Dies ist in Deutschland der Fall, wenn im jeweiligen Unternehmen in der Regel mindestens zwanzig Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt sind.²³ Eine Pflicht zur Benennung kann sich in Deutschland und der EU/EWR aber auch in anderen Konstellationen ergeben, z. B. wenn die Kerntätigkeit des Verantwortlichen in der umfangreichen Verarbeitung besonderer Kategorien von personenbezogener Daten besteht.²⁴

Der Datenschutzbeauftragte muss Fachwissen auf dem Gebiet des Datenschutzrechts und der Datenschutzpraxis besitzen und zur Erfüllung seiner gesetzlichen Aufgabe fähig sein.²⁵ Die Kontaktdaten des Datenschutzbeauftragten sind zu veröffentlichen und der Aufsichtsbehörde mitzuteilen.

Die Benennung zum Datenschutzbeauftragten eines Rheinmetall Unternehmens oder des Rheinmetall Konzerns soll in der Regel auf drei Jahre befristet sein. Hierbei sind einschlägige arbeits-, datenschutzrechtliche sowie vertragliche Bestimmungen zu berücksichtigen (ggf. unter Einbindung der Personalabteilung und des Rechtsbereichs).

3.2.4.8.1.3. Stellung des Datenschutzbeauftragten im Unternehmen

Die Weisungsfreiheit des Datenschutzbeauftragten ist zu gewährleisten. Es ist sicherzustellen, dass der Datenschutzbeauftragte ordnungsgemäß und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängende Fragen eingebunden wird. Er ist bei der Erfüllung seiner Aufgaben zu unterstützen, indem er die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung gestellt bekommt. Der Datenschutzbeauftragte darf von dem Verantwortlichen oder dem Auftragsverarbeiter wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden.

Betroffene Personen können den Datenschutzbeauftragten bei Fragen zur Verarbeitung ihrer personenbezogenen Daten und der Wahrnehmung ihrer Rechte im Zusammenhang mit der DSGVO zu Rate ziehen. Beschwerden zum Thema Datenschutz werden dem Datenschutzbeauftragten zur Kenntnis vorgelegt. Die Bearbeitung erfolgt durch die durchführenden Stellen in Abstimmung mit dem Datenschutzbeauftragten. Wird eine Beschwerde direkt an den Datenschutzbeauftragten gerichtet, erfolgt die Beantwortung in der Regel durch den Datenschutzbeauftragten. Sollte eine Beantwortung durch die durchführende Stelle erforderlich sein, wird dies im Einzelfall abgestimmt. Die durchführenden Stellen liefern die für die Beantwortung notwendigen und aufbereiteten Informationen.

Mit der Zuweisung der Aufgaben aus der DSGVO ist der Datenschutzbeauftragte mit einer umfassenden Überwachungsaufgabe betraut.

Darüber hinaus kann er auch andere Aufgaben und Pflichten wahrnehmen.²⁶ Bei der Übertragung weiterer Aufgaben an den Datenschutzbeauftragten ist ein Interessenkonflikt zu vermeiden. Ein Interessenkonflikt ist eine Situation, in der das Risiko besteht, dass sekundäre Interessen persönlicher, betrieblicher oder institutioneller

²² Die Anforderungen sind in Art. 37, 38 DSGVO und § 38 BDSG normiert.

²³ § 38 Abs. 1 S. 1 BDSG.

²⁴ Vgl. § 38 Abs. 1 S. 2 BDSG, Art. 37 Abs. 1 lit. b und c DSGVO.

²⁵ Vgl. Art. 37 Abs. 5 DSGVO.

²⁶ Vgl. Art. 38 Abs. 6 DSGVO.

Art die primären Interessen gefährden. In solchen Fällen liegt eine Unvereinbarkeit der kollidierenden Interessen vor. Die Abwesenheit eines Interessenkonflikts ist eng mit dem Erfordernis einer unabhängigen Tätigkeit verknüpft. Ein Interessenkonflikt ist u. a. regelmäßig dann anzunehmen, wenn dem Datenschutzbeauftragten operative Aufgaben zugewiesen werden, bei denen ihm das Gesetz Überwachungsaufgaben und -rechte zuweist.

Somit kann der Datenschutzbeauftragte innerhalb einer Gesellschaft keine Position innehaben, welche es mit sich bringt, die Zwecke und Mittel der Verarbeitung personenbezogener Daten festzulegen. Aufgrund der in jeder Gesellschaft vorhandenen, eigenen organisatorischen Unterschiede ist diese Frage fallweise zu betrachten.

3.2.4.8.1.4. Dokumentation

Es existieren keine Formvorgaben für die Benennung, diese sollte jedoch schriftlich erfolgen. Sie sollte den Bezug auf die damit verbundenen gesetzlichen Aufgaben und die damit verbundene Stellung im Unternehmen umfassen sowie ggfs. weitere damit verbundene zugewiesene Aufgaben. Das Dokument ist als Kopie zur Personalakte zu hinterlegen. Auch sind die Veröffentlichung der Kontaktdaten (etwa per Screenshot der entsprechenden Passage der Homepage) und die Mitteilung an die Aufsichtsbehörde zu dokumentieren.

Ist ausnahmsweise kein Datenschutzbeauftragter zu benennen, ist diese Erwägung zu dokumentieren.

Ein Datenschutzbeauftragter kann im Übrigen auch freiwillig benannt werden.

3.2.4.8.1.5. Rollen und Verantwortung

Rolle	Verantwortung
Verantwortlicher gesetzlicher Vertreter der Legal-Einheit = Geschäftsführung	<ul style="list-style-type: none"> ▪ Ist verantwortlich für die Benennung eines Datenschutzbeauftragten (dieser kann Beschäftigter sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen). ▪ Benennt nach Freigabe durch den Corporate Data Privacy Officer den Datenschutzbeauftragten. ▪ Dokumentiert die damit verbundenen gesetzlichen Aufgaben und die damit verbundene Stellung im Unternehmen sowie ggfs. weitere damit verbundene zugewiesene Aufgaben des Datenschutzbeauftragten. ▪ Prüft regelmäßig, ob nicht in der Zwischenzeit, beispielsweise durch Neueinstellungen von Beschäftigten, eine Pflicht zur Benennung eines Datenschutzbeauftragten besteht. ▪ Informiert die Data Privacy Organization bei Neugründung, Zukauf und Verkauf von Unternehmen.
Corporate Data Privacy Officer	<ul style="list-style-type: none"> ▪ Prüft und gibt die Benennung des Datenschutzbeauftragten frei. ▪ Kann sich im Rahmen des Freigabeprozesses an den Chief Compliance Officer wenden.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Kontrolliert alle zwei Jahre die Pflicht zur Benennung eines Datenschutzbeauftragten. ▪ Prüft bei Neugründung, Zukauf und Verkauf von Unternehmen, ob ein Datenschutzbeauftragter zu benennen ist.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berichtet unmittelbar der höchsten Managementebene des Verantwortlichen oder des Auftragsverarbeiters.²⁷ ▪ Erfüllt seine gesetzlichen Aufgaben

²⁷ Vgl. Art. 38 Abs. 3 Satz 3 DSGVO.

3.2.4.8.2 Aufgaben des Datenschutzbeauftragten

3.2.4.8.2.1. Einleitung

Der benannte *Datenschutzbeauftragte* **muss** die ihm gesetzlich zugewiesenen Aufgaben wahrnehmen.

3.2.4.8.2.2. Dokumentation

Die Aufgaben des Datenschutzbeauftragten sind zu dokumentieren. Die Anfragen bzw. Beschwerden von betroffenen Personen unterliegen zumindest in Deutschland der Schweigepflicht. Zudem ist der Geschäftsführung und dem zuständigen Data Privacy Officer regelmäßig (mindestens jährlich) ein Tätigkeitsbericht über die Erfüllung seiner Aufgaben vorzulegen.

3.2.4.8.2.3. Beschreibung

Dem Datenschutzbeauftragten sind zumindest die nachfolgenden Aufgaben bereits per Gesetz zugewiesen:

Aufgabe	Beschreibung
Unterrichtung und Beratung	Der Datenschutzbeauftragte hat die Aufgabe, den Verantwortlichen bzw. die Auftragsverarbeiter und ihre jeweiligen Beschäftigten, die die Verarbeitungen durchführen, hinsichtlich ihrer datenschutzrechtlichen Pflichten zu unterrichten und zu beraten. ²⁸
Überwachung	Der Datenschutzbeauftragte hat die Aufgabe, die Einhaltung der datenschutzrechtlichen Vorschriften und der internen Datenschutzrichtlinien durch den Verantwortlichen bzw. den Auftragsverarbeiter zu überwachen, was auch die Zuweisung von Zuständigkeiten mit einschließt. ²⁹ Hierfür sind eigene Prüf- und Kontrollmaßnahmen des Datenschutzbeauftragten zusätzlich zu anlassbezogenen Prüfungen und Kontrollen zu planen und durchzuführen. Der Datenschutzbeauftragte legt daraus resultierende Erkenntnisse und Maßnahmenempfehlungen der Geschäftsführung vor.
Mitwirkung an der Datenschutz-Folgeabschätzung (DSFA)	Der Datenschutzbeauftragte berät den Verantwortlichen – auf Anfrage – im Zusammenhang mit der Durchführung einer DSFA. ³⁰ Diese Aufgabe korrespondiert mit der Verpflichtung des Verantwortlichen, bei der Durchführung einer DSFA den Rat des Datenschutzbeauftragten einzuholen. ³¹ Darüber hinaus hat er zudem die Aufgabe, die Durchführung der DSFA zu überwachen. ³²
Zusammenarbeit mit der Aufsichtsbehörde	Es obliegt dem Datenschutzbeauftragten auch, mit der Aufsichtsbehörde zusammenzuarbeiten und ihr als Anlaufstelle zu dienen. ³³ Hiervon ist explizit auch das Verfahren der vorherigen Konsultation erfasst.

3.2.4.8.2.4. Rollen und Verantwortung

Rolle	Verantwortung
Verantwortlicher gesetzlicher Vertreter der Legal-Einheit = Geschäftsführung	<ul style="list-style-type: none"> ▪ Stattet den Datenschutzbeauftragten geeignet aus und verankert seine gesetzliche Stellung innerbetrieblich.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Ist in der Durchführung der ihm obliegenden gesetzlichen Aufgaben eigenverantwortlich und weisungsfrei. ▪ Dokumentiert die Bearbeitung seiner Aufgaben. ▪ Legt der Geschäftsführung und dem zuständigen Data Privacy Officer regelmäßig (mindestens jährlich) einen Tätigkeitsbericht über die Erfüllung seiner Aufgaben vor.

²⁸ Vgl. Art. 39 Abs. 1 lit. a DSGVO.

²⁹ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

³⁰ Vgl. Art. 39 Abs. 1 lit. c DSGVO.

³¹ Vgl. Art. 35 Abs. 2 DSGVO.

³² Vgl. Art. 39 Abs. 1 lit. c DSGVO.

³³ Vgl. Art. 39 Abs. 1 lit. d, e DSGVO.

Rolle	Verantwortung
	<ul style="list-style-type: none"> ▪ Berät und prüft die Reichweite, inhaltliche Tiefe und Wirkung der erfolgten Beratungen und Unterrichtungen, bei Bedarf auch durch Befragung der Beschäftigten. ▪ Prüft die Anzahl und inhaltliche Abdeckung der Kontroll- und Prüfmaßnahmen in Bezug auf die fachliche Komplexität des Verantwortlichen und der dazu gegebenen datenschutzrelevanten Risiken sowie die Umsetzung der daraus empfohlenen Maßnahmen. ▪ Prüft die in Anspruch genommene Beratungsleistungen zur DSFA in Bezug auf die gemäß dem Verzeichnis der Verarbeitungen als erforderlich dokumentierten Datenschutzfolgeabschätzungen und berät bei der Durchführung der Datenschutzfolgenabschätzung. ▪ Prüft die Anzahl der stattgefundenen Konsultationen mit den Aufsichtsbehörden. ▪ Ist in seiner Funktion Ansprechpartner der Datenschutzaufsichtsbehörden und muss mit diesen zusammenarbeiten.

3.2.4.8.3 Delegation von datenschutzrelevanten Prozessen an den Datenschutzbeauftragten³⁴

Der Datenschutzbeauftragte kann neben seinen gesetzlich vorgegebenen Aufgaben³⁵ auch ausdrücklich zugewiesene andere Aufgaben und Pflichten im Datenschutz wahrnehmen³⁶. Der Datenschutzbeauftragte sollte jedoch keine aktive Rolle in der Datenschutz-Organisation übernehmen. Er hat daher für das Datenschutzmanagementsystem des Rheinmetall Konzerns eine eingeschränkte Bedeutung und sollte keine operativen, sondern im wesentlichen Überwachungsaufgaben übernehmen. Die zuständige Unternehmensleitung muss sicherstellen, dass „*derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen*“.³⁷

Ein Interessenkonflikt besteht insbesondere, wenn der Datenschutzbeauftragte in erster Linie die Ergebnisse seiner eigenen Arbeit kontrollieren müsste.³⁸

Mithin darf der betriebliche Datenschutzbeauftragte weder im gesamten Unternehmen noch in bestimmten Bereichen noch bei einzelnen Projekten dafür verantwortlich sein, dass die datenschutzrechtlichen Vorgaben eingehalten werden. Denn in einer solchen Konstellation ist eine objektive Kontrolle seiner eigenen Entscheidungen nicht mehr gewährleistet, seine formal geforderte Zuverlässigkeit steht damit in Frage. Diese Vorgabe bringt insbesondere mit sich, dass der Datenschutzbeauftragte innerhalb eines Unternehmens grundsätzlich keine Position innehaben kann, welche beinhaltet, dass er die Zwecke und Mittel der Verarbeitung personenbezogener Daten festlegt.³⁹

Vor diesem Hintergrund erfüllt Rheinmetall mit der Benennung eines Datenschutzbeauftragten eine gesetzliche Verpflichtung.

3.3 Steuerung des Datenschutzes im Rheinmetall Konzern

Wesentlicher Anknüpfungspunkt zur aktiven Steuerung des Datenschutzes und der damit verbundenen Datenschutzrisiken und Datenschutz Compliance Risiken ist das Verzeichnis der Verarbeitungstätigkeiten, das Verzeichnis der die Verarbeitungstätigkeiten unterstützenden Assets sowie der mit den Assets und Verarbeitungstätigkeiten verknüpften „Datenverarbeitungsdienstleister“.

Zentrale Aufgabe der Unternehmen und der Data Privacy Organization ist es somit, sich einen umfassenden Überblick zu den Verarbeitungstätigkeiten, Assets und Dienstleistern zu verschaffen, um nachhaltig und nachvollziehbar Datenschutzrisiken und Datenschutz Compliance Risiken bewerten und Empfehlungen zum Management dieser Risiken geben zu können.

³⁴ Die Benennung eines Datenschutzbeauftragten unterliegt den Anforderungen aus der DSGVO und in Deutschland zusätzlich dem BDSG. Eine Benennungspflicht eines Datenschutzbeauftragten oder einer vergleichbaren Rolle ist durch die Verantwortlichen in den jeweiligen Ländern anhand der nationalen Regelungen zu prüfen.

³⁵ Vgl. Art. 39 Abs. 1 DSGVO.

³⁶ Vgl. Art. 38 Abs. 6 Satz 1 DSGVO.

³⁷ Vgl. Art. 38 Abs. 6 Satz 2 DSGVO.

³⁸ Vgl. etwa Bundesarbeitsgericht, Beschluss vom 22. März 1994, Aktenzeichen: 1 ABR 51/93.

³⁹ Art. 29 Arbeitsgruppe, WP 253, Ziffer 3.5).

Zu diesem Zweck bedient sich der Rheinmetall Konzern eines zentralen Prozesses zur Erfassung und Dokumentation von Verarbeitungstätigkeiten, Assets und datenschutzrelevanten Dienstleistern (vgl. Ziffer 5).

Tools (u. a. Software), Checklisten und Fragebögen zur zentralen Erfassung werden durch die Data Privacy Organization zur Verfügung gestellt. Die Verantwortung zur vollständigen Erfassung liegt jedoch bei demjenigen, der die Datenverarbeitung veranlasst und somit bei dem Hauptabteilungsleiter der für den zugrundeliegenden Geschäftsprozess verantwortlich ist.

Ziel ist es u. a., den Prozess- und Asset-Eigentümern Anleitung zur Gestaltung datenschutzkonformer Prozesse und Assets zu geben, um die zugehörigen Datenschutz- und Datenschutz Compliance Risiken verwalten und steuern zu können. Zudem soll eine Verwaltung und Steuerung wesentlicher Risiken auf Unternehmens-, Divisions- und Konzernebene ermöglicht werden.

3.4 Regelmäßige Überprüfung und Fortschreibung des DSMS

Erforderlich ist eine regelmäßige Überprüfung und Fortschreibung des Datenschutzkonzeptes an die weitere betriebliche und rechtliche Entwicklung im Rahmen eines Plan-Do-Check-Act-Zyklus (PDCA-Zyklus).⁴⁰

Dabei existieren verschiedene Auslöser für einen solchen Zyklus:

- der Ablauf eines Zeitraums (z. B. wird eine jährliche Prüfung auf den Bedarf zur Aktualisierung des DSMS empfohlen);
- Änderungen von rechtlichen (z. B. Gesetze, Verordnungen) oder innerbetrieblichen (z. B. Code of Conduct, Betriebsvereinbarungen) Regelungen;
- Änderungen in der jeweiligen Gesellschaft (z.B. Auslagerungen);
- Sicherheitsmaßnahmen entsprechen nicht mehr dem Stand der Technik bzw. es ist bekannt, dass die Maßnahmen nicht mehr die erforderliche Sicherheit bieten (z.B. Einführung neuer IT-Systemplattformen);
- Änderungen in den konkreten Verarbeitungen (z.B. Verlagerung der Datenverarbeitung);
- bei Aufkommen relevanter Vorkommnisse (z.B. Datenschutzverstöße).

Grundsätzlich ist Datenschutz eine Aufgabe des gesamten Unternehmens. Die Kontrolle des Datenschutzes in der Phase C (Check) ist durch das Unternehmen intern sicherzustellen (z. B. Internes Kontrollsystem (IKS), Data Privacy Organization). (Externe) Überwachung erfolgt durch die Aufsichtsbehörden oder (bei Zertifizierung/Verhaltensregeln) durch Auditoren - und auch durch die betroffenen Personen. Der Datenschutzbeauftragte muss die Organisation unterstützen bzw. beraten (Anknüpfungspunkt ist insbesondere die Phase P (Plan)) sowie überwachen, insbesondere im Hinblick auf die Funktionalität des internen Kontrollsystems. Im Bereich der Überwachung stellt der Datenschutzbeauftragte zugleich auch eine eigenständige, ergänzende Überwachung zur Aufsichtsbehörde dar. Insbesondere die Überwachung durch den Datenschutzbeauftragten erfolgt risikoorientiert. Keine Garantenstellung des Datenschutzbeauftragten besteht durch Beratung insbesondere im Rahmen der Phase P (Plan) und die Überwachung v. a. in Anknüpfung an die Phase C (Check). Die (Umsetzungs-)Verantwortung im Rahmen des vollständigen PDCA-Zyklus liegt bei der verantwortlichen Stelle.



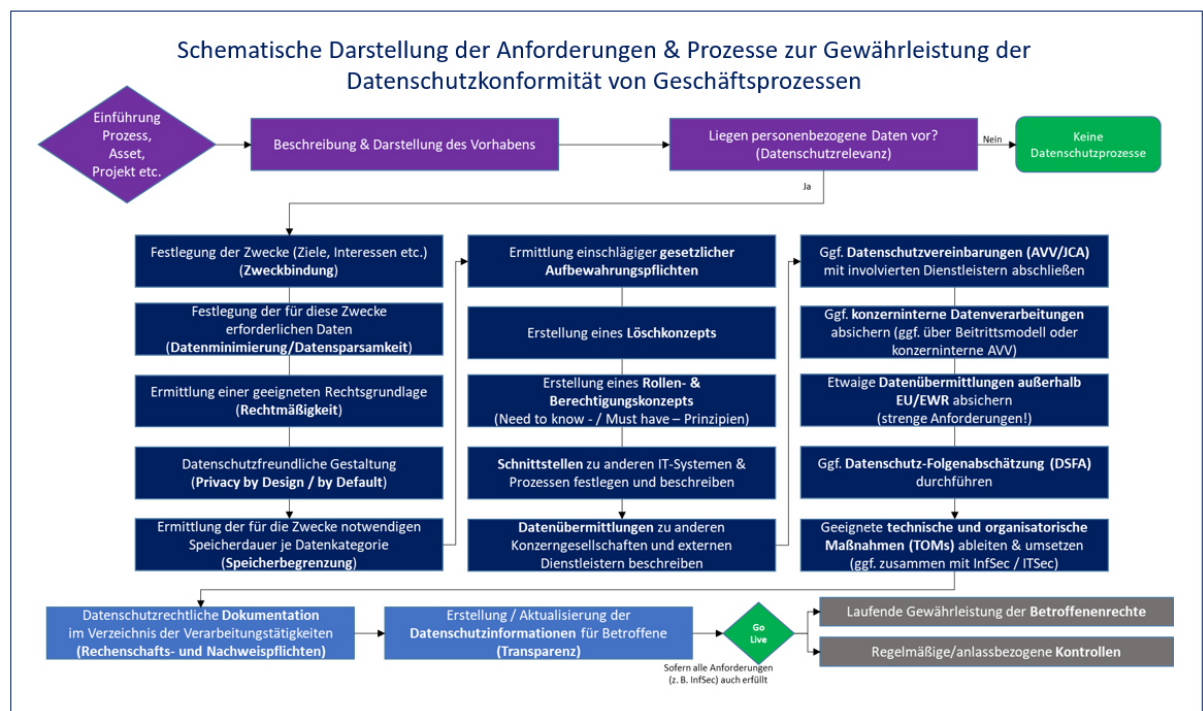
⁴⁰ Vgl. Art. 24 DSGVO.

4 Gestaltung datenschutzkonformer Prozesse

4.1 Einleitung

Die datenschutzkonforme Gestaltung und Durchführung von Datenverarbeitungen ist die wesentliche und zentrale Aufgabe, um dem Datenschutz in den Unternehmen des Rheinmetall Konzerns Geltung zu verschaffen und die Einhaltung datenschutzrechtlicher Vorgaben zu gewährleisten. Der Verantwortliche hat im Rahmen dessen sicherzustellen, dass für jeden Prozess (Geschäftsprozess) ein Prozesseigentümer bestimmt wird.

Da die Datenverarbeitung primär in den Geschäftsprozessen (häufig auch nur als „Beiwerk“) stattfindet, liegt die Verpflichtung und Aufgabe zur datenschutzkonformen Gestaltung der Verarbeitung personenbezogener Daten beim Leiter des Geschäftsbereiches bzw. der Abteilung (i.d.R. der Hauptabteilungsleiter). Der Hauptabteilungsleiter muss somit in seinem Verantwortungsbereich die Einhaltung der datenschutzrechtlichen Anforderungen sicherstellen.



4.2 Besonderheiten im Konzern

Besonderes Augenmerk ist auf die Gestaltung und Dokumentation von Geschäftsprozessen zu legen, welche unternehmensübergreifend bei Rheinmetall stattfinden. Hierzu zählen insbesondere sogenannte Shared Services. Konzerngesellschaften sind im Kontext des Datenschutzes nicht anders zu behandeln als andere (konzernexterne) Unternehmen. Jedes Konzernunternehmen wird als eigenständiger Verantwortlicher verstanden und behandelt. Das bedeutet insbesondere, dass es bei der Gestaltung unternehmensübergreifender Geschäftsprozesse für jede Datenübermittlung einer eigenen Rechtsgrundlage bedarf und/oder zwischen den beteiligten Konzernunternehmen geeignete Datenschutzvereinbarungen abzuschließen sind.

Übergreifende Verarbeitungen und Verfahren sind immer so zu gestalten, dass eine Mandantentrennung (Trennung der Daten nach den beteiligten Verantwortlichen) möglich ist und dass Zugriffsrechte auf diese Daten getrennt nach Verantwortlichen vergeben werden können. Für eine „Vermischung“ von personenbezogenen Daten benötigt jeder beteiligte Verantwortliche wiederum eine eigene Rechtsgrundlage. Die Verantwortung für die datenschutzkonforme Gestaltung solcher Geschäftsprozesse liegt bei dem für den Geschäftsprozess zuständigen Hauptabteilungsleiter. Bei gesellschaftsübergreifenden Prozessen oder Assets, insbesondere bei sogenannten Shared Services, muss es in jeder „nutzenden“ Legal-Einheit zumindest einen Prozesseigentümer sowie einen Prozesseigentümer auf Konzernebene geben, der die Anforderungen an den Geschäftsprozess koordiniert und angemessen umsetzt. Im Falle von Assets genügt ein Asset-Eigentümer, der jedoch dann die Anforderungen der Prozesseigentümer ebenfalls konsolidieren und angemessen berücksichtigen muss.

Die Prozess- und Asset-Eigentümer (auf Konzernebene sowie in jeder Legal-Einheit) **müssen** bei konzernweiten eingesetzten Prozessen und Assets eine Trennung der personenbezogenen Daten nach Verantwortlichen vornehmen können (sogenannte Mandantentrennung).

Die Besonderheiten in einer sogenannten Matrix-Organisation werden bezogen auf Beschäftigte und Datenschutz durch die Personalabteilung in einer eigenen HR-Richtlinie zur Matrix-Organisation geregelt.

Typische unternehmensübergreifende „Shared Services“ finden sich insbesondere in der Personalabteilung (z. B. Personalstammdatenbank), Recruiting (zentrales Recruiting Center), Payroll (z. B. Gehaltsabrechnung) und IT (zentrale IT-Dienstleistungen und –Anwendungen).

4.3 Auslöser des Prozesses „datenschutzkonforme Verarbeitung“

4.3.1 Vorliegen personenbezogener Daten

4.3.1.1 Einleitung

Es ist sicherzustellen, dass beim Vorliegen und bei der Verarbeitung von personenbezogenen Daten die Anforderungen des Datenschutzes in Bezug auf den Umgang mit Daten beachtet werden. Hierzu ist es erforderlich, zu identifizieren und zu dokumentieren, ob und welche personenbezogenen Daten in einem Geschäftsprozess vorliegen.

4.3.1.2 Beschreibung

Diese Vorgaben sind stets einzuhalten, wenn ein Verantwortlicher mit Daten umgeht. In diesem Fall muss geprüft werden, ob es sich bei diesen Daten um personenbezogene Daten handelt. Sollte festgestellt werden, dass im Zusammenhang mit dem Geschäftsprozess personenbezogene Daten erhoben, verarbeitet, genutzt oder übermittelt werden, ist dieser Geschäftsprozess zugleich eine Verarbeitungstätigkeit. Anschließend ist zu ermitteln bzw. festzustellen, welche Datenkategorien und Datenelemente im Geschäftsprozess verarbeitet werden. Hierzu gibt die Data Privacy Organization geeignete Datenkategorien sowie Datenelemente vor. Die Zuordnung dieser Kategorien zur Verarbeitungstätigkeit und Asset erfolgt durch den Prozesseigentümer.

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen („betroffene Person“). Als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.⁴¹

Klassische Beispiele für personenbezogene Daten sind der Name, die Adresse oder das Geburtsdatum einer Person. Weitere Beispiele sind Daten, die in Systemen/Anwendungen einer betroffenen Person zugeordnet werden, z. B. Informationen zur Krankenversicherung oder die Steueridentifikationsnummer. Auch dynamische IP-Adressen können nach einem Urteil des Europäischen Gerichtshofs grundsätzlich personenbezogene Daten sein, wenn der Verantwortliche über rechtliche Mittel verfügt, die es ihm erlauben, den betreffenden Nutzer anhand von Zusatzinformationen, über die der Internetzugangsanbieter verfügt, bestimmen zu lassen.

⁴¹ Vgl. Art. 4 Nr. 1 DSGVO.

Beispiele für personenbezogene Daten <i>Personenbezug auch bei „sachlichen/technischen“ Daten möglich</i>		
Allg. Personendaten Name, Alter, Familienstand, Geburtsdatum...	Finanzdaten Bankdaten, Kreditkarteninfos, Einkommen, Kontostand...	Genetische/ Biometrische Daten Fingerabdruck, DNA...
Physische Merkmale Geschlecht, Größe, Gewicht, Augenfarbe, Statur....	Kontaktdaten Private/Dienstliche Anschrift, Telefonnr., E-Mail...	Werturteile Zeugnisse, Arbeitsbeurteilungen...
Kennnummern Personalausweisnr., Sozialversicherungsnr., Personlnr. ...	Gesundheitsdaten Diagnosen, Krankheitstage, Gesundheitsprognosen ...	Online-Daten / IT-Daten IP-Adresse, Surf- und Suchhistorie, Logfiles...
Präferenzen Vorlieben für bestimmte Produkte, Interessen...	Standortdaten GPS-Koordinaten, Aufenthaltsorte, Tracking ...	u. v. m.

4.3.1.3 Dokumentation

Die Verarbeitung von personenbezogenen Daten ist in einer Verarbeitungsbeschreibung zu dokumentieren. Unterstützende Assets sind in einer Asset-Beschreibung zu dokumentieren. Näheres hierzu in Ziffer 5.

4.3.1.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer bzw. Auftraggeber eines Projekts bei einer neuen Verarbeitung	<ul style="list-style-type: none"> ▪ Prüft gemeinsam mit dem Datenschutz-Koordinator, ob und inwieweit personenbezogene Daten im Rahmen von Verarbeitungen im normalen Geschäftsbetrieb oder im zu gestaltenden Prozess oder im Asset vorliegen bzw. vorkommen. ▪ Prüft regelmäßig mit dem Datenschutz-Koordinator, ob ausreichende organisatorische Maßnahmen zur Überprüfung der Personenbeziehbarkeit von Daten bestehen und dokumentiert dies. ▪ Sofern zutreffend: Prüft regelmäßig mit dem Datenschutz-Koordinator, ob die Verarbeitungen auf einer geeigneten Rechtsgrundlage beruhen. ▪ Bindet bei Verarbeitungen im normalen Geschäftsbetrieb und bei neuen Verarbeitungstätigkeiten bzw. der Planung neuer IT-Tools die Data Privacy Organization ein.
Einkauf bzw. IT-Abteilung (IT-Contract / Vendor Management, IT-License Management, IT-Demand Management)	<ul style="list-style-type: none"> ▪ Prüft bei einem geplanten Geschäftsprozess oder bei einer Bestellung von (IT-) Leistungen/Dienstleistungen, ob personenbezogene Daten vorkommen. ▪ Sofern zutreffend: Meldet dies der Data Privacy Organization und weist den Fachbereich auf die Einbindung der Data Privacy Organization hin. ▪ Verankert die Überprüfung auf das Vorliegen personenbezogener Daten in den Einkaufsprozessen.
Projektmanagement	<ul style="list-style-type: none"> ▪ Verankert die Überprüfung auf das Vorliegen personenbezogener Daten im Projektmanagement-Handbuch.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Prüft anhand von bereitgestellten Hilfsmitteln, ob und welche Kategorien personenbezogener Daten im Rahmen des zu gestaltenden Prozesses oder des Assets vorliegen bzw. vorkommen. ▪ Prüft regelmäßig, ob die Verarbeitungen von personenbezogenen Daten auf einer geeigneten Rechtsgrundlage beruhen.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Berät zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Erkundigt sich in regelmäßigen Abständen (anlasslos, einmal jährlich) bei dem Datenschutz-Koordinator bzw. dem Prozesseigentümer, ob neue Verarbeitungstätigkeiten vorliegen. ▪ Ist unterstützend und beratend tätig. ▪ Stellt geeignete Hilfsmittel zur Überprüfung und Dokumentation zur Verfügung.

Rolle	Verantwortung
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist hierzu überwachend und beratend tätig.⁴²

4.3.2 Besondere Datenkategorien und Daten über strafrechtliche Verurteilungen

4.3.2.1 Einleitung

Es ist sicherzustellen, dass beim Vorliegen von besonderen Kategorien personenbezogener Daten⁴³ oder Daten über strafrechtliche Verurteilungen und Straftaten⁴⁴ die zusätzlichen Beschränkungen des Datenschutzes in Bezug auf den Umgang mit diesen Daten und die deutlich erhöhten Sicherheitsanforderungen beachtet werden.

4.3.2.2 Besondere Kategorien personenbezogener Daten

Es muss geprüft werden, ob es sich bei den Daten um besondere Kategorien personenbezogener Daten handelt.

Besondere Kategorien personenbezogener Daten sind in der EU/EWR Angaben zu rassistischer und ethnischer Herkunft, politischen Meinungen, religiösen oder weltanschaulichen Überzeugungen, Gewerkschaftszugehörigkeiten, genetischen oder biometrischen Daten, Gesundheitsdaten sowie Daten zum Sexualleben oder der sexuellen Orientierung.⁴⁵

Sowohl besondere Kategorien personenbezogener Daten als auch Daten zu strafrechtlichen Verurteilungen stehen in der EU/EWR unter einem besonderen gesetzlichen Schutz und **müssen** betrachtet und deren Verarbeitung entsprechend dokumentiert werden.

Auch andere Rechtsordnungen definieren besonders schützenswerte personenbezogene Daten. Diese sind durch die jeweiligen Unternehmen im Rheinmetall Konzern zu identifizieren und entsprechend diesem Handbuch gesondert festzuhalten sowie der Data Privacy Organization zur Verfügung zu stellen.

Der *Regional Data Privacy Manager* **muss** ermitteln, welche Arten personenbezogener Daten nach seiner Rechtsordnung sensibel sind und diese in einer Liste an den für ihn zuständigen *Data Privacy Officer* melden.

Während die Verarbeitung einfacher personenbezogener Daten häufig auf die gängigen gesetzlichen Erlaubnistatbestände gestützt werden kann⁴⁶, genügen diese nicht, wenn es um die Verarbeitung besonderer Kategorien personenbezogener Daten geht. Ist eine Verarbeitung von besonderen Kategorien personenbezogener Daten beabsichtigt, muss diese Verarbeitung auf einer gesonderten Rechtsgrundlage oder einer ausdrücklichen Einwilligung beruhen.⁴⁷ Eine solche Verarbeitung kann in den folgenden Kontexten möglich sein:

- die betroffene Person hat in die Verarbeitung der genannten personenbezogenen Daten für einen oder mehrere festgelegte Zwecke ausdrücklich eingewilligt;⁴⁸
- die Verarbeitung ist erforderlich, damit der Verantwortliche oder die betroffene Person die ihm bzw. ihr aus dem Arbeitsrecht und dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte ausüben und seinen bzw. ihren diesbezüglichen Pflichten nachkommen kann;⁴⁹
- die Verarbeitung ist zum Schutz lebenswichtiger Interessen der betroffenen Person oder einer anderen natürlichen Person erforderlich und die betroffene Person ist aus körperlichen oder rechtlichen Gründen außerstande, ihre Einwilligung zu geben;⁵⁰

⁴² Vgl. Art. 39 Abs. 1 lit b DSGVO.

⁴³ Art. 9 Abs. 1 DSGVO.

⁴⁴ Art. 10 DSGVO.

⁴⁵ Vgl. Art. 9 Abs. 1 DSGVO.

⁴⁶ Vgl. Art. 6 Abs. 1 DSGVO.

⁴⁷ Vgl. Art. 9 Abs. 2 DSGVO.

⁴⁸ Vgl. Art. 9 Abs. 2 lit. a DSGVO.

⁴⁹ Vgl. Art. 9 Abs. 2 lit. b DSGVO.

⁵⁰ Vgl. Art. 9 Abs. 2 lit. c DSGVO.

- die Verarbeitung bezieht sich auf personenbezogene Daten, die die betroffene Person offensichtlich öffentlich gemacht hat;⁵¹
- die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder bei Handlungen der Gerichte im Rahmen ihrer justiziellen Tätigkeit erforderlich;⁵²
- die Verarbeitung ist für Zwecke der Gesundheitsvorsorge oder der Arbeitsmedizin, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Versorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- oder Sozialbereich erforderlich;⁵³
- die Verarbeitung ist für im öffentlichen Interesse liegende Archivzwecke, für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke erforderlich.⁵⁴

Neben diesen besonderen Erlaubnistatbeständen müssen immer noch die allgemeinen Datenschutzbestimmungen (insbesondere die Datenschutzgrundsätze⁵⁵) eingehalten werden. Sofern neben den besonderen Kategorien personenbezogener Daten auch noch einfache Kategorien personenbezogener Daten verarbeitet werden, müssen hierfür die üblichen Erlaubnistatbestände⁵⁶ ergänzend herangezogen werden.

4.3.2.3 Daten über strafrechtliche Verurteilungen und Straftaten (EU/EWR)

Die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Sicherungsmaßnahmen darf in der EU/ EWR nur unter behördlicher Aufsicht vorgenommen werden.⁵⁷

4.3.2.4 Dokumentation

Die Verarbeitung von besonderen Kategorien personenbezogener Daten⁵⁸ ist in der Verarbeitungsbeschreibung und Asset-Beschreibung zu dokumentieren. Konkret müssen hierzu insbesondere die besondere Kategorie der personenbezogenen Daten, der jeweilige Zweck sowie die einschlägige Rechtsgrundlage der Datenverarbeitung dokumentiert werden.

4.3.2.5 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer bzw. Auftraggeber eines Projekts bei einer neuen Verarbeitung	<ul style="list-style-type: none"> ▪ Prüft anhand von bereitgestellten Hilfsmitteln gemeinsam mit dem Datenschutz-Koordinator, ob und inwieweit besondere Kategorien personenbezogener Daten und/oder Daten über strafrechtliche Verfolgung im Rahmen von Verarbeitungen im normalen Geschäftsbetrieb oder im zu gestaltenden Prozesses oder Asset vorliegen bzw. vorkommen. ▪ Prüft regelmäßig, ob ausreichende organisatorische Maßnahmen (TOM) zur Überprüfung der Kategorie der Daten bestehen. ▪ <u>Sofern zutreffend:</u> Prüft mit dem Datenschutz-Koordinator regelmäßig, ob die Verarbeitung von besonderen Kategorien personenbezogener Daten und/oder Daten über strafrechtliche Verfolgung auf einer geeigneten Rechtsgrundlage beruhen. ▪ <u>In bestimmten Fällen erforderlich:</u> Prüft, ob ausreichende technische und organisatorische Maßnahmen bestehen (vgl. Vorgaben aus Ziffer 4.11), um eine Verarbeitung ausschließlich durch Personen, die dem Berufsgeheimnis oder einer gesonderten Verschwiegenheit unterliegen, zu gewährleisten. ▪ Bindet bei Verarbeitungen im normalen Geschäftsbetrieb und bei neuen Verarbeitungstätigkeiten bzw. der Planung neuer IT-Tools die Data Privacy Organization ein.

⁵¹ Vgl. Art. 9 Abs. 2 lit. e DSGVO.

⁵² Vgl. Art. 9 Abs. 2 lit. f DSGVO.

⁵³ Vgl. Art. 9 Abs. 2 lit. h DSGVO.

⁵⁴ Vgl. Art. 9 Abs. 2 lit. j DSGVO, Art. 89 Abs. 1 DSGVO und § 27 BDSG.

⁵⁵ Vgl. Art. 5 DSGVO.

⁵⁶ Vgl. Art. 6 Abs. 1 DSGVO.

⁵⁷ Vgl. Art. 10 DSGVO.

⁵⁸ Nachfolgend sind hiermit vereinfacht die besonderen personenbezogenen Daten nach Art. 9 und Art. 10 DSGVO gemeint.

Rolle	Verantwortung
Einkauf bzw. IT-Abteilung (IT-Contract / Vendor Management, IT-Li- cense Management, IT-De- mand Management)	<ul style="list-style-type: none"> ▪ Prüft bei einem geplanten Geschäftsprozess oder bei einer Bestellung von (IT-) Leistungen/Dienstleistungen, ob besondere Kategorien personenbezogener Daten oder Daten über strafrechtliche Verurteilungen und Straftaten vorkommen. ▪ Sofern zutreffend: Meldet dies der Data Privacy Organization und weist den Fachbereich auf die Einbindung der Data Privacy Organization hin. ▪ Verankert die Überprüfung auf das Vorliegen von besondere Kategorien personenbezogener Daten oder Daten über strafrechtliche Verurteilungen und Straftaten in den Einkaufsprozessen.
Projektmanagement	<ul style="list-style-type: none"> ▪ Verankert die Überprüfung auf das Vorliegen von besondere Kategorien personenbezogener Daten oder Daten über strafrechtliche Verurteilungen und Straftaten im Projektmanagement-Handbuch.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Prüft anhand von bereitgestellten Hilfsmitteln, ob und inwieweit besondere Kategorien personenbezogener Daten im Rahmen des zu gestaltenden Prozesses oder des Assets vorliegen bzw. vorkommen. ▪ Prüft regelmäßig, ob die Verarbeitung von besonderen Kategorien personenbezogener Daten und/oder Daten über strafrechtliche Verfolgung auf einer geeigneten Rechtsgrundlage beruhen.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Berät zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist unterstützend und beratend tätig. ▪ Stellt geeignete Hilfsmittel zur Überprüfung und Dokumentation zur Verfügung.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist hierzu überwachend und beratend tätig.⁵⁹

4.4 Zuständigkeit bei Datenverarbeitungen und Projekten

4.4.1 Neue Verarbeitungen und neue Assets

Neue Verarbeitungen und neue Assets **müssen** durch die zuständigen *Projektleiter* oder *Eigentümer* vor der ersten Verarbeitung personenbezogener Daten den geforderten datenschutzrelevanten Prozessen unterzogen werden, um ihre Datenschutzkonformität zu gewährleisten.

Zuständig dafür ist grundsätzlich der Fachbereich, der auch für die Einholung von Freigaben seiner Geschäftsprozesse für den Produktivbetrieb zuständig ist. Das kann bei überwiegend technischen Verarbeitungen oder Assets auch ein IT-Fachbereich sein. Wenn hierzu keine eindeutige Zuordnung zu Fachbereichen vorliegt, z. B. weil eine Verarbeitung von vielen Fachbereichen genutzt wird, wie beispielsweise eine Textverarbeitung, ein Email-Programm oder ein übergreifend verfügbares Archivsystem, dann ist der jeweilige Projektleiter in Abstimmung mit dem Auftraggeber des Projektes zuständig dafür, dass die geforderten datenschutzrelevanten Prozesse bearbeitet werden.

Spätestens zur Produktivsetzung eines Geschäftsprozesses oder Assets wird durch den Fachbereich, dem die fachliche Verantwortung für den Geschäftsprozess zugeordnet ist, der Prozesseigentümer bzw. Asset Eigentümer sowie ein Ansprechpartner für die Data Privacy Organization bestimmt. Andernfalls liegt diese Rolle bei dem Hauptabteilungsleiter im Fachbereich. Der Prozesseigentümer und der Asset-Eigentümer sind in der Verarbeitungsbeschreibung bzw. Asset-Beschreibung zu dokumentieren.

4.4.2 Besonderheit: „Alte“ Geschäftsprozesse ohne Zuständigkeit

In Zusammenhang mit alten Geschäftsprozessen sind ebenfalls die datenschutzrechtlichen Anforderungen einzuhalten und eine datenschutzkonforme Verarbeitung zu gewährleisten. Sollte es sich um einen bestehenden, alten Geschäftsprozess ohne Zuständigkeit handeln und sich kein Prozesseigentümer finden, so wird durch den zuständigen Data Privacy Officer ein Fachbereich bestimmt. Eskalationsstufe an dieser Stelle ist die zuständige Geschäftsführung. Bei divisionsweiten Geschäftsprozessen ist es die Divisionsleitung und bei divisionsübergreifenden Geschäftsprozessen der Vorstand der Rheinmetall AG.

⁵⁹ Vgl. Art. 39 Abs. 1 lit b DSGVO.

4.4.3 Änderung der Verarbeitung oder des Assets

Jede Änderung von Verarbeitungen personenbezogener Daten oder Assets müssen vor Produktivübergabe (Beginn der produktiven Nutzung) dahingehend überprüft werden, ob datenschutzrelevante Prozesse zu bearbeiten sind (Berücksichtigung datenschutzrechtlicher Anforderungen). Sofern zutreffend, müssen die datenschutzrelevanten Prozesse vor Produktivübergabe durchlaufen und abgeschlossen werden. Die Zuständigkeit hierfür liegt bei dem benannten Prozesseigentümer bzw. dem Asset-Eigentümer.

Prozess- und Asset-Eigentümer müssen sicherstellen, dass wesentliche Änderungen bei der Verarbeitung oder am Asset datenschutzkonform erfolgen und aktuell im Verzeichnis der Verarbeitungstätigkeiten erfasst sind.

4.5 Rechtmäßigkeit der Verarbeitung

4.5.1 Zweckbestimmung und Rechtsgrundlagen

4.5.1.1 Einleitung

Es ist sicherzustellen, dass für jede Datenverarbeitung die konkreten Zwecke und Rechtsgrundlagen festgelegt und dokumentiert sind.

Der Prozesseigentümer **muss** die Rechtmäßigkeit der Verarbeitung personenbezogener Daten sicherstellen.

Jede Erhebung, Verarbeitung, Nutzung und Übermittlung von personenbezogenen Daten sind im Grundsatz unzulässig, es sei denn, die Datenverarbeitung ist im Einzelfall durch eine gesetzliche Rechtfertigung oder die wirksame Einwilligung der betroffenen Personen erlaubt.

4.5.1.2 Beschreibung

Die Verarbeitung personenbezogener Daten ist grundsätzlich untersagt. Zulässig wird die Verarbeitung erst dann, wenn die konkreten Zwecke der Verarbeitung formuliert sind und diese auf eine Rechtsgrundlage gestützt werden können. Als Rechtsgrundlagen kommen die Einwilligung der betroffenen Personen oder eine gesetzliche Erlaubnis in Betracht.⁶⁰ Relevante gesetzliche Erlaubnistatbestände in der EU/EWR sind beispielsweise:

- Die Verarbeitung personenbezogener Daten ist für die Erfüllung eines Vertrages mit der betroffenen Person erforderlich sind. Erfasst wird auch die Datenverarbeitung für die Durchführung vorvertraglicher Maßnahmen, soweit diese auf eine Initiative der betroffenen Person zurückgehen.⁶¹ Dieser Erlaubnistatbestand kann beispielsweise für das Anfordern eines Angebots, das Bewerberauswahlverfahren oder für den Abschluss von Beschäftigten- oder Mietverträgen herangezogen werden. Achtung: Es muss sich hierbei um einen Vertrag bzw. eine Vertragsanbahnung zwischen dem Verantwortlichen und der betroffenen Person handeln!
- Die Verarbeitung personenbezogener Daten ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt.⁶² Mit anderen Worten: Das Unternehmen ist aufgrund einer gesetzlichen Regelung zur Verarbeitung der Daten verpflichtet. Hierzu zählen häufig Regelungen aus dem Handels-, Gesellschafts-, Aktien-, Steuer-, Sozialversicherungs- oder Arbeitsrecht.
- Die Verarbeitung personenbezogener Daten ist erforderlich, um berechnete Interessen des Verantwortlichen oder eines Dritten zu wahren.⁶³ Dieser Erlaubnistatbestand kann beispielsweise für die Erstellung von Statistiken mit einfachen personenbezogenen Daten herangezogen werden. Hierbei müssen die berechtigten Interessen des Verantwortlichen/Dritten an der Verarbeitung jedoch gegenüber den Interessen der betroffenen Personen (gegen diese Verarbeitung) überwiegen. Es ist daher durch den Prozess- bzw. Asset-Eigentümer eine Interessenabwägung im Einzelfall durchzuführen.
- In Deutschland gelten für den Beschäftigtenkontext zusätzlich u. a. folgende besondere Erlaubnistatbestände:

⁶⁰ Die Einwilligung wird an anderer Stelle gesondert dargestellt.

⁶¹ Vgl. Art. 6 Abs. 1 lit. b DSGVO.

⁶² Vgl. Art. 6 Abs. 1 lit. c DSGVO, hier kommen insbesondere steuerrechtliche Aufbewahrungspflichten aus dem Handelsgesetzbuch (§ 257 HGB) oder der Abgabenordnung (§ 147 AO) in Betracht.

⁶³ Vgl. Art. 6 Abs. 1 lit. f DSGVO.

- Die Verarbeitung personenbezogener Daten ist zur Begründung, Durchführung oder Beendigung des Beschäftigungsverhältnisses mit der betroffenen Person erforderlich.⁶⁴ Dies gilt z. B. für die Führung der Personalakte oder die Nutzung von IT-Arbeitsmitteln.
- Die Verarbeitung personenbezogener Daten ist zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich. Hier sind insbesondere Betriebsvereinbarungen relevant, die etwa den Einsatz bestimmter IT-Anwendungen und die damit verbundenen Verarbeitungstätigkeiten regeln.

Welche Rechtsgrundlage im Einzelfall maßgeblich ist, bestimmt sich insbesondere nach den konkreten Verarbeitungszwecken sowie den jeweiligen Kategorien von personenbezogenen Daten und von betroffenen Personen. Für eine Verarbeitungstätigkeit können auch mehrere Rechtsgrundlagen einschlägig sein, wenn etwa mehrere Kategorien von betroffenen Personen (z. B. Beschäftigte und Dritte) und/oder verschiedene Kategorien von personenbezogenen Daten (z. B. Stammdaten zur Vertragserfüllung, zusätzliche Daten im Rahmen einer Befragung) vorliegen.

4.5.1.3 Dokumentation

Die Verarbeitung von personenbezogenen Daten, die konkreten Verarbeitungszwecke und die entsprechende Rechtsgrundlage sind in der jeweiligen Verarbeitungstätigkeit und Asset-Beschreibung zu dokumentieren (vgl. Ziffer 5) sowie in die Datenschutzinformationen (vgl. Ziffer 4.6) für die von der Datenverarbeitung betroffenen Personen aufzunehmen.

4.5.1.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer & Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Stellt sicher, dass für seine Verarbeitungen entsprechende Zwecke und geeignete Rechtsgrundlagen festgelegt und dokumentiert sind. ▪ Prüft bei Änderung oder Neueinführung einer Verarbeitungstätigkeit, ob ausreichende organisatorische Maßnahmen zur Überprüfung des Vorliegens von geeigneten Rechtsgrundlagen zu Datenverarbeitungsvorgängen bestehen und dokumentiert dies.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Prüft das Vorliegen von Rechtsgrundlagen zu Datenverarbeitungsvorgängen in seinem Bereich und dokumentiert dies.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Berät zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Unterstützt bei der Durchführung und Dokumentation von Interessenabwägungen. ▪ Ist unterstützend und beratend tätig. ▪ Stellt geeignete Hilfsmittel zur Überprüfung und Dokumentation zur Verfügung.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist hierzu überwachend und beratend tätig.⁶⁵

4.5.2 Weiterverarbeitung personenbezogener Daten zu anderen Zwecken

4.5.2.1 Einleitung

Eine nachträgliche Änderung der festgelegten Zwecke einer Verarbeitungstätigkeit ist nur unter besonderen Voraussetzungen zulässig.⁶⁶ Es ist sicherzustellen, dass bei der Zweckänderung die rechtlichen Anforderungen eingehalten werden. Der Prozesseigentümer muss regelmäßig prüfen, ob bei der Änderung der Verarbeitungstätigkeit oder bei einer neuen Verarbeitungstätigkeit, die mit bestehenden Daten durchgeführt werden soll, die rechtlichen Anforderungen eingehalten werden.

⁶⁴ Vgl. § 26 Abs. 1 S. 1 BDSG.

⁶⁵ Vgl. Art. 39 Abs. 1 lit b DSGVO.

⁶⁶ Vgl. Art. 5 Abs. 1 lit. b, Art. 6 Abs. 4, Art. 13 Abs. 3 DSGVO.

4.5.2.2 Regelfall

Der Prozess ist durchzuführen, wenn eine Zweckänderung beabsichtigt ist und die Voraussetzungen für eine zulässige Zweckänderung vorliegen. Eine Zweckänderung liegt vor, wenn die Daten zu einem anderen Zweck als dem bei der Datenerhebung festgelegten und mitgeteilten Zweck verarbeitet werden sollen.

Vor einer Weiterverarbeitung zu einem neuen Zweck **muss** der *Prozesseigentümer* prüfen, ob der neue Zweck mit den bei Erhebung bekannten Zwecken vereinbar/kompatibel ist (Kompatibilitätsprüfung).

Dazu ist es erforderlich, dass der Prozesseigentümer sicherstellt, dass bei Zweckänderungen die ursprünglich mitgeteilten Zwecke ohne größeren Aufwand selektiert und die hiervon betroffenen Personen identifiziert werden können (beispielsweise durch Versionierung von ausgehändigten/bereitgestellten Datenschutzinformationen).

Bei der Prüfung der Zulässigkeit einer Zweckänderung sind folgende Kriterien zu berücksichtigen:

- inhaltliche Verbindung zwischen den Zwecken,
- der Zusammenhang, in dem die personenbezogenen Daten erhoben wurden, insbesondere das Verhältnis zwischen betroffener Person und Verantwortlichem,
- Art der personenbezogenen Daten,
- mögliche Folgen für die betroffene Person,
- Vorhandensein geeigneter Garantien (z. B. Verschlüsselung oder Pseudonymisierung).⁶⁷

Außerdem muss die Weiterverarbeitung stets auf einer eigenständigen Rechtsgrundlage⁶⁸ beruhen, die bloße Kompatibilität der neuen und ursprünglichen Zwecke genügt nicht.⁶⁹

Liegen die Voraussetzungen inkl. der notwendigen Kompatibilität vor, ist die betroffene Person vor der Weiterverarbeitung über den neuen Zweck sowie über folgende Punkte zu informieren:⁷⁰

- geplante Speicherdauer, falls möglich, andernfalls die Kriterien für die Festlegung der Speicherdauer,
- Information über das Recht auf Auskunft, Berichtigung, Löschung oder Einschränkung der Verarbeitung oder das Widerspruchsrecht gegen diese Verarbeitung und das Recht auf Datenübertragbarkeit,
- Beschwerderecht der betroffenen Person bei der Aufsichtsbehörde,
- Herkunft der Daten, soweit diese nicht bei der betroffenen Person selbst erhoben wurden,
- das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren und
- im Falle eines Datentransfers in ein Drittland auch die geeigneten Garantien für den Datentransfer (z. B. vereinbarte Standard-Datenschutzklauseln oder verbindliche interne Datenschutzvorschriften).

Die Information über die zuvor genannten Punkte kann entfallen, soweit die betroffene Person bereits über die Informationen verfügt.

Nach erfolgter Information über den neuen Zweck darf die Weiterverarbeitung zu dem neuen Zweck durchgeführt werden.

Liegt keine Kompatibilität der Zwecke vor, ist eine Weiterverarbeitung unzulässig.

Die Entscheidung über das Vorliegen der Voraussetzung einer zulässigen Zweckänderung darf nur nach Rücksprache mit der Data Privacy Organization getroffen werden.

⁶⁷ Vgl. Art. 6 Abs. 4 DSGVO sowie Art. 6 Abs. 1 DSGVO.

⁶⁸ Etwa nach Art. 6 Abs. 1 DSGVO. Hierbei kann es sich auch um die gleiche Art der Rechtsgrundlage wie vor der Zweckänderung handeln.

⁶⁹ Auch wenn ausweislich des Wortlautes des ErwGr. 50 S.2 der DSGVO keine andere gesonderte Rechtsgrundlage als erforderlich erachtet, wird dies gemeinhin als redaktionelles Versehen betrachtet.

⁷⁰ Vgl. Art. 13 Abs. 2 DSGVO.

4.5.2.3 Ausnahme

In bestimmten Fällen ist ausnahmsweise keine Prüfung der Zweckvereinbarkeit durchzuführen und es bedarf auch keiner neuen Rechtsgrundlage. Dies ist beispielsweise der Fall, wenn die Weiterverarbeitung auf einer erneuten Einwilligung beruht⁷¹ oder im öffentlichen Interesse liegenden statistischen Zwecken dient.⁷²

Außerdem können in den jeweiligen nationalen Regelungen zum Datenschutz Aufgaben und Zwecke bestimmt und konkretisiert werden, für die eine Weiterverarbeitung als vereinbar und rechtmäßig erachtet wird.⁷³ In Deutschland ist eine Verarbeitung zu anderen Zwecken auch ohne Kompatibilitätsprüfung in folgenden Fällen möglich⁷⁴:

- Die Verarbeitung ist zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist.
- Die Verarbeitung ist zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist, sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

4.5.2.4 Dokumentation

Die Durchführung der Zweckänderung sowie der neue Zweck sind im Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren. Konkret müssen hierzu insbesondere das Ergebnis der Prüfung der Zweckvereinbarkeit sowie die Rechtsgrundlage der Weiterverarbeitung und die erfolgte Information an die betroffene Person dokumentiert werden. Der neue Zweck ist ebenfalls in die betroffenen Verarbeitungsbeschreibungen aufzunehmen. Zudem sind beispielsweise die unterschiedlichen Versionen von Datenschutzinformationen und Einwilligungserklärung im Zeitablauf abzulegen.

4.5.2.5 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none"> ▪ Prüft im Rahmen einer neuen Verarbeitung bzw. eines Projekts gemeinsam mit dem Datenschutz-Koordinator, ob und inwieweit personenbezogene Daten vorliegen. ▪ <u>Sofern sich eine Zweckänderung im normalen Geschäftsbetrieb (ohne Projekt) ergibt: Prüft</u> gemeinsam mit dem Datenschutz-Koordinator und/oder dem Asset-Eigentümer die Zweckänderung und dokumentiert dies. ▪ Zieht die Data Privacy Organization zur Beratung hinzu. ▪ Prüft regelmäßig, ob ausreichende organisatorische Maßnahmen für eine Prüfung der Zweckvereinbarkeit getroffen wurden, durch die eine zulässige Weiterverarbeitung erfolgen kann. ▪ Erfüllt die Informationspflicht nach Ziffer 4.6.2.3.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Aktualisiert ggfs. die Datenschutzinformationen (neue Zwecke können ggfs. umfangreiche aktive Informationspflichten auslösen).
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Berät zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist unterstützend und beratend tätig. ▪ Stellt geeignete Hilfsmittel zur Überprüfung und Dokumentation zur Verfügung.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist hierzu überwachend und beratend tätig.⁷⁵

⁷¹ Ausnahmen nach Art. 6 Abs. 4 DSGVO sowie § 24 BDSG, nationale Regelungen der jeweiligen Länder sind zu beachten.

⁷² Vgl. Art. 5 Abs. 1 lit. b DSGVO.

⁷³ Vgl. Erwägungsgrund 50.

⁷⁴ Vgl. § 24 BDSG.

⁷⁵ Vgl. Art. 39 Abs. 1 lit b DSGVO.

4.5.3 Einwilligung

4.5.3.1 Einleitung

Die Einwilligung der betroffenen Person in die Verarbeitung ihrer personenbezogenen Daten ist eine weitere mögliche Rechtsgrundlage. Soll die Datenverarbeitung auf eine Einwilligung gestützt werden, ist sicherzustellen, dass die strengen Anforderungen an eine wirksame Einwilligung eingehalten werden.

4.5.3.2 Regelfall: Erteilung einer Einwilligung

Die betroffene Person kann sowohl in die Verarbeitung personenbezogener Daten als auch in die Verarbeitung besonderer Kategorien personenbezogener Daten „ausdrücklich“ einwilligen.

Eine Einwilligung ist jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen, eindeutig bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist. Die Einwilligung muss

- in Kenntnis der Sachlage (sogenannte Informiertheit),
- für den konkreten Einzelfall (sogenannte Bestimmtheit) und
- ohne Zwang (sogenannte Freiwilligkeit) abgegeben werden.

Hierbei ist zu berücksichtigen, dass sich die betroffene Person nicht einer Drucksituation ausgesetzt sehen darf. Zudem müssen Datenverarbeitungen, die auf eine Einwilligung gestützt werden, von der betroffenen Person erwartbar sein. Die betroffene Person muss somit mit dem Umfang einer Datenverarbeitung rechnen können (Stichworte: Treu und Glauben, vernünftige Erwartungshaltung). Dies kann beispielsweise der Fall sein, wenn die Erfüllung eines Vertrages von der Einwilligung in eine Datenverarbeitung abhängig gemacht wird (Kopplungsverbot). Besonders im Beschäftigungsverhältnis wird es regelmäßig an der „Freiwilligkeit“ der Einwilligung eines Beschäftigten gegenüber seinem Arbeitgeber (aufgrund des Abhängigkeitsverhältnisses) fehlen. Für die Freiwilligkeit wird hier insbesondere das Vorliegen eines rechtlichen oder wirtschaftlichen Vorteils für den Beschäftigten (z. B. Privatnutzung eines dienstlichen Smartphones) oder zumindest gleichgelagerte Interessen zwischen dem Beschäftigten und seinem Arbeitgeber (z. B. Foto des Beschäftigten im Intranet) gefordert.⁷⁶

Die Einwilligungserklärung sollte inhaltlich zumindest den Verantwortlichen nennen und den Zweck der Verarbeitung enthalten. Ist die Einwilligungserklärung Teil einer schriftlichen Vereinbarung, muss die Erklärung abgrenzbar von anderen Sachverhalten sein. Die Einwilligung bedarf, außer im Beschäftigungsverhältnis, keiner besonderen Form und kann schriftlich, elektronisch sowie mündlich eingeholt werden. Bei einer Einwilligung im Beschäftigungsverhältnis ist grundsätzlich die Textform vorzusehen.

Bei der Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten ist darüber hinaus eine ausdrückliche Einwilligungserteilung erforderlich.

4.5.3.3 Widerruf der Einwilligung

Die Einwilligung kann jederzeit mit Wirkung für die Zukunft widerrufen werden. Dabei muss der Widerruf genauso einfach wie die Erteilung der Einwilligung gestaltet sein. Die betroffene Person ist zudem vor Abgabe der Einwilligungserklärung über die Möglichkeit des jederzeitigen Widerrufs in Kenntnis zu setzen. Die Rechtmäßigkeit der Datenverarbeitung bis zum Zeitpunkt des Widerrufs wird durch den Widerruf nicht berührt.

Ab dem erklärten Widerruf der Einwilligung **muss** die Verarbeitung der personenbezogenen Daten der widerrufenden Person unverzüglich eingestellt oder zumindest auf das gesetzlich zulässige Maß (z. B. zur Erfüllung gesetzlicher Aufbewahrungspflichten) eingeschränkt werden.

⁷⁶ Vgl. § 26 Abs. BDSG.

4.5.3.4 Ausnahmefall: Fortgeltung einer Einwilligung⁷⁷

Von betroffenen Personen, die bereits vor dem 25. Mai 2018 in eine Datenverarbeitung gemäß der bis dahin maßgeblichen Datenschutzrichtlinie 95/46/EG wirksam eingewilligt haben, muss keine erneute Einwilligung eingeholt werden, wenn die Art der bereits erteilten Einwilligung den Anforderungen der DSGVO entspricht.⁷⁸

Im Fall der Fortgeltung einer Einwilligung **muss** Rücksprache mit der *Data Privacy Organization* oder dem zuständigen *Datenschutzbeauftragten* gehalten werden.

4.5.3.5 Dokumentation

Die Erteilung der Einwilligung (digital sowie analog) und der Hinweis auf das Widerrufsrecht sind in dem genutzten elektronischen System zu dokumentieren. Aus Gründen der Rechenschaftspflicht sollte die Einwilligung in Schrift- oder Textform eingeholt und dokumentiert werden.

4.5.3.6 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none"> ▪ Prüft regelmäßig, ob für eine beabsichtigte Verarbeitung personenbezogener Daten die Einholung einer Einwilligung bei der betroffenen Person erforderlich ist. ▪ Prüft (sofern eine Einwilligung bereits vorliegt), ob die Voraussetzungen für eine wirksame Einwilligung noch vorliegen und ob der beabsichtigte Zweck der Verarbeitung noch von der Reichweite der Einwilligung gedeckt ist. ▪ Überprüft die Formulierung der Einwilligungserklärung (Einwilligungstext), die Einholung einer wirksamen Einwilligung und die Reichweite der Einwilligung. ▪ Überprüft gemeinsam mit dem Datenschutz-Koordinator die Auswirkungen auf die Verarbeitung, wenn keine Einwilligung vorliegt oder eine Einwilligung widerrufen wird und dokumentiert die Auswirkungen zur jeweiligen Verarbeitungstätigkeit. ▪ Dokumentiert die Erteilung der Einwilligung (digital sowie analog). ▪ Stellt sicher, dass keine Datenverarbeitung erfolgt, so lange keine Einwilligung der betroffenen Person vorliegt. ▪ Führt die Kontrollen sowohl regelmäßig (mindestens alle zwei Jahre) als auch anlassbezogen bei der Veränderung der zu Grunde liegenden Verarbeitungstätigkeit oder des genutzten Assets durch.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Formuliert den Einwilligungstext und legt diese der Data Privacy Organization zur Überprüfung vor.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Prüft die Einwilligungstext auf Datenschutzkonformität. ▪ Ist unterstützend und beratend tätig. ▪ Stellt geeignete Hilfsmittel zur Überprüfung und Dokumentation zur Verfügung.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist hierzu überwachend und beratend tätig.⁷⁹

4.6 Informationspflichten

4.6.1 Einleitung

Es ist sicherzustellen, dass betroffene Personen rechtzeitig und im geforderten Rahmen über die sie betreffende Verarbeitung personenbezogener Daten informiert werden.⁸⁰ Der Prozess der Informationsgewährung unterscheidet sich dabei geringfügig, wenn die Daten entweder bei der Person selbst oder aber bei einem Dritten

⁷⁷ Hierbei handelt es sich um eine Besonderheit der DSGVO.

⁷⁸ Vgl. ErwGr. 171 DSGVO.

⁷⁹ Vgl. Art. 39 Abs. 1 lit b DSGVO.

⁸⁰ Vgl. Art. 13 und Art. 14 DSGVO.

erhoben werden. Die Vorgaben aus Ziffer 7.2 sind bei der Gestaltung und Erteilung von Informationen ebenfalls zu berücksichtigen.

4.6.2 Beschreibung

4.6.2.1 Regelfall: Erhebung bei der betroffenen Person

Der Prozess ist bei jeder Erhebung von personenbezogenen Daten zu beachten. Dabei ist eine Erhebung das Beschaffen personenbezogener Daten durch aktives Tätigwerden, wie etwa die Aufforderung zur Beantwortung von Fragen, die Bereitstellung eines Formulars oder einer Eingabemaske.

Spätestens zum Zeitpunkt einer solchen Erhebung sind der betroffenen Person mitzuteilen:

- Kontaktdaten des Verantwortlichen,
- ggf. des Vertreters und
- ggf. des DSB,
- Zweck und Rechtsgrundlage,
- ggf. berechtigtes Interesse der Verarbeitung,
- Kategorien der Daten,
- Empfänger/Empfängerkategorien,
- geplante Übermittlung in ein Drittland,
- Dauer der Verarbeitung,
- Betroffenenrechte,
- Verpflichtung der Obliegenheit zur Bereitstellung der Daten und
- Bestehen einer automatisierten Entscheidungsfindung.

Die Unternehmen im Rheinmetall Konzern halten für die mitzuteilenden Informationen entsprechende Übersichten (die sogenannten „Datenschutzinformationen“) bereit, mit denen die relevanten Informationspflichten zielgruppengerecht erfüllt werden können. Die Datenschutzinformationen sind je nach Unternehmen, Zwecken der Verarbeitung und Rolle der betroffenen Person bedarfsgerecht gestaltet.

Im Rahmen von Kontaktaufnahmen, bei denen personenbezogene Daten erhoben werden, lösen beispielsweise bereits implementierte Prozesse den Versand geeigneter Datenschutzinformationen (siehe Ziffer 7.2) zur Erfüllung der Informationspflichten aus oder die Datenschutzinformation erfolgt gesondert, z. B. mündlich bei Telefonkontakt. In solchen Fällen wird der betroffenen Person angeboten, die Informationen schriftlich zur Verfügung zu stellen oder es erfolgt ein Verweis auf eine entsprechende Datenschutzinformation im Internetauftritt.

4.6.2.2 Erhebung bei Dritten

In dem Sonderfall, dass die Daten nicht bei der betroffenen Person selbst (z. B. durch Ausfüllen eines Formulars), sondern bei einem Dritten (z. B. in einer Personen-Datenbank oder bei Behörden) erhoben werden, sind der betroffenen Person die oben genannten Datenschutzinformationen zuzüglich der Quellen der Daten innerhalb eines Monats mitzuteilen. Zudem ist anzugeben, ob es sich hierbei um eine öffentlich zugängliche Quelle handelt.

Ausnahme: Stammen die Daten aus mehreren Quellen und kann die Herkunft nicht mehr eindeutig bestimmt werden, muss ausnahmsweise eine allgemeine Information gegeben werden.

4.6.2.3 Zweckänderung

Sollen bereits erhobene Daten für einen anderen als den ursprünglich geplanten Zweck verarbeitet werden (vgl. Ziffer 4.5.2), so müssen der betroffenen Person all jene Informationen zur Verfügung gestellt werden, die sich aus der Zweckänderung ergeben. Dies betrifft mindestens die neue Zweckbeschreibung und die Rechtsgrundlage.

4.6.2.4 Ausnahmen

Ausnahmsweise kann die Informationspflicht entfallen. Dies ist insbesondere in folgenden Fällen gegeben:

- Die betroffene Person gibt ohne jede Aufforderung eigene personenbezogene Daten preis;
- Die betroffene Person verfügt bereits über die Informationen, die mitzuteilen wären;

- Die Erteilung der Information wäre unmöglich oder mit unverhältnismäßigem Aufwand verbunden oder
- es liegt eine privilegierte Verarbeitung oder eine Gefährdung des Verarbeitungszweckes vor.

Die Entscheidung über das Entfallen einer Informationspflicht **darf** nur nach Rücksprache mit der *Data Privacy Organization* oder dem *Datenschutzbeauftragten* getroffen werden und **muss** schriftlich durch den *Prozesseigentümer* dokumentiert werden.

4.6.3 Dokumentation

Die Erfüllung der Informationspflichten ist zu dokumentieren. Der Inhalt und Umstand der Erfüllung der Informationspflicht ist in der jeweiligen Verarbeitungstätigkeit zu hinterlegen (vgl. Ziffer 5).

4.6.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none"> ▪ Prüft regelmäßig, ob Regelungen für die Informationspflicht an allen relevanten Kontaktpunkten zur Erhebung personenbezogener Daten getroffen wurden. ▪ Hält die Datenschutzinformationen inhaltlich aktuell sowie aussagekräftig. ▪ Stellt gemeinsam mit dem Datenschutz-Koordinator sicher, dass betroffene Personen rechtzeitig über die Datenverarbeitungen mittels der Datenschutzinformationen informiert werden. ▪ Stellt sicher, dass die Durchführung der Informationspflichten gegenüber der betroffenen Person in geeigneter Form erfolgt. ▪ Meldet alle für die Datenschutzinformationen relevanten Angaben unverzüglich an den Datenschutz-Koordinator. ▪ Führt Kontrollen mindestens alle zwei Jahre oder bei Änderung der Art und des Umfangs der Datenverarbeitung durch.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Stellt für seinen Bereich die Organisation der ordnungsgemäßen Erteilung von Informationen an betroffene Personen sicher. ▪ Erstellt zielgruppengerechte Datenschutzinformationen und legt diese der Data Privacy Organization zur Prüfung vor. ▪ Stellt gemeinsam mit dem Prozesseigentümer sicher, dass betroffene Personen rechtzeitig über die Datenverarbeitungen mittels der Datenschutzinformationen informiert werden. ▪ Führt die Datenschutzinformationen für die Abteilung/den Bereich zusammen. ▪ Übermittelt die Datenschutzinformationen an die Data Privacy Organization.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Hält die Datenschutzinformationen dokumentiert im Zeitablauf vor (Versionierung). ▪ Berät den Datenschutz-Koordinator. ▪ Stellt ein Muster für Datenschutzinformationen bereit.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist hierzu überwachend und beratend tätig.⁸¹

4.7 Datenübermittlung an Drittländer oder an internationale Organisationen (EU)

4.7.1 Einleitung

Grundsätzlich ist eine Übermittlung personenbezogener Daten nur innerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums erlaubt, eine Übermittlung an Drittländer (Länder außerhalb der EU / des EWR) oder internationale Organisationen ist nur unter zusätzlichen Voraussetzungen möglich.⁸² Es ist daher sicherzustellen, dass diese Voraussetzungen bei einer beabsichtigten Übermittlung an Drittländer eingehalten werden.

⁸¹ Vgl. Art. 39 Abs. 1 lit b DSGVO.

⁸² Drittländer sind alle Länder, die nicht Mitgliedstaat der EU oder des EWR sind.

Eine Übermittlung von Daten an Drittländer ist nur nach vorheriger Rücksprache mit der Data Privacy Organization zulässig.

4.7.2 Beschreibung

Wird eine Übermittlung personenbezogener Daten in ein Drittland beabsichtigt, müssen neben der Rechtmäßigkeit der Datenverarbeitung auch die Bedingungen an die Übermittlung in ein Drittland eingehalten werden. Dies gilt für den Verantwortlichen sowie für den Auftragsverarbeiter.⁸³

Durch den *Asset- oder Prozesseigentümer* **müssen** vor Übermittlung der Daten in ein Drittland geeignete Garantien etabliert werden.

4.7.2.1 Regelfall

In folgenden Fällen kann eine Übermittlung der personenbezogenen Daten zulässig sein:

4.7.2.2 Angemessenheitsbeschluss

Eine Übermittlung ist zulässig, wenn für das betreffende Land ein Angemessenheitsbeschluss besteht.⁸⁴ Durch einen solchen Beschluss legt die Europäische Kommission fest, dass in diesem Land ein angemessenes Datenschutzniveau gewährleistet ist. Drittländer mit angemessenem Datenschutzniveau sind beispielsweise Kanada und die Schweiz.⁸⁵

4.7.2.3 Geeignete Garantien

Besteht für ein Drittland kein Angemessenheitsbeschluss, ist eine Übermittlung personenbezogener Daten nur erlaubt, sofern geeignete Garantien für die Datenübermittlung bestehen und der betroffenen Person durchsetzbare Rechte und wirksame Rechtsbehelfe zur Verfügung stehen⁸⁶. Geeignete Garantien sind beispielsweise verbindliche interne Datenschutzvorschriften, sogenannte Binding Corporate Rules⁸⁷, oder von der Europäischen Kommission erlassene Standarddatenschutzklauseln⁸⁸.

Standarddatenschutzklauseln (bisher: Standardvertragsklauseln) kommen auch künftig grundsätzlich als geeignete Garantien für Übermittlungen in Nicht-EU-Staaten in Betracht. Die drei bislang von der Kommission beschlossenen Standardverträge bleiben in Kraft, bis sie „erforderlichenfalls“ durch die Kommission geändert, ersetzt oder aufgehoben werden.

Verbindliche interne Datenschutzvorschriften (Binding Corporate Rules) werden in der DSGVO als Möglichkeit zur Erbringung „geeigneter Garantien“ für Datenübermittlungen in Drittländer ausdrücklich anerkannt.

Genehmigte Verhaltensregeln (Code of Conduct, CoC) sowie genehmigte Zertifizierungsmechanismen können als Grundlage für Übermittlungen in Betracht kommen. Diese Instrumente können auch Übermittlungen aus mehreren Mitgliedstaaten abdecken. Für diesen Fall sind sie mit den Datenschutzbehörden aller Mitgliedstaaten im Kohärenzverfahren abzustimmen.

Für den Rheinmetall Konzern kommen grundsätzlich nur EU-Standarddatenschutzklauseln in Betracht, da die anderen vorgenannten Instrumente nicht wirksam zur Verfügung stehen.

Im Rahmen einer Auftragsverarbeitung kommt es u. a. maßgeblich darauf an, ob der Datenverarbeiter im Drittland ein angemessenes Datenschutzniveau einhält und einhalten kann. Ist dies nicht der Fall, ist zu prüfen, ob eine Ausnahme für die Übermittlung eingreift. Diese Regelung betrifft insbesondere sämtliche moderne Cloud

⁸³ Vgl. Art. 44 DSGVO.

⁸⁴ Vgl. Art. 45 Abs. 1 DSGVO.

⁸⁵ Bei einer Datenübermittlung in die Vereinigten Staaten ist in diesem Zusammenhang insbesondere die Selbstzertifizierung nach dem sogenannten „Privacy Shield“ zu berücksichtigen.

⁸⁶ Vgl. Art. 46 Abs. 1 DSGVO.

⁸⁷ Vgl. Art. 46 Abs. 2 lit. b DSGVO, wobei die Anforderungen des Art. 47 DSGVO eingehalten werden müssen.

⁸⁸ Vgl. Art. 46 Abs. 2 bis 3 DSGVO.

Services, die von Anbietern mit Sitz außerhalb der EU erbracht werden (z. B. Microsoft, Amazon oder Google), unabhängig davon, welchen Standort das Rechenzentrum hat.

Die Anforderungen an die Feststellung des angemessenen Datenschutzniveaus wurden im Vergleich zur bisherigen Rechtslage verschärft.⁸⁹

Ergänzend muss nun vom Datenexporteur geprüft werden, ob die gewählte Garantie in dem Drittland tatsächlich ein angemessenes Datenschutzniveau sicherstellt. Der Prüfungsmaßstab hierfür ergibt sich vornehmlich aus den Empfehlungen des Europäischen Datenschutzausschuss (EDSA)⁹⁰.

4.7.2.4 Zusätzliche (technische) Maßnahmen zur Absicherung

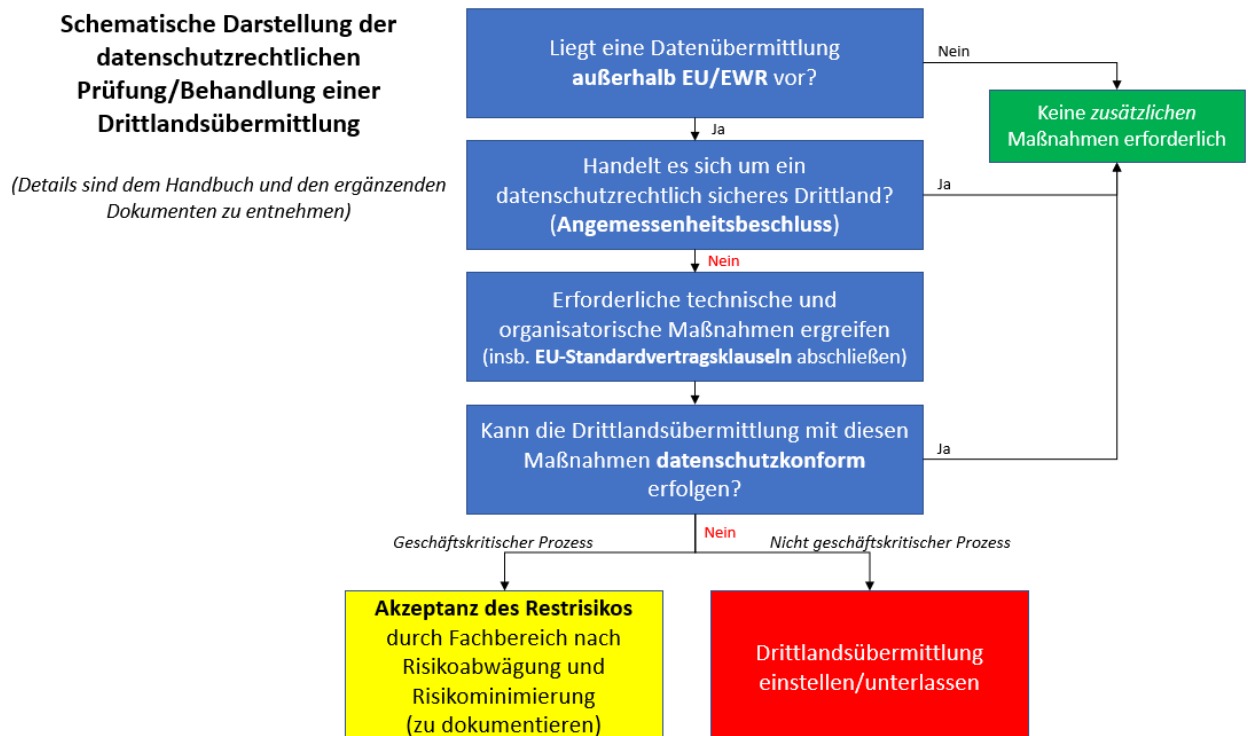
Führen die Standarddatenschutzklauseln nach Prüfung der Rechtslage im Drittland nicht zu einem angemessenen Datenschutzniveau, sind zusätzliche Maßnahmen zur Absicherung der Drittlandübermittlung zu ermitteln und festzulegen.

Sollte kein Angemessenheitsbeschluss oder geeignete Garantien vorliegen, **muss** der *Prozesseigentümer* bzw. der *Asset-Eigentümer* bei einer geplanten Datenübermittlung in ein Drittland den *Data Privacy Officer* oder *Datenschutzbeauftragten* zur Beratung hinzuziehen.

Die *Data Privacy Organization* **muss** bei jeder Drittlandübermittlung in der Datenschutzdokumentation ein entsprechendes Risiko für das Asset und die Verarbeitung dokumentieren.

Der *Prozess-* oder *Asset-Eigentümer* muss in Abstimmung mit dem *Data Privacy Officer* eine entsprechende Risikoübernahme/-akzeptanz durch das zuständige *Management* / *die Geschäftsführung* herbeiführen.

Für Unternehmen im Rheinmetall Konzern in der EU/EWR **müssen** zur Legitimierung eines Drittlandtransfers grundsätzlich EU-Standarddatenschutzklauseln eingesetzt werden. Zuständig für den Abschluss ist der *Prozesseigentümer* bzw. *Asset-Eigentümer*.



⁸⁹ vgl. Art. 45 Abs. 2 DSGVO.

⁹⁰ abgeleitet aus Art. 45 Abs. 2 DSGVO und aus den Empfehlungen 02/2020 des EDSA.

4.7.2.5 Fortgeltung

Bisher erteilte Genehmigungen sowie bisher ergangene Angemessenheitsbeschlüsse bleiben so lange gültig, bis sie von der Aufsichtsbehörde, den Gerichten oder mit einem Beschluss der Kommission geändert, ersetzt oder aufgehoben werden.⁹¹

4.7.2.6 Ausnahmefall

Liegt weder ein Angemessenheitsbeschluss noch eine geeignete Garantie vor, kann eine beabsichtigte Übermittlung noch ausnahmsweise unter bestimmten Bedingungen zulässig sein.

Die in der Praxis wichtigsten Ausnahmen sind insbesondere:

- Übermittlung zur Erfüllung eines Vertrages oder zur Durchführung von vorvertraglichen Maßnahmen auf Antrag der betroffenen Person,
- Übermittlung zum Abschluss oder zur Erfüllung eines im Interesse der betroffenen Person von dem Verantwortlichen mit einer anderen natürlichen oder juristischen Person geschlossenen Vertrags,
- Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen,
- Übermittlung zum Schutz lebenswichtiger Interessen der betroffenen Person oder anderer Personen, sofern die betroffene Person aus physischen oder rechtlichen Gründen außerstande ist, ihre Einwilligung zu geben,
- wenn eine Einzelgenehmigung einer Aufsichtsbehörde vorliegt,
- wenn die betroffenen Personen nach Information über die spezifischen Risiken der Datenübermittlung eingewilligt haben,
- wenn die Datenübermittlung einen überschaubaren Umfang hat und aufgrund zwingender berechtigter Interessen des Verantwortlichen gerechtfertigt ist (allerdings ist hier eine Information der Datenschutzaufsichtsbehörde und der betroffenen Personen erforderlich).⁹²

Der Prozess- bzw. Asset-Eigentümer **muss** bei Bestimmung von Ausnahmen *den* zuständigen Data Privacy Officer und Datenschutzbeauftragten einbinden.

Es obliegt dem Data Privacy Officer zu entscheiden ob eine der vorgenannten Ausnahmen vorliegt.

4.7.3 Dokumentation

Die Übermittlung personenbezogener Daten an ein Drittland oder eine internationale Organisation ist zu dokumentieren. In dem genutzten Archivsystem, Vertragsmanagementsystem und Verzeichnis von Verarbeitungstätigkeiten müssen konkret das betroffene Drittland, an das die Übermittlung erfolgt, benannt werden und die Art der personenbezogenen Daten sowie die rechtliche Grundlage, auf derer die Übermittlung erfolgt, dokumentiert werden. Insbesondere müssen auch die vorgenommene Interessenabwägung sowie die angemessenen Garantien dokumentiert werden.⁹³ Bei Datenübermittlungen in Drittländer sind erweiterte Angaben in die Datenschutzhinweise aufzunehmen (vgl. Ziffer 4.6). Dies umfasst z.B. die Absicht des Verantwortlichen, personenbezogene Daten an einen Empfänger in einem Drittland oder einer internationalen Organisation zu übermitteln, das Vorhandensein oder das Fehlen eines Angemessenheitsbeschlusses der Kommission oder im Falle von weiteren Übermittlungssachverhalten⁹⁴ ein Verweis auf die geeigneten oder angemessenen Garantien und die Möglichkeit, eine Kopie von ihnen zu erhalten oder einen Hinweis darauf, wo sie verfügbar sind.

4.7.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none">▪ Beachtet, dass nach Möglichkeit keine Dienstleister mit Sitz im Drittland ausgewählt werden. Es ist auch darauf zu achten, dass keine Sub-Dienstleister mit Sitz im Drittland eingesetzt werden.

⁹¹ Vgl. Art. 45 Abs. 9 und Art. 46 Abs. 5 DSGVO

⁹² Vgl. Art. 49 Abs. 1 S. 1 lit. a – g DSGVO, Vgl. zur Interessenabwägung und deren Voraussetzungen: Art. 49 Abs. 1 S. 2 bis S. 4 DSGVO.

⁹³ Vgl. Art. 49 Abs. 6 DSGVO.

⁹⁴ Vgl. Art. 46, Art. 47 und Art. 49 Abs. 1 DSGVO.

Rolle	Verantwortung
	<ul style="list-style-type: none"> ▪ Sofern erforderlich: Stellt eine Prüfung der Rechtslage im Drittland unter Einbindung der Rechtsabteilung sicher. ▪ Schließt zur Herstellung eines angemessenen Datenschutzniveaus grundsätzlich EU Standarddatenschutzklauseln mit dem Dienstleister oder Sub-Dienstleister im Drittland ab, sofern ein Dienstleister oder Sub-Dienstleister mit Sitz außerhalb der EU / des EWR (aus dem Drittland) zum Einsatz kommt. ▪ Holt die Vereinbarungen zwischen Dienstleister bzw. Sub-Dienstleister und den betroffenen Rheinmetall Gesellschaften ein. ▪ Prüft regelmäßig, ob ausreichende technische und organisatorische Maßnahmen zur Überprüfung der Zulässigkeit der Datenübermittlung in ein Drittland getroffen wurden. ▪ Bindet in Zweifelsfragen die Data Privacy Organization oder den zuständigen Datenschutzbeauftragten mit ein.
Einkauf	<ul style="list-style-type: none"> ▪ Beachtet, dass nach Möglichkeit keine Dienstleister mit Sitz im Drittland ausgewählt werden. Es ist auch darauf zu achten, dass keine Sub-Dienstleister mit Sitz im Drittland eingesetzt werden.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Erstellt und pfl egt geeignete Fragebögen und Checklisten und stellt diese zur Verfügung. ▪ Hält die jeweils aktuell gültigen EU Standarddatenschutzklauseln vor und stellt diese auf Anfrage zur Verfügung. ▪ Berät den Fachbereich und den Einkauf.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist hierzu überwachend und beratend tätig.⁹⁵

4.8 Löschung, Sperrung, Anonymisierung und Berichtigung von Daten

4.8.1 Einleitung

Es ist sicherzustellen, dass personenbezogene Daten betroffener Person gelöscht werden, soweit die in diesem Abschnitt genannten Voraussetzungen vorliegen. In diesem Fall müssen die Daten vernichtet oder unkenntlich gemacht werden.

4.8.2 Löschung von Daten, Vernichtung von Datenträgern

Eine Löschung ist vorzunehmen, wenn

- die Daten für den Zweck der Verarbeitung nicht mehr notwendig sind,
- die betroffene Person ihre Einwilligung zur Verarbeitung widerruft,
- die betroffene Person der Verarbeitung widerspricht oder
- die personenbezogenen Daten unrechtmäßig verarbeitet wurden.⁹⁶

Die Daten sind gelöscht, wenn es praktisch unmöglich ist, die zuvor in den zu löschenden Daten verkörperte Information zu erkennen. Dies erfordert unter Umständen den Einsatz spezieller Löschsoftware oder die physische Zerstörung des Datenträgers. Hierzu sind durch die *Informationssicherheit* und *IT-Sicherheit* konkrete Vorgaben zu machen. Konkrete Vorgaben können bei der Informations- und Unternehmenssicherheit angefordert werden.⁹⁷

Für Verarbeitungen, die personenbezogene Daten außerhalb von zentralen Lösungen/Systemen betreffen (z. B. sogenannte unstrukturierte Daten), sind von den jeweiligen Hauptabteilungsleitern Regelungen zu treffen, die die geforderte Löschung personenbezogener Daten organisatorisch sicherstellen (z. B. Aufbewahrung in nach Jahren sortierten Ordnern und löschen dieser Ordner bei Ablauf der Aufbewahrungsfrist). Zuständig sind der

⁹⁵ Vgl. Art. 39 Abs. 1 lit b DSGVO.

⁹⁶ Vgl. Art. 5 Abs. 1 lit. e DSGVO sowie Art. 17 Abs. 1 lit. a bis lit. f DSGVO.

⁹⁷ Vgl. bspw. DIN 66399.

Datenschutz-Koordinator des Bereiches und - sofern dieser nicht benannt sein sollte - der jeweilige Hauptabteilungsleiter.

Der *Prozesseigentümer* und der *Asset-Eigentümer* **müssen** je Verarbeitungstätigkeit ein Lösch- und Sperrkonzept erstellen, aus welchem strukturiert hervorgeht, wie und wann personenbezogene Daten gelöscht werden.⁹⁸

Hierzu **müssen** u. a. für jede Kategorie betroffener Personen und personenbezogener Daten die Aufbewahrungszeiträume, Löschfristen und Auslöser von Löschungen ermittelt und dokumentiert werden. Löschfristen können sich neben der jeweiligen Zweckerreichung u. a. aus gesetzlichen Aufbewahrungspflichten (z. B. aus dem Handels- und Steuerrecht) oder aus berechtigten Aufbewahrungsgründen (z. B. Abwehr, Geltendmachung und Durchsetzung von Rechtsansprüchen) ergeben.

Die Löschpflicht bezieht sich auch auf technische Protokollverfahren mit Eingabekontrolldaten zu personenbezogenen Daten. Hier sind grundsätzlich Aufbewahrungsfristen vorzusehen, die den Zweck der Eingabekontrollen berücksichtigen.

Betroffene Dokumente müssen einer geeigneten sicheren Vernichtung zugeführt werden. Für informationstechnische Datenträger erfordert dies den Einsatz spezieller Löschmodules oder die geeignete physische Zerstörung des Datenträgers. Vorgaben für die Vernichtung von Dokumenten und Datenträgern sind nach Stand der Technik durch die *Informationssicherheit* bereitzustellen. Entsprechend geeignete Verfahren sind seitens *Informationssicherheit* zu regeln. In Zweifelsfällen ist die Informationssicherheit, die Data Privacy Organization oder der zuständige Datenschutzbeauftragte zu kontaktieren.

4.8.3 Ausnahmen von der Löschpflicht

In bestimmten Fällen kann eine Löschung trotz Löschgründen ausnahmsweise unterbleiben, z. B. wenn die Verarbeitung zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist.⁹⁹ Dies gilt insbesondere für steuer- oder handelsrechtliche Aufbewahrungspflichten.¹⁰⁰ In den vorgenannten Fällen sind die Daten für die weitere Verarbeitung einzuschränken (zu sperren) und nach Abschluss der Aufbewahrungspflicht zu löschen.

Sofern die Löschpflicht entfallen soll, **muss** der zuständige *Prozess- oder Asset-Eigentümer* Rücksprache mit dem zuständigen *Data Privacy Officer* oder Datenschutzbeauftragten halten.

Der Sachverhalt ist zu begründen sowie zu dokumentieren. Entsprechende Risiken sind durch die Data Privacy Organization im Verzeichnis von Verarbeitungstätigkeiten zu dokumentieren.

Bei resultierenden hohen Risiken **muss** durch den *Prozess- oder Asset-Eigentümer* eine Risikoübernahme durch die zuständige *Geschäftsführung* herbeigeführt werden.

4.8.4 Sperrung von Daten

Die Verarbeitung muss eingeschränkt werden, wenn eine Speicherung, jedoch nicht mehr die weitere Verarbeitung zulässig ist.¹⁰¹ In diesem Fall werden die Daten in einer Art und Weise markiert, dass ihre künftige Verarbeitung nur in begründeten Ausnahmefällen möglich ist.

Dies kann beispielsweise über folgende Methoden stattfinden:¹⁰²

- Daten werden vorübergehend auf ein anderes Verarbeitungssystem übertragen,
- Daten werden für Nutzer gesperrt,
- veröffentlichte Daten werden vorübergehend von einer Website entfernt.

In automatisierten Dateisystemen (Assets) soll die Einschränkung der Verarbeitung grundsätzlich durch technische Mittel erfolgen, sodass die Daten nicht weiterverarbeitet oder verändert werden können. Im System wird wirksam darauf hingewiesen, dass die Verarbeitung eingeschränkt wurde.

⁹⁸ Vgl. DIN 66398 „Leitlinie zur Entwicklung eines Löschkonzepts mit Ableitung von Löschfristen für personenbezogene Daten“.

⁹⁹ Vgl. Art. 17 Abs. 3 lit. a bis lit. e DSGVO sowie § 35 BDSG.

¹⁰⁰ Vgl. bspw. § 147 der Abgabenordnung und § 257 des Handelsgesetzbuchs.

¹⁰¹ Vgl. Art. 5 Abs. 1 lit. c und e DSGVO.

¹⁰² Vgl. EG 67 DSGVO.

In diesem Fall muss auch durch geeignete technischen Maßnahmen sichergestellt werden, dass eine Verarbeitung der eingeschränkten Daten nur noch in bestimmten Ausnahmefällen erfolgt.¹⁰³ Dies kann z.B. durch restriktive Berechtigungen umgesetzt werden.

Im Zeitraum der Einschränkung der Verarbeitung ist, mit Ausnahme der Speicherung, die Verarbeitung nur ausnahmsweise in bestimmten Fällen erlaubt, beispielsweise

- mit ausdrücklicher Einwilligung der betroffenen Person,
- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen oder

zum Schutz der Rechte einer anderen natürlichen oder juristischen Person oder aus Gründen eines wichtigen öffentlichen Interesses.

4.8.5 Anonymisierung von Daten

Eine Speicherung der Daten in einer Form, durch die eine Identifizierung der betroffenen Person möglich ist, darf nur solange erfolgen, wie es für den Zweck der Verarbeitung erforderlich ist. Statt einer erforderlichen Löschung kann auch eine Anonymisierung der Daten erfolgen, die einer Löschung gleichkommt. An eine Anonymisierung sind jedoch strenge Anforderungen geknüpft.

Für eine datenschutzkonforme Anonymisierung muss gewährleistet werden, dass anhand der anonymisierten Daten keinerlei Rückschlüsse mehr auf die Identität der betroffenen Personen möglich sind. Die Anonymisierung geht daher über die bloße Pseudonymisierung hinaus.

Sofern eine Anonymisierung der Daten beabsichtigt wird, **muss** durch den *Prozesseigentümer oder Asset-Eigentümer* Rücksprache mit dem zuständigen *Datenschutzbeauftragten* oder der *Data Privacy Organization* gehalten werden.

4.8.6 Berichtigung von Daten

Sind die Daten zwar unrichtig, aber für den Verarbeitungszweck nach wie vor erforderlich, müssen sie berichtigt werden. Die Daten sind unrichtig, wenn sie mit der Tatsachenlage nicht übereinstimmen oder sich nicht auf dem neuesten Stand befinden.¹⁰⁴ Eine Berichtigung erfolgt durch eine Veränderung der betreffenden Daten. Beispielsweise wird die falsche Rechtschreibung des Namens verbessert oder der Familienname durch eine Heirat geändert.

Der *Prozess- und Asset-Eigentümer* **müssen** Verfahren und Prozessschritte zur Berichtigung falscher Daten vorsehen.

4.8.7 Dokumentation

In dem genutzten Dokumentations- oder Archivsystem müssen insbesondere die vorgenommene Art und Weise der Löschung sowie die getroffenen Maßnahmen zur Information Dritter über ein etwaiges Lösungsverlangen dokumentiert werden.

Für jede Verarbeitungstätigkeit muss ein Lösch- und Sperrkonzept erstellt und dokumentiert werden. In bestimmten Fällen kann ein Lösch- und Sperrkonzept auch für mehrere Verarbeitungstätigkeiten gelten.

Werden die Daten hingegen berichtigt, sind der Inhalt und Umstand der Erfüllung der Berichtigungspflicht zu dokumentieren. Konkret muss hierzu insbesondere dokumentiert werden, welche personenbezogenen Daten berichtigt wurden.

Die Dokumentation ist **3 Jahre** aufzubewahren.

¹⁰³ Vgl. Ziffer 7.6.2.2.

¹⁰⁴ Vgl. Art. 5 Abs. 1 lit. d DSGVO.

4.8.8 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none"> ▪ Stellt sicher, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden. ▪ Stellt die für seine Verarbeitung erforderlichen Aufbewahrungsfristen fest, dokumentiert diese in einem Löschkonzept zur Verarbeitungsbeschreibung und stellt die technische Möglichkeit der Berichtigung und Löschung bezogen auf seine Verarbeitung sicher. ▪ Erstellt geeignete Löscho- und Sperrkonzepte (schriftlich) auf Basis der Muster. ▪ Sieht Verfahren und Prozessschritte zur Berichtigung falscher Daten vor. ▪ Führt bei resultierenden hohen Risiken eine Risikoübernahme durch die zuständige Geschäftsführung herbei. ▪ Prüft regelmäßig (alle zwei Jahre und bei Änderungen an der Datenverarbeitung), ob geeignete technische oder organisatorische Maßnahmen zur Erfüllung der Löschungs- und Berichtigungspflicht getroffen wurden, durch die eine Löschung oder Berichtigung in geeigneter Form erfolgen kann.
Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Stellt sicher, dass die personenbezogenen Daten nicht länger als nötig gespeichert werden. ▪ Sieht Verfahren und Prozessschritte zur Berichtigung falscher Daten vor. ▪ Führt bei resultierenden hohen Risiken eine Risikoübernahme durch die zuständige Geschäftsführung herbei. ▪ Erstellt geeignete Löscho- und Sperrkonzepte (schriftlich) auf Basis der Muster.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Stellt allgemeine Empfehlungen für Fristen zur Löschung personenbezogener Daten (Aufbewahrungsfrist) zur Verfügung. ▪ Stellt Muster für Löscho- und Sperrkonzepte bereit.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Gibt geeignete Verfahren zur sicheren Löschung und Sperrung von Daten vor.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist hierzu überwachend und beratend tätig.¹⁰⁵

4.9 „Privacy by Design“ und „Privacy by Default“

4.9.1 Datenschutzfreundliche Technikgestaltung („Privacy by Design“)

4.9.1.1 Einleitung

Jede Verarbeitung von personenbezogenen Daten muss angemessen technisch und organisatorisch abgesichert sein. Es müssen daher stets geeignete technische und organisatorische Maßnahmen (TOM) getroffen werden, die darauf ausgerichtet sind, die Datenschutzgrundsätze umzusetzen und die notwendigen Garantien in die Verarbeitung aufzunehmen, um den Anforderungen der DSGVO sowie der Datenschutz-Leitlinie zu genügen und die Rechte der betroffenen Personen zu schützen.¹⁰⁶

Unternehmen sind angehalten, zum frühestmöglichen Zeitpunkt der Gestaltung der Verarbeitungstätigkeiten (inkl. Auswahl der Mittel wie z. B. IT-Systeme/-Anwendungen) technische und organisatorische Maßnahmen zu treffen, die darauf ausgelegt sind, die Privatsphäre der von der Datenverarbeitung betroffenen Personen zu schützen und Datenschutzgrundsätze von Beginn an zu garantieren („Datenschutz durch Technikgestaltung“ bzw. „Privacy by Design“). Solche Maßnahmen können u. a. darin bestehen, dass die Verarbeitung personenbezogener Daten minimiert wird, personenbezogene Daten so schnell wie möglich pseudonymisiert werden, eine starke Verschlüsselung der Daten implementiert wird, Transparenz in Bezug auf die Funktionen und die Verarbeitung personenbezogener Daten hergestellt wird, der betroffenen Person ermöglicht wird, die Verarbeitung

¹⁰⁵ Vgl. Art. 39 Abs. 1 lit b DSGVO.

¹⁰⁶ Vgl. Art. 25 Abs. 1 DSGVO.

personenbezogener Daten zu überwachen, und der Verantwortliche in die Lage versetzt wird, Sicherheitsfunktionen zu schaffen und zu verbessern.

4.9.1.2 Beschreibung

Es müssen geeignete technische und organisatorische Maßnahmen zur Gewährleistung des Datenschutzes durch Technikgestaltung getroffen werden. Im Rahmen der Beschaffung müssen Produkte und Anwendungen (Assets) ausgewählt werden, die eine möglichst datenschutzfreundliche Verarbeitung ermöglichen. Diese Produkte und Anwendung sind nach der Anschaffung entsprechend zu verwenden.¹⁰⁷ Die technischen und organisatorischen Maßnahmen müssen dabei so ausgerichtet sein, dass die Einhaltung von Datenschutzgrundsätzen bei der Verarbeitung gewährleistet wird. Datenschutzgrundsätze sind beispielsweise die Datenminimierung oder die Einhaltung der Zweckbindung. Geeignete Maßnahme sind beispielsweise die Pseudonymisierung oder Verschlüsselung der Daten sowie regelmäßige Schulungen der Beschäftigten.¹⁰⁸

Der Prozess- und Asset-Eigentümer **müssen** bei Beschaffung von Assets, Einkauf von Leistungen oder Gestaltung von Prozessen sicherstellen, dass die nachfolgend genannten Vorgaben zu „Privacy by Design“ berücksichtigt werden.

4.9.1.3 Dokumentation

Die getroffenen technischen und organisatorischen Maßnahmen sind zu dokumentieren. Hierzu dienen insbesondere die Verarbeitungsbeschreibung und die Asset-Beschreibung (siehe Ziffer 5).

Konkret muss hierzu zunächst die durchgeführte Risikobewertung (vgl. Ziffer 4.10) dokumentiert werden. Dies kann beispielsweise im Rahmen des Informationssicherheitsmanagementsystems (ISMS) oder eines IT-Sicherheitskonzeptes erfolgen.

4.9.1.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer & Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Stellt sicher, dass bezogen auf die Verarbeitungstätigkeit und auf das Asset geeignete und angemessene technische und organisatorische Sicherheitsmaßnahmen ausgewählt und umgesetzt werden. ▪ Prüft regelmäßig (ggf. mit Unterstützung der Informationssicherheit und die IT-Sicherheit), ob geeignete technische und organisatorische Maßnahmen getroffen wurden und ob sich diese auf dem Stand der Technik befinden. ▪ Berücksichtigt im Rahmen des Beschaffungsprozesses, dass die zu beschaffenden Lösungen (z. B. Cloud, Geräte oder Software) die Datenschutzgrundsätze und datenschutzrechtlichen Anforderungen erfüllen.
Einkauf & IT-Abteilung (IT-Contract / Vendor Management, IT-License Management, IT-Demand Management)	<ul style="list-style-type: none"> ▪ Stellt sicher, dass Vorgaben der Informationssicherheit und des Datenschutzes („Privacy by Design“) berücksichtigt werden.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Ist beratend und überwachend tätig.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Ist beratend und überwachend tätig. ▪ Prüft laufend und regelmäßig, ob die bei Rheinmetall eingesetzten technischen und organisatorischen Sicherheitsmaßnahmen dem Stand der Technik entsprechen und geeignet sind, Schäden für betroffene Personen und Rheinmetall zu verhindern. ▪ Dokumentiert die technischen und organisatorischen Sicherheitsmaßnahmen in einem Maßnahmenkatalog.

¹⁰⁷ Vgl. Art. 25 Abs. 1 DSGVO.

¹⁰⁸ Vgl. Art. 25 Abs. 1 DSGVO, Datenschutzgrundsätze sind in Art. 5 Abs. 1 DSGVO verankert.

Rolle	Verantwortung
	<ul style="list-style-type: none"> ▪ Prüft den Maßnahmenkatalog in Hinblick auf den aktuellen Stand der Technik und den aktuellen Gegebenheiten und passt diesen erforderlichenfalls an (Die Überprüfung erfolgt regelmäßig (mindestens jährlich) und wenn neue Techniken, Verarbeitungstätigkeiten, Sicherheitslücken oder Assets bekannt werden).
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Unterstützt bei Anfragen des Prozesseigentümers. ▪ Ist hierzu überwachend und beratend tätig.

4.9.2 Datenschutzfreundliche Voreinstellung („Privacy by Default“)

4.9.2.1 Einleitung

Es ist sicherzustellen, dass Verarbeitungstätigkeiten und Assets durch geeignete technische und organisatorische Maßnahmen so voreingestellt werden, dass nur personenbezogene Daten verarbeitet werden, die für den Zweck der Verarbeitung tatsächlich erforderlich sind.¹⁰⁹ Diese Verpflichtung gilt für die Menge der erhobenen personenbezogenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit.

Durch datenschutzfreundliche Voreinstellung sollen Unternehmen sicherstellen, dass personenbezogene Daten mit dem größtmöglichen Datenschutz (z. B. Datenminimierung, kurze Speicherfristen und begrenzte Zugänglichkeit) verarbeitet werden („datenschutzfreundliche Voreinstellungen“ bzw. „Privacy by Default“).

4.9.2.2 Beschreibung

Der Prozess ist vor einer beabsichtigten Verarbeitung von personenbezogener Daten durchzuführen. Alle Verarbeitungen müssen vor ihrer ersten Aufnahme datenschutzfreundlich voreingestellt sein. Standardmäßig dürfen nur so viele Daten erfasst, verarbeitet und weitergegeben werden, wie für die Nutzung unbedingt erforderlich sind. Konkrete Beispiele sind:

- Ein Opt-Out ist bei Einwilligungssachverhalten nicht mehr möglich, Verarbeitungen sind durchgängig auf Opt-In umzustellen. Dies bedeutet, dass betroffene Personen ausdrücklich im Vorfeld aktiv einwilligen müssen (z. B. durch aktives Setzen eines Häkchens, aktives Anklicken eines Knopfes);
- Bei Verarbeitungen auf Webseiten sind die Browservoreinstellungen „do-not-track“ zu berücksichtigen. Dies bedeutet, dass keine Tracking-Cookies bzw. –Tools zum Einsatz kommen dürfen, wenn der Browser des Webseitenbesuchers diese Voreinstellung aktiviert hat;
- Bei Kontaktformularen oder Fragebögen sollten die Pflichtfelder auf das erforderliche Minimum reduziert werden;
- Aufbewahrungszeiträume von Daten/Dokumenten sollten bzw. müssen auf das erforderliche Maß beschränkt werden (hierbei sind gesetzliche und betriebliche Aufbewahrungsfristen zu berücksichtigen).

Personenbezogene Daten werden durch Voreinstellung automatisch geschützt, d. h., selbst wenn eine Person nichts unternimmt, muss der Datenschutz maximal und die Menge der verarbeiteten Daten minimal sein.

Basierend auf dem Zweck der Verarbeitung sind geeignete technische und organisatorische Maßnahmen zu bestimmen. Die Maßnahmen sind so auszuwählen, dass folgende Prinzipien eingehalten werden:

- Es werden nur solche und nur so viele personenbezogene Daten erhoben, die für den jeweiligen Zweck tatsächlich erforderlich sind (**Datenminimierung – Menge der Daten**),
- die Daten werden nur in einer Weise verarbeitet, die für den jeweiligen Zweck tatsächlich erforderlich ist (**Umfang der Verarbeitung**),
- die Daten werden nur denjenigen Personen zugänglich gemacht, die für den Verarbeitungszweck zwingend Kenntnis von den Daten nehmen müssen (**need-to-know / need-to-use - Zugänglichkeit**),
- die Daten werden nur so lange gespeichert, wie es für den jeweiligen Zweck erforderlich ist und so schnell wie möglich gelöscht oder anonymisiert (Speicherbegrenzung - Speicherfrist),
- ein Zugänglichmachen der Daten an einen unbestimmten Personenkreis darf nur durch ein ausdrückliches Eingreifen der betroffenen Person möglich sein.¹¹⁰

¹⁰⁹ Vgl. Art. 25 Abs. 2 DSGVO.

¹¹⁰ Vgl. Art. 25 Abs. 2 DSGVO.

Das wesentliche Ziel dieser Anforderung besteht darin, die personenbezogenen Daten auf das Mindestmaß zu reduzieren. Dies gilt insbesondere für unübersichtliche Verarbeitungssituationen (z. B. Portale, Apps oder soziale Netzwerke), bei denen mitunter viele persönliche Informationen, teils ohne vollständiges Bewusstsein der Nutzer, allen anderen Nutzern oder sogar weiteren Dritten zugänglich gemacht werden. Hier ist insbesondere der Maßnahmenkatalog zu den technischen und organisatorischen Maßnahmen zu berücksichtigen (siehe Ziffer 4.11).

4.9.2.3 Dokumentation

Die getroffenen technischen und organisatorischen Maßnahmen sind zu dokumentieren. Hierzu dienen insbesondere die Verarbeitungsbeschreibung und die Asset-Beschreibung (siehe Ziffer 5).

Konkret muss hierzu zunächst die durchgeführte Risikobewertung (vgl. hierzu Ziffer 4.10) dokumentiert werden. Dies kann beispielsweise im Rahmen des Informationssicherheitsmanagementsystems (ISMS) oder eines IT-Sicherheitskonzeptes erfolgen.

4.9.2.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none"> ▪ Beachtet bei der Auswahl und der Gestaltung von Verarbeitungstätigkeiten die Vorgaben zu „Privacy by Design“ und „Privacy by Default“. ▪ Prüft regelmäßig, ob geeignete technische und organisatorische Maßnahmen umgesetzt wurden, die sicherstellen, dass durch Voreinstellungen nur solche personenbezogenen Daten verarbeitet werden, die für den Zweck der Verarbeitung tatsächlich erforderlich sind. ▪ Prüft, ob diese Maßnahmen vor Verarbeitung der Daten implementiert sind. ▪ Prüft regelmäßig (mindestens jährlich), ob Rollen und vergebene Berechtigungen noch erforderlich oder aktuell sind. ▪ Führt regelmäßig alle zwei Jahre Kontrollen bezogen auf seine Verarbeitungen durch und dokumentiert diese.
Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Beachtet bei der Auswahl und der Gestaltung von Assets die Vorgaben zu „Privacy by Design“ und „Privacy by Default“. ▪ Führt regelmäßig alle zwei Jahre Kontrollen bezogen auf seine Assets durch und dokumentiert diese.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Unterstützt bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Unterstützt bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Beachtet bei der Erstellung und Pflege des Maßnahmenkatalogs sowie bei der Überprüfung der technischen und organisatorischen Maßnahmen die Prinzipien zu „Privacy by Design“ und „Privacy by Default“.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist hierzu überwachend und beratend tätig.¹¹¹

4.10 Risiko im Datenschutz

4.10.1 Einleitung

Um ein dem Risiko angemessenes Schutzniveau zu gewährleisten, treffen der Verantwortliche und der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen unter Berücksichtigung der folgenden Aspekte¹¹²:

- Stand der Technik
- Implementierungskosten
- Art

¹¹¹ Vgl. Art. 39 Abs. 1 lit b DSGVO.

¹¹² Vgl. u. a. Art. 24 Abs. 1 DSGVO, Art. 32 Abs. 1 DSGVO.

- Umfang
- Umstände der Verarbeitung
- Zwecke der Verarbeitung
- Unterschiedliche Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen

Die Risiken im Bereich des Datenschutzes beziehen sich auf natürliche Personen und auf den Verantwortlichen selbst. Um eine saubere Abgrenzung zu gewährleisten, wird vorliegend zwischen Datenschutzrisiken aus Sicht der betroffenen Personen und datenschutzbezogenen Compliance Risiken aus Sicht des Verantwortlichen (d. h. jedes Unternehmens im Rheinmetall Konzern, welches mit personenbezogenen Daten umgeht) unterschieden.

Bei Datenschutzrisiken handelt es sich um Risiken für die Rechte und Freiheiten natürlicher Personen, die mit der Verarbeitung ihrer personenbezogenen Daten verbunden sind und insbesondere bei einer Datenschutzverletzung bzw. Datenpanne realisiert werden können. Sie resultieren somit aus einer Datenverarbeitung und können zu einem physischen, materiellen oder immateriellen Schaden (beispielsweise Diskriminierung, Identitätsdiebstahl) führen. Ein Datenschutzrisiko ist somit die Auswirkung von Unsicherheiten (z.B. Sicherheitslücken in Systemen, unrechtmäßige Offenbarung von Daten) speziell auf die Rechte und Freiheiten von natürlichen Personen.¹¹³

Datenschutzbezogene Compliance Risiken (Datenschutz Compliance Risiken) resultieren aus der Nichteinhaltung bzw. einer unzureichenden Einhaltung datenschutzrechtlicher Vorschriften. Mögliche Schäden derartiger Compliance-Risiken für die Unternehmen im Rheinmetall Konzern können u. a. Bußgelder¹¹⁴, Schadensersatzansprüche betroffener Personen, aber auch Image-Schäden bei Kunden, Beschäftigten und Partnern sowie andere immaterielle und finanzielle Verluste sein.

In diesem Abschnitt werden ausschließlich die Ermittlung der Datenschutzrisiken (für betroffene Personen) sowie mögliche Methoden für die Zuordnung risikoadäquater Maßnahmen (Maßnahmen zur Behandlung dieser Datenschutzrisiken) beschrieben.

Risikoabhängige Behandlung von Datenverarbeitungen und Datenschutzverletzungen

	Kein oder geringes Risiko*	Normales oder mittleres Risiko*	Hohes oder sehr hohes Risiko*
Datenverarbeitung	Risikoadäquate technische und organisatorische Maßnahmen (TOMs)	Risikoadäquate TOMs	Risikoadäquate TOMs DSFA Ggf. Konsultation mit Behörde
Datenschutzverletzung	Dokumentation	Dokumentation + Meldung bei zuständiger Datenschutz-Aufsichtsbehörde	Dokumentation + Meldung bei zuständiger Datenschutz-Aufsichtsbehörde + Benachrichtigung der Betroffenen

* Wahrscheinliches Risiko für die durch die Datenverarbeitung oder Datenschutzverletzung betroffene Person

Datenschutz Compliance Risiken sind im Rahmen der Ermittlung der allgemeinen Compliance Risiken zu berücksichtigen. Dazu wird das Datenschutz Compliance Risiko bezogen auf den Fachbereich ermittelt. Ausgangspunkt sind die einzelnen durch den Fachbereich vorgenommenen Verarbeitungen.

4.10.2 Beschreibung

Das Datenschutzrisiko ist bezogen auf jede Verarbeitung bzw. Verarbeitungsbeschreibung in Verbindungen mit den genutzten Assets zu ermitteln. Nur so können je Verarbeitung und Asset risikoadäquate Datensicherheitsmaßnahmen zugewiesen werden. Ausgangspunkt der Risikoermittlung ist also zunächst eine möglichst vollständige Beschreibung der Verarbeitungstätigkeit und des Assets.

Ein Datenschutzrisiko ist vereinfacht ein hypothetisches Szenario, welches beschreibt,

- welche **Schäden** potentiell

¹¹³ Vgl. „effect of uncertainty on privacy“, ISO 29100, Privacy framework, 2011, S. 3.

¹¹⁴ Vgl. Art. 83 DSGVO.

- durch welche **Ereignisse**,
- ausgelöst durch welche Handlungen und Umstände,
- für die von der Verarbeitung **betroffenen Personen** (z. B. Beschäftigter, Kunden)
- unter Berücksichtigung der **zu verarbeitenden Daten** (z. B. Kontaktdaten, Gehaltsdaten) und
- **Art und Umfang** der Verarbeitung (z. B. IT-Monitoring, Erstellung von Nutzerprofilen Videoüberwachung) eintreten können.

Zur Identifizierung von etwaigen Datenschutzrisiken müssen potenzielle

- **Schäden** (negative **Auswirkungen** für die betroffenen Personen)
- **Ereignisse** (Auslöser der Schäden) bzw. **Risikoquellen**
- **Ursachen** (Handlungen und Umstände, die zum schadensauslösenden Ereignis führen) bzw. **Bedrohungen** und **Schwachstellen**

in Beziehung zu Art und Umfang der Datenverarbeitung bestimmt und in einem Risikokatalog dokumentiert werden.

Grundsätzlich lassen sich die Anforderungen der DSGVO bezogen auf die Risikobetrachtung einer Verarbeitung in drei Datenschutzziele abbilden:

- Verfügbarkeit,
- Vertraulichkeit,
- Integrität.¹¹⁵

Um eine Übereinstimmung mit den Schutzziele der Informationssicherheit zu erhalten, wird das durch die DSGVO adressierte Schutzziel der Belastbarkeit (z. B. Standhalten eines Systems bei einer gewissen Beanspruchung, Widerstandsfähigkeit eines Systems) unter dem Schutzziel Verfügbarkeit behandelt.

Im Rahmen der Ermittlung des Datenschutzrisikos muss zunächst betrachtet werden, welche Risiken eine Verletzung der vorgenannten Datenschutzziele für die betroffenen Personen nach sich ziehen können. Hierzu ist ein Risikokatalog zu führen. Im Risikokatalog sind die Datenschutzrisiken zu dokumentieren. Der Risikokatalog soll nach Möglichkeit alle potentiellen Datenschutzrisiken enthalten.

Um ein dem Risiko einer Verarbeitung angemessenes Schutzniveau zu gewährleisten, werden insbesondere die Risiken beurteilt, die mit der Verarbeitung personenbezogener Daten verbunden sind. Hierbei handelt es sich v. a. um Risiken durch – ob unbeabsichtigt oder unrechtmäßig – Vernichtung, Verlust, Veränderung oder unbefugte Offenlegung von bzw. unbefugten Zugang zu personenbezogenen Daten, die übermittelt, gespeichert oder auf andere Weise verarbeitet wurden.¹¹⁶

Die Beurteilung der Risiken einer Verarbeitung erfolgt toolgestützt und mithilfe von Arbeitshilfen. Ein Ergebnis der Beurteilung ist die Entscheidung, ob für die Verarbeitung oder Auftragsverarbeitung eine Datenschutzfolgenabschätzung (Ziffer 4.10) vorgenommen werden muss. Eine solche durchgeführte datenschutzrelevante Risikobetrachtung wird als Bestandteil des Verzeichnisses der jeweiligen Verarbeitungen dokumentiert.

Die Data Privacy Organization ermittelt auf Basis der von Prozess- und Asset-Eigentümer dokumentierten Verarbeitungstätigkeit einen Vorschlag für das zugrundeliegende Datenschutzrisiko.

Prozess- und Asset-Eigentümer prüfen die Bewertung des Datenschutzrisikos und übernehmen diese Bewertung bei Akzeptanz in ihre Verarbeitungsbeschreibung.

Die Data Privacy Organization ermittelt anschließend auf Basis der Angaben und des Datenschutzrisikos das Datenschutz Compliance Risiko. Die Data Privacy Organization teilt das Ergebnis dem Prozess- und Asset-Eigentümer mit und dokumentiert das aus einer Verarbeitungstätigkeit resultierende Datenschutz Compliance Risiko (siehe Ziffer 5.3.2.4).

Bei resultierenden hohen Risiken **müssen** der *Prozess- und Asset-Eigentümer* eine Risikoübernahme durch die zuständige *Geschäftsführung* herbeiführen.

¹¹⁵ Vgl. Art. 32 Abs. 1 lit. b DSGVO.

¹¹⁶ Vgl. Art. 32 Abs. 2 DSGVO.

4.10.3 Risikoidentifikation

Zunächst müssen mögliche Risikoszenarien und die daraus resultierenden potenziellen Folgen identifiziert und dokumentiert werden.

Dazu sind ausgehend von den Risikoquellen (interne und externe Personen, nicht-menschliche Quellen) potentielle Schäden und mögliche Ereignisse (z. B. Änderung, Verlust, Beschädigung, Missbrauch) zu berücksichtigen, die sich auf Handlungen und Umstände im Zusammenhang mit der Verarbeitung von personenbezogenen Daten beziehen. Dies ist im Datenschutz-Risikokatalog zu dokumentieren.

Mögliche interne und externe menschliche Quellen können sein:

- Beschäftigte,
- Empfänger personenbezogener Daten,
- berechtigte Dritte (z. B. Gerichte oder BaFin),
- Dienstleister,
- Hacker,
- Besucher,
- ehemalige Beschäftigte,
- Aktivisten,
- Konkurrenten,
- Kunden,
- Wartungspersonal,
- Gewerkschaften,
- Journalisten,
- Nichtregierungsorganisationen,
- kriminelle Organisationen,
- Organisationen unter der Kontrolle eines fremden Staates,
- terroristische Organisationen.

Mögliche nicht-menschliche Quellen können sein:

- Bösartiger Code unbekannter Herkunft (Viren, Würmer usw.),
- Wasser (Rohrleitungen, Wasserwege usw.),
- brennbare, ätzende oder explosive Stoffe,
- Naturkatastrophen,
- Epidemien,
- Tiere.

Schadensauslösende Ereignisse/Umstände können durch unbeabsichtigtes oder vorsätzliches Handeln von Menschen (intern/extern) oder durch nicht-menschliche Ursachen (z. B. Naturkatastrophen, technische Defekte) entstehen.

Wenn die relevanten Risikoquellen identifiziert wurden, sind die unterstützenden Systeme/Werte (Assets) zu ermitteln. Assets können insbesondere sein:

- Hardware und Datenmedien (Personal-Computer, Server, Switches, Router, USB-Laufwerke, Festplatten, Smartphones, etc.)
- Software (Betriebssysteme, Messaging-Software (u. a. MS Exchange, Skype), Datenbanken, Anwendungssoftware, etc.)
- Kommunikationskanäle (Kabel, WiFi, Glasfaser, etc.)
- Papierdokumente (Ausdrucke, Fotokopien, handgeschriebene Dokumente)
- Übertragungswege für Papierdokumente (Post, Workflow (Prozess), etc.)

Zu berücksichtigen ist, dass die Sicherheitslösungen (z. B. Firewall, Virens Scanner) in diesem Kontext keine unterstützenden Assets der Verarbeitung personenbezogener Daten, sondern Maßnahmen zur Risikobehandlung darstellen. Dies bedeutet jedoch nicht, dass zentrale Sicherheitsverfahren und -systeme nicht als eigenständige Assets und Verarbeitungen zu dokumentieren sind.

Auf Assets können u. a. die folgenden Ereignisse wirken:

- Fehlverhalten/-funktion,
- Beschädigung,
- Spionage,
- Verlust,
- Veränderung,
- Überlastung,
- Unangemessener Gebrauch,
- Überwachung,
- Manipulation.

Die *Data Privacy Organization* **muss** für die identifizierten Bedrohungen die möglichen negativen - befürchteten - Ereignisse bzw. Schäden initial ermitteln. Die Ergebnisse werden im Datenschutz-Risikokatalog dokumentiert.

4.10.4 Risikobewertung

Die Risiken sind hinsichtlich der Schwere des Schadens und der Eintrittswahrscheinlichkeit zu bewerten. Sowohl die Schwere des Schadens als auch die Eintrittswahrscheinlichkeit wird in vier Kategorien unterteilt.¹¹⁷ Die Gesamtbewertung des Risikos ergibt sich aus einer fallbezogenen Gewichtung der Schwere der Schadensauswirkung und der Höhe der Eintrittswahrscheinlichkeit (vgl. Ziffer 4.10.5).

4.10.4.1 Datenschutzziele

Die Auswirkungen von Bedrohungen auf die folgenden drei Schutzziele durch bestimmte Ereignisse bzw. Szenarien müssen im Rahmen der Risikobewertung genauer betrachtet werden:

- Vertraulichkeit (z. B. illegaler Zugriff auf personenbezogene Daten),
- Integrität (z. B. unerlaubte oder ungewollte Modifikation von personenbezogenen Daten),
- Verfügbarkeit (z. B. Verlust von personenbezogenen Daten).

Um eine Übereinstimmung mit den Schutzzielen der Informationssicherheit zu erhalten, wird das durch die DSGVO adressierte Schutzziel der Belastbarkeit (z. B. Standhalten eines Systems bei einer gewissen Beanspruchung, Widerstandsfähigkeit eines Systems) unter dem Schutzziel Verfügbarkeit behandelt.

4.10.4.2 Schadensauswirkung und Schadensschwere

Die DSGVO macht keine konkreten Vorgaben zur Bewertung von Risiken bzw. Schäden, geht aber mindestens von zwei Risikograden aus: (normales) Risiko und hohes Risiko.¹¹⁸ Zudem bietet sich die Aufteilung nach einer

- physischen,
- materiellen und
- immateriellen

Schadensauswirkung an.¹¹⁹ Die Schwere der Auswirkungen bzw. des Schadens bei der Realisierung eines Risikos wird in Anlehnung an das Informationssicherheitsmanagementsystem (ISMS) in vier Risiko-Niveaus unterteilt:

- gering,
- mittel (normal),
- hoch,
- sehr hoch.

¹¹⁷ Vgl. PIA der CNIL und ISO 29134.

¹¹⁸ Vgl. Art. 35 DSGVO.

¹¹⁹ Vgl. ErwGr. 75 DSGVO.

4.10.4.3 Eintrittswahrscheinlichkeit

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

Bei einer qualitativen Risikobeurteilung kann die Eintrittswahrscheinlichkeit ebenfalls in verschiedene Stufen unterteilt werden:

- unwahrscheinlich,
- möglich,
- wahrscheinlich,
- sehr wahrscheinlich.

4.10.5 Ermittlung des Datenschutzrisikos

Zur Ermittlung des Datenschutzrisikos werden geeignete Hilfsmittel zur Verfügung gestellt. Aus den Katalogen werden die für die Verarbeitung relevanten Schadensauswirkungen sowie Eintrittswahrscheinlichkeiten ausgewählt und nebst einer kurzen Begründung dokumentiert. Das Risiko bzw. der Risikograd wird durch die Kombination aus Eintrittswahrscheinlichkeit und Schwere/Auswirkung bestimmt. Dies lässt sich in einer Risikomatrix darstellen. Die einzelnen Felder der Risikomatrix gehören zu einem bestimmten Risikobereich, z. B. gering, mittel, hoch oder sehr hoch. Den Risikobereichen lassen sich unterschiedliche Maßnahmen aus einem Maßnahmenkatalog zuordnen (TOM). Wird ein hohes oder sehr hohes Risiko ermittelt, so ist zwingend eine Datenschutzfolgenabschätzung (DSFA) vorzunehmen¹²⁰ (vgl. Ziffer 4.12).

Wahrscheinlichkeit	Auswirkung / Schaden			
	öffentlich	intern	vertraulich	streng vertraulich
Sehr wahrscheinlich	MITTEL	HOCH	SEHR HOCH	SEHR HOCH
Wahrscheinlich	MITTEL	MITTEL	HOCH	SEHR HOCH
Möglich	GERING	MITTEL	MITTEL	HOCH
Unwahrscheinlich	GERING	GERING	MITTEL	MITTEL

Matrix zur Risikobewertung

Ein hohes Risiko liegt zudem auch vor, wenn mindestens zwei der nachfolgenden Fallgruppen auf die jeweilige Verarbeitung zutreffen:¹²¹

- Bewertung und Einstufung (Scoring), einschließlich Profiling oder Prognose von persönlichen Aspekten natürlicher Personen (insbesondere zur Analyse und Prognose von Aspekten bzgl. Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben oder Interessen, Zuverlässigkeit oder Verhalten, Aufenthaltsort oder Ortswechsel der betroffenen Person¹²²,
- Automatisierte Entscheidungsfindung, die rechtliche Wirkung für die betroffene Person entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt,
- Systematische Überwachung einschließlich der systematischen Überwachung öffentlich zugänglicher Bereiche an,

¹²⁰ Vgl. Art. 35 DSGVO.

¹²¹ Vgl. WP 248 der Artikel 29 Datenschutzgruppe.

¹²² Vgl. ErwGr. 71 und ErwGr. 91 DSGVO.

- Vertrauliche oder höchst persönliche Daten einschließlich der besonderen Kategorien personenbezogener Daten¹²³ sowie personenbezogene Daten über strafrechtliche Verurteilungen oder Straftaten¹²⁴,
- Datenverarbeitung in großem Umfang, die dazu dienen, große Mengen personenbezogener Daten auf regionaler, nationaler oder supranationaler Ebene (insbesondere außerhalb EU/EWR) zu verarbeiten, eine große Zahl von Personen betreffen und eine lange Dauer der Verarbeitung/Speicherung haben könnten¹²⁵,
- Abgleich oder Zusammenführung von Datenbanken, die zu unterschiedlichen Zwecken von unterschiedlichen verantwortlichen Stellen erhoben wurden, mit denen die betroffenen Personen nicht rechnen mussten¹²⁶,
- Datenverarbeitung personenbezogener Daten schutzbedürftiger natürlicher Personen¹²⁷, insbesondere Daten von Kindern¹²⁸,
- Verarbeitungsvorgänge unter innovativer Nutzung oder Anwendung neuer technologischer oder organisatorischer Lösungen und bei denen der Verantwortliche noch keine Datenschutzfolgenabschätzung (DSFA) durchgeführt hat, wie z. B. Kombination aus Fingerabdruck und Gesichtserkennung bei der Zutrittskontrolle¹²⁹ sowie
- Verarbeitungsvorgänge, bei denen den betroffenen Personen die Ausübung ihrer Rechte oder die Nutzung einer Dienstleistung bzw. Durchführung eines Vertrages erschwert wird¹³⁰.

Darüber hinaus liegt ein hohes Risiko auch dann vor, wenn mindestens einer der folgenden Fälle auf die Verarbeitung zutrifft¹³¹:

- systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen, die sich auf automatisierte Verarbeitung einschließlich Profiling gründet und die ihrerseits als Grundlage für Entscheidungen dient, die Rechtswirkung gegenüber natürlichen Personen entfalten oder diese in ähnlich erheblicher Weise beeinträchtigen;
- umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten gemäß Art. 9 Absatz 1 oder von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten gemäß Art. 10 DSGVO oder
- systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche.

Der Asset- und Prozesseigentümer **müssen** über die Etablierung geeigneter technischer und organisatorischer Maßnahmen erreichen, dass das Datenschutzrisiko für betroffene Personen auf ein geringes bis mittleres Maß gebracht wird.

4.10.6 Dokumentation

Die Beschreibung der potentiellen Schadensauswirkungen, der Schadensschwere und der Eintrittswahrscheinlichkeiten werden bezogen auf die unterschiedlichen Niveaus ebenfalls im Datenschutz-Risikokatalog dokumentiert.¹³²

Die Anforderungen an die Risikobewertung im Hinblick auf die Dokumentation ergeben sich aus den Darstellungen zu den einzelnen Prozessen.

¹²³ Vgl. Art. 9 DSGVO.

¹²⁴ Vgl. Art. 10 DSGVO.

¹²⁵ Vgl. ErwGr. 91 DSGVO.

¹²⁶ Vgl. WP29-Stellungnahme zur Zweckbindung: 13/EN WP 203, S. 24.

¹²⁷ Laut Europäischen Datenschutzausschuss sind Beschäftigte besonders schutzbedürftige Personen.

¹²⁸ Vgl. ErwGr. 75 DSGVO.

¹²⁹ Vgl. ErwGr. 89 und ErwGr. 91 DSGVO.

¹³⁰ Vgl. Art. 22 und ErwGr. 91 DSGVO.

¹³¹ Vgl. Art. 35 Abs. 3 DSGVO.

¹³² Siehe Arbeitshilfe „Beispiele/Hinweise für die Schadensauswirkung, Bedrohung und Eintrittswahrscheinlichkeit“.

4.10.7 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer & Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Ermittelt und dokumentiert den Schutzbedarf bezogen auf seine Verarbeitungstätigkeiten. ▪ Bestätigt bzw. korrigiert die initiale Risikobewertung durch die Data Privacy Organization (vgl. Ziffer 5.3.2.4). ▪ Führt bei resultierenden hohen Datenschutz Compliance Risiken eine Risikoübernahme durch die zuständige Geschäftsführung herbei.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Ermittelt die Datenschutzrisiken bezogen auf den Fachbereich. ▪ Meldet die datenschutzbezogenen Compliance Risiken an den zuständigen Risk Manager im Rahmen des Risikomanagement-Meldeprozesses.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Ermittelt und bewertet initial mit dem Prozesseigentümer das Datenschutzrisiko und den Schutzbedarf bezogen auf die Verarbeitung. ▪ Ermittelt auf Basis der Angaben und des Datenschutzrisikos das Datenschutz Compliance Risiko. Teilt das Ergebnis dem Prozess- und Asset-Eigentümer mit und dokumentiert das aus einer Verarbeitungstätigkeit resultierende Datenschutz Compliance Risiko. ▪ Dokumentiert das Ergebnis in der Verarbeitungsbeschreibung. ▪ Unterstützt bei Anfragen des Prozess- und Asset-Eigentümers. ▪ Führt und pflegt den Datenschutzrisiko-Katalog. ▪ Stimmt den Datenschutzrisiko-Katalog regelmäßig u. a. mit der Informationssicherheit, dem Datenschutzbeauftragten und der Revision ab. ▪ Ist unterstützend und beratend tätig. ▪ Stellt geeignete Hilfsmittel zur Überprüfung und Dokumentation zur Verfügung.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Unterstützt bei Anfragen des Prozesseigentümers.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Unterstützt bei Anfragen des Prozesseigentümers. ▪ Ist hierzu überwachend und beratend tätig.¹³³

4.11 Technische und organisatorische Maßnahmen (TOM)¹³⁴

4.11.1 Anforderungen an die Informationssicherheit und das ISMS

Das Unternehmen vertreten durch die Geschäftsführung **muss** die Vertraulichkeit, Integrität und Verfügbarkeit seiner Informationen auf Dauer sicherstellen (Informationssicherheitsprozess).

Der Informationssicherheitsprozess **muss** durch den *Leiter der Informationssicherheit* so gestaltet werden, dass die Anforderungen des Datenschutzes berücksichtigt und sämtliche IT-Systeme, mobilen Datenträger, Verbindungen und sonstige Assets abdeckt werden, mit denen auch personenbezogene Daten verarbeitet werden.

Der *Leiter der Informationssicherheit* **muss** ein angemessenes ISMS etablieren.

Personenbezogene Daten sind in diesem Kontext ebenfalls als zu schützende Informationen einzuordnen.

4.11.2 Maßnahmenkatalog technischer und organisatorischer Maßnahmen

4.11.2.1 Einleitung

Es ist sicherzustellen, dass durch die *Informationssicherheit* ein Maßnahmenkatalog geführt und zur Verfügung gestellt wird, in dem geeignete technische und organisatorische Maßnahmen (TOM) zur Sicherstellung der Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität abhängig vom Schutzbedarf bzw. dem Risiko und dem Stand der Technik beschrieben werden.

¹³³ Vgl. Art. 39 Abs. 1 lit b DSGVO.

¹³⁴ Bezogen auf die Daten-/Informationssicherheit.

Derzeit führt die *Informationssicherheit* hierzu die konzernweit geltende Richtlinie „Information Security Controls 3 - Anforderungen der Informationssicherheit“ (ISec 3).

Darüber hinaus ist durch die *Data Privacy Organization* ein Katalog von insbesondere organisatorischen Maßnahmen bereitzustellen, der alle datenschutzrechtlichen Sonderanforderungen abdeckt, die durch den Maßnahmenkatalog der *Informationssicherheit* nicht angemessen berücksichtigt werden können. Solchermaßen gear- tete Maßnahmen dienen insbesondere der Sicherstellung der Rechtmäßigkeit der Verarbeitung, der Verarbei- tung nach Treu und Glauben, der Transparenz und der Zweckbindung sowie der Herstellung eines angemessenen Datenschutzniveaus im Rahmen der Übermittlung in einen sogenannten unsicheren Drittstaat. Des Weiteren umfasst der Maßnahmenkatalog der *Data Privacy Organization* flankierende organisatorische Maßnahmen zur Sicherstellung der Gewährleistung der Betroffenenrechte.

4.11.2.2 Beschreibung

Die in dem Maßnahmenkatalog der *Informationssicherheit* und dem darauf aufsetzenden Maßnahmenkatalog der *Data Privacy Organization* dargestellten TOM müssen derart ausgestaltet sein, dass die Rechte und Freihei- ten der betroffenen Personen angemessen geschützt sind und die rechtlichen Anforderungen gewahrt werden können. Welche TOM geeignet sind, ist unter Berücksichtigung folgender Faktoren zu beurteilen:

- Art, Umfang und Umstände der Verarbeitung,
- Risiken der Verarbeitung,
- Stand der Technik sowie
- die Implementierungskosten.¹³⁵

Die TOM sind so zu gestalten, dass die **Datenschutzprinzipien** bezogen auf die gesetzlichen Anforderungen ein- gehalten werden können.

- **Rechtmäßigkeit** der Verarbeitung¹³⁶

Die Verarbeitung von personenbezogenen Daten ist rechtmäßig, wenn eine Rechtsgrundlage für die Da- tenverarbeitung vorliegt, insbesondere eine Einwilligung der betroffenen Person¹³⁷ oder eine andere rechtliche Grundlage (z. B. in der EU/EWR aus der DSGVO¹³⁸)

- Verarbeitung nach **Treu und Glauben**¹³⁹

Die Verarbeitung nach Treu und Glauben lässt sich nur am konkreten Einzelfall unter Berücksichtigung aller Umstände beurteilen. Dieser Grundsatz betrifft die Art und Weise der Rechtsausübung im Verhältnis zwischen Verantwortlichem und betroffener Person.

- **Transparenz**¹⁴⁰

Der Grundsatz der Transparenz soll insbesondere gewährleisten, dass die betroffenen Personen im enge- ren Sinne ihre Betroffenenrechte und im weiteren Sinne generell ihr Recht auf informationelle Selbstbe- stimmung wahrnehmen können.

- **Zweckbindung**¹⁴¹

Der Grundsatz der Zweckbindung legt fest, dass die Zwecke der Datenverarbeitung bereits bei der Erhe- bung personenbezogener Daten festgelegt, eindeutig und legitim sein müssen. Eine Weiterverarbeitung zu anderen Zwecken kann möglich sein, sofern die Zwecke der Weiterverarbeitung nicht mit den ur- sprünglichen Erhebungszwecken unvereinbar sind und eine Rechtsgrundlage hierfür vorliegt.

¹³⁵ Vgl. Art. 25 Abs. 1 DSGVO.

¹³⁶ Vgl. Art. 5 Abs. 1 lit. a DSGVO i.V.m. Art. 6 DSGVO.

¹³⁷ Vgl. Art. 6 Abs. 1 lit. a DSGVO i.V.m. Art. 7-9 DSGVO.

¹³⁸ Vgl. Art. 6 Abs. 1 DSGVO.

¹³⁹ Vgl. Art. 5 Abs. 1 lit. a DSGVO.

¹⁴⁰ Vgl. Art. 5 Abs. 1 lit. a DSGVO und ErwGr. 39 DSGVO.

¹⁴¹ Vgl. Art. 5 Abs. 1 lit. b DSGVO.

- **Datenminimierung¹⁴²**

Personenbezogene Daten müssen dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt werden (Grundsatz der Datenminimierung).

- **Richtigkeit der Datenverarbeitung¹⁴³**

Personenbezogene Daten müssen sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein. Personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, sind unverzüglich zu löschen¹⁴⁴ oder zu berichtigen¹⁴⁵.

- **Speicherbegrenzung¹⁴⁶**

Mit der normierten Speicherbegrenzung dürfen personenbezogene Daten nur in einer Form gespeichert werden, die die Identifizierung der Person nur solange ermöglicht, wie es für die Zwecke der Verarbeitung erforderlich ist. Sobald die Speicherung personenbezogener Daten für den Verarbeitungszweck also nicht mehr erforderlich ist, müssen die personenbezogenen Daten gelöscht¹⁴⁷ oder die Identifizierung der betroffenen Person aufgehoben werden. Ausnahmen ergeben sich in der EU/EWR für

- im öffentlichen Interesse liegende Archivzwecke,
- für wissenschaftliche oder historische Forschungszwecke und
- für statistische Zwecke¹⁴⁸.

Der Grundsatz der Speicherbegrenzung ist beginnend bei der Erfassung über den Lebenszyklus eines Datums bis hin zur Löschung zu berücksichtigen, insbesondere in einem Lösch- und Sperrkonzept.

- **Integrität und Vertraulichkeit¹⁴⁹**

Personenbezogene Daten müssen in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet. Dies umfasst auch den Schutz vor unbefugter sowie unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder Schädigung der personenbezogenen Daten. Hierfür sind geeignete technische und organisatorische Maßnahmen zu treffen¹⁵⁰.

- **Widerspruchsrecht¹⁵¹**

Das Widerspruchsrecht beinhaltet zum einen die Möglichkeit, der Verarbeitung eigener Daten zu werblichen Zwecken zu widersprechen. Daneben kann beim Vorliegen besonderer Gründe auch einer ursprünglich rechtmäßigen Datenverarbeitung zu anderen Zwecken widersprochen werden.

- **Recht auf Datenübertragbarkeit¹⁵² und Auskunftsrecht¹⁵³**

Berücksichtigung des Rechts der betroffenen Personen auf Zugang zu ihren Daten und darauf, eine Kopie der Daten im maschinenlesbaren Format zu erhalten.

- **Recht auf Berichtigung¹⁵⁴**

Das Recht auf Berichtigung umfasst einen Anspruch der betroffenen Person, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger personenbezogener Daten zu verlangen.

¹⁴² Vgl. Art. 5 Abs. 1 lit. c DSGVO.

¹⁴³ Vgl. Art. 5 Abs. 1 lit. d DSGVO.

¹⁴⁴ Vgl. Art. 17 Abs. 1 lit. d DSGVO.

¹⁴⁵ Vgl. Art. 16 DSGVO.

¹⁴⁶ Vgl. Art. 5 Abs. 1 lit. e DSGVO.

¹⁴⁷ Vgl. Art. 17 Abs. 1 lit. a DSGVO.

¹⁴⁸ Vgl. Art. 5 Abs. 1 lit. e DSGVO.

¹⁴⁹ Vgl. Art. 5 Abs. 1 lit. f DSGVO.

¹⁵⁰ Vgl. Art. 32 DSGVO.

¹⁵¹ Vgl. Art. 21 DSGVO.

¹⁵² Vgl. Art. 20 DSGVO.

¹⁵³ Vgl. Art. 15 DSGVO.

¹⁵⁴ Vgl. Art. 16 DSGVO.

- Recht auf **Löschung** und „**Recht auf Vergessenwerden**“¹⁵⁵

Die betroffene Person hat das Recht, von dem Verantwortlichen zu verlangen, dass sie betreffende, personenbezogene Daten unverzüglich gelöscht werden, insbesondere wenn diese Daten für die Zwecke, für die sie erhoben wurden, nicht mehr erforderlich sind oder wenn die Daten unrechtmäßig erhoben wurden.

- Recht auf **Einschränkung** der Verarbeitung¹⁵⁶

Mit dem Recht auf Einschränkung der Verarbeitung können betroffene Personen beim Vorliegen bestimmter Voraussetzungen erreichen, dass ihre personenbezogenen Daten beim für die Verarbeitung Verantwortlichen gesperrt und somit nicht weiterverarbeitet werden. So kann die Sperrung für die Dauer einer Aufklärung verlangt werden, wenn die Richtigkeit der gespeicherten Daten bestritten wird.

- **Angemessenes Datenschutzniveau** im Drittland¹⁵⁷

Zudem müssen die Verpflichtungen im Zusammenhang mit der Übermittlung von Daten außerhalb der Europäischen Union bzw. des europäischen Wirtschaftsraumes berücksichtigt werden. Jedwede Übermittlung personenbezogener Daten, die bereits verarbeitet werden oder nach ihrer Übermittlung an ein Drittland oder eine internationale Organisation verarbeitet werden sollen, ist nur zulässig, wenn der Verantwortliche und der Auftragsverarbeiter ein angemessenes Datenschutzniveau im Drittland nachweisen können.

Eine Übermittlung liegt bereits dann vor, wenn zu Support- und Wartungszwecken aus dem Drittland auf personenbezogene Daten zugegriffen werden kann. Der Standort des Rechenzentrums ist dabei unerheblich.

- **Kontrolle** der eingesetzten **Auftragnehmer**¹⁵⁸

Es dürfen nur Auftragnehmer eingesetzt werden, die hinreichende Garantien dafür bieten, dass geeignete TOM so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen des Datenschutzes und den Sicherheitsvorgaben der IT- und Informationssicherheit erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet.

Darüber hinaus sind folgende Maßnahmen zu berücksichtigen, abhängig vom Risiko der Verarbeitung:

- organisatorische Kontrollen/Maßnahmen zu: Organisation (Aufbau und Ablauf), Policy, Risiko-management, Projektmanagement, Störungsmanagement, Überwachung usw.
- logische Sicherheitskontrollen/Sicherheitsmaßnahmen zu: Anonymisierung, Pseudonymisierung, Verschlüsselung, Backups, Datenpartitionierung, logische Zugriffskontrolle usw.
- physische Sicherheitskontrollen/Sicherheitsmaßnahmen zu: physische Zugangskontrolle, Sicherheit der Hardware, Schutz vor nichtmenschlichen Risikoquellen usw.

Bei der Festlegung der geeigneten technischen und organisatorischen Maßnahmen **müssen** insbesondere die folgenden potentiellen Risiken berücksichtigt werden (vgl. Ziffer 4.10):

- unberechtigter Zugang zu Verarbeitungsanlagen/Assets
- unbefugtes Lesen, Kopieren, Verändern oder Löschen von Daten bzw. Datenträgern
- unbefugte Eingabe von personenbezogenen Daten sowie unbefugte Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten
- unbefugte Nutzung von IT-Systemen über Verbindungen (Netzwerke) hinweg
- unbefugter Zugang der zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten auf personenbezogene Daten
- es kann nicht nachträglich überprüft und festgestellt werden, welche personenbezogene Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind
- Verlust der Vertraulichkeit und Integrität bei der Übermittlung personenbezogener Daten sowie beim Transport von entsprechenden Datenträgern

¹⁵⁵ Vgl. Art. 17 DSGVO.

¹⁵⁶ Vgl. Art. 18 DSGVO.

¹⁵⁷ Vgl. Art. 44 ff. DSGVO.

¹⁵⁸ Vgl. Art 28 Abs. 1 DSGVO.

- IT-Systeme lassen sich im Störfall nicht oder nicht rechtzeitig wiederherstellen
- Funktionen stehen nicht zur Verfügung oder auftretende Fehlfunktionen werden nicht gemeldet
- gespeicherte personenbezogene Daten werden durch Fehlfunktion des Systems beschädigt
- personenbezogene Daten, die im Auftrag verarbeitet werden, werden nicht entsprechend der Weisungen des Auftraggebers verarbeitet.
- personenbezogene Daten sind nicht gegen Zerstörung oder Verlust geschützt
- personenbezogene Daten die zu unterschiedlichen Zwecken und für unterschiedliche Verantwortliche erhoben wurden, werden nicht getrennt verarbeitet

4.11.2.3 Dokumentation

Die Erstellung und Führung des Maßnahmenkatalogs ist in einer eignen Richtlinie/Anweisung zu dokumentieren.

4.11.2.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer & Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Prüft regelmäßig, ob die für die Verarbeitung bzw. für das Asset gewählten TOM noch angemessen sind, d. h. insbesondere der Art und dem Umfang der Verarbeitung sowie dem Stand der Technik entsprechen. ▪ Berücksichtigt bei der Einführung oder Änderung einer Verarbeitung die Datenschutzprinzipien.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Unterstützt den Prozesseigentümer/Asset-Eigentümer bei der Prüfung, ob die gewählten TOM noch angemessen sind. ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Unterstützt den Prozesseigentümer/Asset-Eigentümer bei der Prüfung, ob die gewählten TOM noch angemessen sind. ▪ Pflegt den Maßnahmenkatalog und bindet hierbei u. a. die IT-Sicherheit, den Datenschutzbeauftragten und die Data Privacy Organization ein. ▪ Informiert bei wichtigen/wesentlichen Änderungen und Ereignissen bezogen auf die Datensicherheit die Data Privacy Organization und insbesondere die Prozesseigentümer sowie Asset-Eigentümer über sicherheitsrelevante Änderungen und Anpassungen, damit diese in Verfahren, Assets und Projekten zeitnah berücksichtigt werden können. ▪ Schafft (mit Unterstützung) Prozesse zur regelmäßigen Beobachtung aktuell verfügbarer Technologien und passt die im Maßnahmenkatalog beschriebenen Maßnahmen ggf. an, soweit die Beteiligten hierbei feststellen, dass diese nicht mehr dem Stand der Technik entsprechen. ▪ Prüft regelmäßig, ob die in dem Maßnahmenkatalog beschriebenen TOM dem Stand der Technik entsprechen.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.¹⁵⁹

4.12 Datenschutz-Folgenabschätzung (DSFA)

4.12.1 Einleitung

Es ist sicherzustellen, dass eine DSFA durchgeführt wird, wenn die jeweilige Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat.

Die DSFA findet statt, wenn eine Schwellwert-Analyse ein hohes Risiko für betroffene Personen ermittelt hat.

Dies ist stets (aber nicht nur dann) der Fall, wenn bei einer Verarbeitung ein gesetzliches Regelbeispiel¹⁶⁰ oder die behördlich festgelegten Schwellwerte für eine DSFA vorliegen (vgl. Ziffer 4.10.5).

¹⁵⁹ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

¹⁶⁰ Vgl. Art. 35 Abs. 3 DSGVO.

4.12.2 Beschreibung

4.12.2.1 Regelfall

Der Prozess ist durchzuführen, wenn die jeweilige Datenverarbeitung (insbesondere bei Verwendung neuer Technologien beispielsweise in Form von künstlicher Intelligenz) aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies richtet sich nach dem Ergebnis einer formalen Schwellwertanalyse bei Erfassung der Verarbeitungstätigkeit im VVT (vgl. Ziffer 5.3). Die DSFA ist kein einmaliger Prozess zur Dokumentation eines Verfahrens, vielmehr handelt es sich hierbei um einen iterativen Prozess.

Ist eine DSFA durchzuführen, so umfasst sie mindestens die folgenden Punkte:

- Eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung, ggf. einschließlich der von dem für die Verarbeitung 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;
- die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen, einschließlich Garantien, Sicherheitsvorkehrungen und Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und der Nachweis dafür erbracht werden soll, dass die Bestimmungen dieser Verordnung eingehalten werden, wobei den Rechten und berechtigten und schutzwürdigen Interessen der betroffenen Personen und sonstiger betroffener Personen Rechnung getragen werden soll.¹⁶¹

Hierfür ist für die jeweilige Verarbeitung eine Betrachtung der technischen Prozesse, IT-Systeme (Assets) sowie Datenflüsse und Systemgrenzen im Detail erforderlich. Die Bewertung des Risikos erfolgt mit Blick auf die Risiken der Verarbeitung aus der Sicht der betroffenen Person (vgl. Ziffer 4.10).

Bis die Data Privacy Organization eine einheitliche Vorgehensweise zur DSFA definiert und beschrieben hat, wird für den Rheinmetall Konzern zunächst grundsätzlich das DSFA-Modell der französischen Datenschutzbehörde CNIL als organisatorischer Rahmen vorgegeben. Bei Durchführung sind die Vorgaben aus diesem Abschnitt zu beachten. Abweichungen von diesem Grundsatz müssen durch den zuständigen Data Privacy Officer genehmigt werden.

4.12.2.2 Ausnahmen zur DSFA

Eine DSFA ist nicht erforderlich, wenn die Datenverarbeitung in Erfüllung rechtlicher Verpflichtungen oder zur Wahrnehmung einer Aufgabe im öffentlichen Interesse oder in Ausübung öffentlicher Gewalt erfolgt.¹⁶² Entsprechende Vorschriften finden sich beispielsweise im Geldwäschegesetz oder in der Abgabenordnung.

Die Entscheidung über das Vorliegen eines solchen Ausnahmefalls **darf** nur nach Rücksprache mit der *Data Privacy Officer* oder dem *Datenschutzbeauftragten* getroffen werden.

4.12.2.3 Whitelist und Blacklist

Eine DSFA ist stets durchzuführen, wenn die beabsichtigte Tätigkeit auf der sogenannten „Blacklist“ zu finden ist. Dies ist eine von den Aufsichtsbehörden erstellte Liste von Verarbeitungstätigkeiten, bei denen stets eine DSFA erforderlich ist.¹⁶³

Soweit von den Aufsichtsbehörden auch eine Liste mit Arten von Verarbeitungsvorgängen erstellt worden ist, für die keine DSFA erforderlich ist (sogenannte „Whitelist“), so ist auch diese Liste zu berücksichtigen.¹⁶⁴

¹⁶¹ Mindestinhalte der Datenschutz-Folgenabschätzung nach Art. 35 Abs. 7 DSGVO.

¹⁶² Vgl. Art. 35 Abs. 10 DSGVO.

¹⁶³ Vgl. Art. 35 Abs. 4 DSGVO.

¹⁶⁴ Art. 35 Abs. 5 DSGVO.

4.12.2.4 Voraussichtlich hohes Risiko für die betroffene Person

Zur Ermittlung eines (hohen oder sehr hohen) Risikos ist eine Risikobewertung nach Ziffer 4.10 durchzuführen.

Ein hohes Risiko für die betroffene Person ist stets anzunehmen, wenn ein gesetzliches Regelbeispiel, z. B. die umfangreiche Verarbeitung besonderer Kategorien personenbezogener Daten, vorliegt.¹⁶⁵

4.12.2.5 Einholung des Standpunktes der betroffenen Person oder seines Vertreters

Es kann auch der Standpunkt der betroffenen Personen oder ihrer Vertreter zu der beabsichtigten Verarbeitung eingeholt werden.¹⁶⁶ Dies umfasst beispielsweise die Einbindung von Gremien der Mitbestimmung oder ggfs. Verbraucherschutzverbänden.

4.12.3 Dokumentation

Die Durchführung der DSFA ist zu dokumentieren. In dem genutzten Archivsystem sind insbesondere die Durchführung der DSFA und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen zu hinterlegen. Dies geschieht regelmäßig durch die Anfertigung eines umfassenden Protokolls des Ablaufs der DSFA, welches eine detaillierte Erläuterung der gefundenen Ergebnisse und der getroffenen Maßnahmen enthält.

4.12.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer & Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Initiiert bei Vorliegen der Voraussetzungen die Vornahme einer DSFA vor Beginn der Datenverarbeitung. ▪ Dokumentiert toolgestützt die Durchführung der DSFA und die zur Bewältigung der Risiken geplanten Abhilfemaßnahmen. ▪ Zieht die Data Privacy Organization und die Informationssicherheit bei der Durchführung einer DSFA hinzu. ▪ Entwickelt auf Grundlage der Bewertung durch die Data Privacy Organization gemeinsam mit dieser und der Informationssicherheit einen Aktionsplan. ▪ Nimmt die finale Validierung der DSFA vor. ▪ Kann zur Steigerung der Objektivität, Nachvollziehbarkeit und Glaubwürdigkeit einer DSFA eine konzernfremde, unabhängige Instanz (beispielsweise externe Rechtsberatung) hinzuziehen. ▪ Prüft, ob die vorgeschlagenen Abhilfemaßnahmen tatsächlich umgesetzt wurden¹⁶⁷ und wirksam sind, sodass die Datenverarbeitung rechtmäßig und beanstandungsfrei durchgeführt werden kann. ▪ Kann die Data Privacy Organization zur Beratung hinzuziehen.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Unterstützt die Prozesseigentümer und Asset-Eigentümer bei der Dokumentation.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Überprüft die Beschreibung und prüft bei der Durchführung der DSFA, ob der Maßnahmenkatalog (Ziffer 4.11) und die Vorgaben zur Methodik der Risikobewertung (Ziffer 4.10) entsprechend berücksichtigt wurden. ▪ Erstellt eine erste Bewertung der Datenverarbeitung und formuliert einen Vorschlag für die Ziele der DSFA. ▪ Prüft, ob die vorgeschlagenen Abhilfemaßnahmen tatsächlich umgesetzt wurden¹⁶⁸ und wirksam sind, sodass die Datenverarbeitung rechtmäßig und beanstandungsfrei durchgeführt werden kann. ▪ Regelt den Prozess der DSFA in einer eigenen Richtlinie/Anweisung.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Entwickelt auf Grundlage der Bewertung durch die Data Privacy Organization gemeinsam mit dieser und dem Prozesseigentümer einen Aktionsplan.

¹⁶⁵ Regelbeispiele nach Art. 35 Abs. 3 DSGVO.

¹⁶⁶ Vgl. Art. 35 Abs. 9 DSGVO.

¹⁶⁷ Vgl. Art. 35 Abs. 11 DSGVO.

¹⁶⁸ Vgl. Art. 35 Abs. 11 DSGVO.

Rolle	Verantwortung
Datenschutzbeauftragter	<ul style="list-style-type: none">▪ Ist per Gesetz bei der DSFA eine überwachende Rolle zugewiesen.¹⁶⁹▪ Kann auf Anfrage des Prozesseigentümers beratend tätig werden.▪ Überwacht die Durchführung der DSFA.

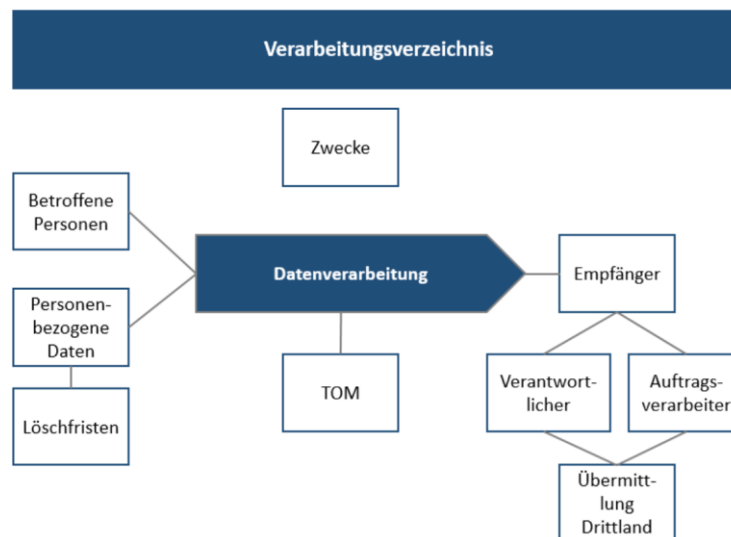
¹⁶⁹ Vgl. Art. 39 Abs. 1 lit. c DSGVO.

5 Verarbeitungstätigkeiten, Assets und verarbeitungsbasierte Risiken

5.1 Einleitung

Die ordnungsgemäße Beschreibung und Dokumentation von Verarbeitungstätigkeiten gehört nicht nur zu den zentralen Anforderungen des Datenschutzes¹⁷⁰, sondern ist wesentliche Grundlage für jede datenschutzrechtliche Prüfung und Bewertung. Jede Verarbeitung von personenbezogenen Daten muss erfasst, beschrieben, dokumentiert und in das sogenannte Verzeichnis von Verarbeitungstätigkeiten (VVT)¹⁷¹ des jeweiligen Unternehmens (der Legaleinheit) aufgenommen werden. Das VVT enthält die Summe aller Beschreibungen von Verarbeitungstätigkeiten des jeweiligen Unternehmens.

Aus den Verarbeitungsbeschreibungen muss sich u. a. entnehmen lassen, welche personenbezogenen Daten von welchen betroffenen Personen (Kategorien) zu welchen Zwecken verarbeitet werden, wer Zugriff auf diese Daten erhält (Empfänger), wer für die jeweilige Verarbeitung verantwortlich und wer ggf. als Auftragsverarbeiter tätig ist, durch welche technischen und organisatorischen Maßnahmen (TOM) die Verarbeitung abgesichert wird, ob eine Übermittlung in ein Drittland stattfindet und wie lange die Daten gespeichert werden (Löschfristen). Die nachfolgende Abbildung fasst dies grafisch kurz zusammen:



Jedes *Unternehmen* im Rheinmetall Konzern **muss** ein Verzeichnis seiner Verarbeitungen (Verarbeitungsverzeichnis bzw. Verzeichnis von Verarbeitungstätigkeiten) führen.

Das Verzeichnis **muss** alle internen und ausgelagerten Verarbeitungen beinhalten.

Die Verarbeitungstätigkeiten (Geschäftsprozesse mit personenbezogenen Daten) und die Assets (insbesondere IT-Anwendungen) **müssen** durch ihre jeweiligen *Eigentümer* (Prozesseigentümer, Asset-Eigentümer) dokumentiert und datenschutzgerecht beschrieben werden.

Die *Data Privacy Organization* **muss** geeignete Tools und / oder Checklisten zur datenschutz-gerechten Dokumentation und Beschreibung zur Verfügung stellen.

5.2 Allgemeine Vorgaben zu den Verarbeitungs- und Asset-Beschreibungen

Es muss sichergestellt werden, dass alle Verarbeitungstätigkeiten ordnungsgemäß erfasst, beschrieben und im Verzeichnis von Verarbeitungstätigkeiten (VVT) dokumentiert sind. Außerdem muss gewährleistet werden, dass alle in Verarbeitungstätigkeiten involvierten Assets (insbesondere IT-Anwendungen) ebenfalls erfasst, beschrieben und dokumentiert sind. Die ordnungsgemäße Beschreibung und Dokumentation der Verarbeitungstätigkeiten

¹⁷⁰ Vgl. Art. 5 Abs. 3, Art. 30 DSGVO.

¹⁷¹ Gesetzlich vorgeschrieben nach Art. 30 DSGVO. Oft synonym bezeichnet als „Verzeichnis aller Verarbeitungstätigkeiten“, „Verzeichnis der Verarbeitungstätigkeiten“ und „Verarbeitungsverzeichnis“.

ten und Assets ist zur Erfüllung der datenschutzrechtlichen Anforderungen unerlässlich. Eine datenschutzrechtliche Betrachtung und Bewertung eines Geschäftsprozesses (bzw. einer Verarbeitungstätigkeit) ist ohne gleichzeitige Betrachtung und Bewertung der involvierten Assets nicht möglich.

5.2.1 Beschreibung

5.2.1.1 Regelfall: Pflicht zur Führung eines Verzeichnisses von Verarbeitungstätigkeiten

Dieser Prozess (datenschutzrechtliche Erfassung, Beschreibung, Dokumentation und Bewertung) **muss** bei jeder Verarbeitungstätigkeit beachtet werden.

Für jede neue Verarbeitungstätigkeit ist eine Verarbeitungsbeschreibung zu erstellen. Die Gesamtheit aller Verarbeitungsbeschreibungen bildet das Verzeichnis von Verarbeitungstätigkeiten.

Eine Verarbeitungsbeschreibung ist mindestens mit folgenden Angaben zu erstellen und zu pflegen:

- den Namen und die Kontaktdaten des Verantwortlichen und ggf. des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten,
- die Zwecke der Verarbeitung,
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten,
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen,
- ggf. Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation sowie
- ggf. die Dokumentation geeigneter Garantien,
- wenn möglich, die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien und
- eine allgemeine Beschreibung der getroffenen technischen und organisatorischen Maßnahmen.¹⁷²

Da Verarbeitungsbeschreibungen zudem als zentrale Grundlage insbesondere für die datenschutzrechtliche Beratung, bei Betroffenenanfragen, bei Datenschutz-Risikobewertungen, bei Datenschutz-Folgenabschätzungen (DSFA), bei der Gestaltung von Datenschutzvereinbarungen und bei der Bearbeitung von Datenschutzvorfällen dienen, sind darüber hinaus weitergehende Angaben erforderlich, die über die einschlägigen Checklisten/Tools geeignet abgefragt werden.

Das Verzeichnisse sollte sich am Aufbau und an der Komplexität des Unternehmens orientieren. Der Detailgrad des Verzeichnisses sollte sich auch an den Anforderungen der lokalen Datenschutz Organisation und ihrer Arbeitsweise orientieren. Gleichzeitig muss das Verzeichnisse so ausgestaltet sein, dass es den gesetzlichen Anforderungen genügt.¹⁷³

Jede Veränderung einer bestehenden Verarbeitungstätigkeit sowie jede Veränderung der technischen und organisatorischen Maßnahmen **muss** umgehend in die Verarbeitungsbeschreibung aufgenommen werden.

Die einzelnen Verarbeitungsbeschreibungen sind an geeigneter Stelle innerhalb des Verantwortlichen (des Unternehmens) zum Verzeichnis aller Verarbeitungstätigkeiten zusammenzuführen. Die Beschreibung bzw. Dokumentation einer Verarbeitung muss mit der weiteren Entwicklung der Verarbeitung fortgeschrieben werden, wenn sich für das Verzeichnis relevante Sachverhalte ändern.

Auf Anfrage **muss** das Verzeichnis von Verarbeitungstätigkeiten der Aufsichtsbehörde zur Verfügung gestellt werden.¹⁷⁴

5.2.1.2 Besonderheit: Verarbeitungsbeschreibung im Konzern

Der *Prozesseigentümer* hat festzulegen und in der Verarbeitungsbeschreibung zu dokumentieren, welche Konzerngesellschaften die Verantwortung für die Verarbeitung tragen, ob eine gemeinsame Verantwortlichkeit für

¹⁷² Pflichtangaben nach Art. 30 Abs. 1 DSGVO.

¹⁷³ Vgl. Art. 5 Abs. 2, Art. 24 und Art. 30 DSGVO.

¹⁷⁴ Vgl. Art. 30 Abs. 4 DSGVO.

die Verarbeitung oder ob eine Auftragsverarbeitung vorliegt. Die Konzerngesellschaften sind als (eigenständige) Verantwortliche, gemeinsame Verantwortliche oder Auftragsverarbeiter in der Verarbeitungsbeschreibung zu dokumentieren.

5.2.1.3 Führung eines Verzeichnisses von Verarbeitungstätigkeiten als Auftragsverarbeiter

Wird die Verarbeitungstätigkeit ausnahmsweise als Auftragsverarbeiter durchgeführt, so ist ebenfalls ein Verzeichnis von den Verarbeitungstätigkeiten zu erstellen, die im Auftrag des Verantwortlichen durchgeführt werden. In diesem Fall muss es mindestens die folgenden Pflichtangaben enthalten:

- den Namen und die Kontaktdaten des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie ggf. des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen DSB,
- die Kategorien von Verarbeitungen, die im Auftrag jedes Verantwortlichen durchgeführt werden,
- ggf. Übermittlungen von personenbezogener Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation sowie
- ggfs. die Dokumentierung geeigneter Garantien und
- eine allgemeine Beschreibung der getroffenen technischen und organisatorischen Maßnahmen.¹⁷⁵

Im Regelfall wird sich ein Verzeichniseintrag für den Auftragsverarbeiter aus einem entsprechenden Eintrag des Auftraggebers (Verantwortlichen) ableiten lassen.

Das Verzeichnis von Verarbeitungstätigkeiten als Auftragsverarbeiter ist der Aufsichtsbehörde auf Anfrage zur Verfügung zu stellen.¹⁷⁶

Die Beschreibung bzw. Dokumentation einer Verarbeitung muss mit der weiteren Entwicklung der Verarbeitung fortgeschrieben werden, wenn sich für das Verzeichnis relevante Sachverhalte ändern.

5.2.1.4 Art der Darstellung

Die Beschreibung und Dokumentation von Verarbeitungstätigkeiten und Assets sowie die Erstellung des Verzeichnisses von Verarbeitungstätigkeiten **müssen** nach einem vorgegebenen Muster (vgl. Ziffer 5.3) erfolgen.

Die Angaben müssen detailliert, systematisiert, geordnet und zeitlich zuordenbar (z. B. durch eine Versionsnummer und die Angabe eines Datums) sein.¹⁷⁷ Hierfür werden Tools und Arbeitshilfen durch die Data Privacy Organization zur Verfügung gestellt.

Bei konzerninternen Verarbeitungen sind Verantwortlicher und Auftragsverarbeiter sauber zu trennen und in der Verarbeitungsbeschreibung zu dokumentieren.

5.2.1.5 Ausnahmen

Das Verzeichnis von Verarbeitungstätigkeiten muss laut Gesetzeswortlaut ausnahmsweise dann nicht geführt werden, wenn im Unternehmen weniger als 250 Beschäftigte beschäftigt sind und die vorgenommene Verarbeitung kein Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, die Verarbeitung nur gelegentlich erfolgt oder keine besonderen Kategorien personenbezogener Daten oder Daten über strafrechtliche Verurteilungen oder Straftaten verarbeitet werden.¹⁷⁸

Die Entscheidung über das Entfallen der Verpflichtung zur Erstellung des Verzeichnisses der Verarbeitungstätigkeiten **darf** nur nach Rücksprache mit dem zuständigen *Data Privacy Officer* getroffen werden.

¹⁷⁵ Pflichtangaben nach Art. 30 Abs. 2 DSGVO.

¹⁷⁶ Vgl. Art. 30 Abs. 4 DSGVO.

¹⁷⁷ Vgl. Art. 30 Abs. 3 DSGVO.

¹⁷⁸ Ausnahmen nach Art. 30 Abs. 5 DSGVO.

5.2.2 Dokumentation

Die Verarbeitungs- und Asset-Beschreibungen sind bei dem jeweiligen Verantwortlichen (der jeweiligen Legal-einheit) abzulegen bzw. zu dokumentieren. Die durchgeführten Risikobewertungen und Datenschutz-Folgenabschätzung sowie die zugeordneten technischen und organisatorischen Maßnahmen sind den Verarbeitungsbeschreibungen beizufügen.

Sofern einer der unter dem Kapitel 5.2.1.5 dargestellten Ausnahmefälle vorliegt, muss dies dokumentiert werden.

5.2.3 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none"> ▪ Beschreibt und dokumentiert die datenschutzrechtliche Beschreibung seiner Verarbeitungstätigkeiten nach Maßgabe dieses Handbuchs. ▪ Ist für die Erstellung, Richtigkeit und Vollständigkeit der Verarbeitungsbeschreibung zuständig. ▪ Ist für die Vornahme der Risikoabschätzung verantwortlich und initiiert ggf. die Durchführung einer Datenschutz-Folgenabschätzung. ▪ Prüft regelmäßig (mindestens alle zwei Jahre), ob eine zu dem Entwicklungsstand der Verarbeitung passende, aktuelle Verarbeitungsbeschreibung vorliegt. ▪ Prüft regelmäßig (mindestens alle zwei Jahre), ob die dokumentierte datenschutzrelevante Risikobeurteilung einer Verarbeitung einschließlich der zugeordneten technischen und organisatorischen Maßnahmen noch den aktuellen Erkenntnissen entspricht.
Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Ist für die datenschutzrechtliche Beschreibung und Dokumentation seiner Assets nach Maßgabe dieses Handbuchs zuständig. ▪ Prüft regelmäßig (mindestens alle zwei Jahre), ob eine zu dem Entwicklungsstand des Assets passende, aktuelle Asset-Beschreibung vorliegt.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Meldet (neue/geänderte) Verarbeitungstätigkeiten an die Data Privacy Organization.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Stellt die technischen Einrichtungen und Prozesse zum Führen des Verzeichnisses von Verarbeitungstätigkeiten zur Verfügung. ▪ Unterstützt mit Methoden- und Fachwissen. ▪ Unterstützt durch Vorgaben zu Dokumentationsstandards und ein geeignetes technisches Verfahren. ▪ Unterstützt den Prozesseigentümer bei der Erstellung der Verarbeitungsbeschreibung und der Durchführung der Risikoabschätzung.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Unterstützt bei der Zuordnung, Beschreibung und Dokumentation der risikoadäquaten Datensicherheitsmaßnahmen.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Erstellung des VVT. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.¹⁷⁹ ▪ Hat dauerhaft Zugriff auf das VVT.

5.3 Vorgaben zum Verzeichnisses von Verarbeitungstätigkeiten (VVT)

5.3.1 Einleitung

Jeder Geschäftsprozess, bei dem auch personenbezogene Daten vorkommen (= Verarbeitungstätigkeit, Verarbeitung), muss erfasst und detailliert beschrieben werden, um den datenschutzrechtlichen Dokumentations-, Nachweis- und Rechenschaftspflichten¹⁸⁰ nachzukommen. Diese umfassende Dokumentation von Verarbei-

¹⁷⁹ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

¹⁸⁰ Vgl. insb. Art. 5 Abs. 2, Art. 24, Art. 30 DSGVO.

tungstätigkeiten dient nicht nur der Erfüllung der Pflicht zur Führung des sogenannten Verzeichnisses von Verarbeitungstätigkeiten („VVT“)¹⁸¹, sondern ist zugleich eine unerlässliche Basis für die notwendige datenschutzrechtliche Bewertung eines jeden Geschäftsprozesses.

Die Erfassung, Beschreibung und anschließende Bewertung von Geschäftsprozessen/Verarbeitungstätigkeiten sollte im Rheinmetall Konzern primär anhand toolbasierter Fragebögen und Auswertungen erfolgen.

Hierbei werden nicht nur die Verarbeitungstätigkeiten als solche betrachtet, sondern auch die jeweils involvierten Assets (insbesondere IT-Anwendungen), Dienstleister/Lieferanten (insbesondere Auftragsverarbeiter) und Entitäten (Rheinmetall Gesellschaften). Diese Gesamtschau ermöglicht zudem eine sorgfältige Bewertung von Datenschutzrisiken (für die betroffenen Personen) und Datenschutz Compliance Risiken (für den Rheinmetall Konzern) sowie die Ableitung eventuell erforderlicher Maßnahmen.

5.3.2 Beschreibung

Die Erfassung, Beschreibung und Bewertung der Geschäftsprozesse bzw. Verarbeitungstätigkeiten erfolgt in mehreren Phasen und anhand der folgenden Fragebögen:

1. **Initialfragebogen:** Dient der Erfassung aller Geschäftsprozesse je Hauptabteilung und der Identifikation von Verarbeitungstätigkeiten.
2. **Verarbeitungsfragebogen:** Dient der detaillierten Beschreibung aller identifizierten Verarbeitungstätigkeiten. Je Verarbeitungstätigkeit ist ein Verarbeitungsfragebogen auszufüllen.
3. **Assetfragebogen:** Dient der detaillierten Beschreibung aller eingesetzten Assets (insbesondere IT-Anwendungen) je Verarbeitungstätigkeit. Je Asset ist ein Assetfragebogen auszufüllen.
4. **Risikofragebogen:** Dient der Identifikation und Bewertung der sogenannten Datenschutzrisiken einer Verarbeitungstätigkeit (einschließlich Assets). Je Verarbeitungstätigkeit ist ein Risikofragebogen auszufüllen.
5. **Datenverarbeitungsdienstleister(DVD)-Fragebogen:** Dient der Erfassung und Beschreibung der je Verarbeitungstätigkeit eingesetzten Lieferanten/Dienstleister. Je Lieferant/Dienstleister ist ein Lieferantenfragebogen auszufüllen.

Die Fragebögen werden von der Data Privacy Organization versendet. Der jeweilige Fragebogen ist durch den Ansprechpartner zu beantworten. Zur inhaltlichen Beantwortung der einzelnen Fragebögen sind allerdings eingehende Informationen zu den jeweiligen Geschäftsprozessen bzw. Verarbeitungstätigkeiten inklusive der eingesetzten Assets und Lieferanten/Dienstleister erforderlich (vgl. Ziffer 5.2).

5.3.2.1 Initialfragebogen

Zunächst hat jede Hauptabteilung ihre eigenen Geschäftsprozesse zu identifizieren und zu beschreiben (sofern nicht bereits geschehen) und sodann in einem „Initialfragebogen“ zu erfassen. Im Rahmen der konzernweiten Ersterfassung erhalten alle Hauptabteilungen nach vorheriger Ankündigung und ggf. Schulung diesen Fragebogen zur initialen Erfassung aller Geschäftsprozesse. Im späteren Verlauf (nach der Ersterfassung) sind neue Geschäftsprozesse oder wesentliche Änderungen an bestehenden Geschäftsprozessen unaufgefordert die Data Privacy Organization zu melden, um eine entsprechende Erfassung zu initiieren.

Im „Initialfragebogen“ muss für jeden Geschäftsprozess u. a. ein Prozesseigentümer bzw. zuständiger Ansprechpartner benannt werden, der anschließend auch für die Beantwortung der weiteren Fragebögen für seine jeweilige(n) Verarbeitungstätigkeit(en) zuständig ist. Zudem werden hier schon Kurzbeschreibungen, eventuell involvierte IT-Anwendungen sowie die relevanten Kategorien personenbezogener Daten und Betroffenenkategorien (z. B. Beschäftigte im Rheinmetall Konzern, Kunden B2B/B2C) abgefragt.

Nach Beantwortung des Initialfragebogens erfolgt die Auswertung durch die Data Privacy Organization. Hier wird ermittelt, bei welchen Geschäftsprozessen es sich zugleich um Verarbeitungstätigkeiten handelt, die einer näheren Dokumentation bedürfen. Für jede identifizierte Verarbeitungstätigkeit wird anschließend ein erweiterter Verarbeitungsfragebogen an den im Initialfragebogen benannten Prozesseigentümer bzw. zuständigen Ansprechpartner übersendet.

¹⁸¹ Vgl. Art. 30 DSGVO.

5.3.2.2 Verarbeitungsfragebogen

Über den Verarbeitungsfragebogen erfolgt eine umfassende Beschreibung der einzelnen Verarbeitungstätigkeiten durch den jeweils vom zuständigen Prozesseigentümer benannten Ansprechpartner. Hier werden wesentliche Informationen abgefragt, die für die Erfüllung der verschiedenen datenschutzrechtlichen Vorgaben notwendig sind.

U. a. werden hier auch die konkreten Assets (inkl. Asset-Eigentümer bzw. zuständigem Ansprechpartner je Asset) und Datenverarbeitungsdienstleister näher erfasst, für welche anschließend die Asset- und Dienstleisterfragebögen beantwortet werden müssen. Außerdem werden relevante Dokumente (u. a. Löschkonzept, Rollen- und Berechtigungskonzept, Betriebskonzept, Prozessdarstellung, Datenschutzinformationen, Datenschutz- oder Leistungsverträge) erfragt, die – soweit vorhanden – jeweils als Anlagen im Fragebogen hochzuladen sind.

Soweit erforderlich, führt die Data Privacy Organization für jede Hauptabteilung einen Workshop durch, in welchem exemplarisch die Beantwortung der verschiedenen Fragebögen für eine ausgewählte Verarbeitungstätigkeit (inkl. Asset und Risiko) durchgegangen wird. Auf diese Weise werden die zuständigen Beschäftigten befähigt, die Fragebögen für ihre weiteren Verarbeitungstätigkeiten, Assets und Datenverarbeitungsdienstleister eigenständig zu beantworten.

Nach Beantwortung des Verarbeitungsfragebogens erfolgt die Auswertung durch die Data Privacy Organization (je Verarbeitungstätigkeit). Hierbei können insbesondere Datenschutz und Datenschutz Compliance Risiken identifiziert, etwaige Rückfragen gestellt und erforderliche Handlungsbedarfe festgelegt werden.

5.3.2.3 Assetfragebogen

Über den Assetfragebogen erfolgt eine umfassende Beschreibung der einzelnen Assets (insbesondere IT-Anwendungen) durch den jeweils zuständigen Asset-Eigentümer. Hier werden wesentliche Informationen abgefragt, die für die Erfüllung der verschiedenen datenschutzrechtlichen Vorgaben notwendig sind.

Je nach Asset ist eine von drei Varianten des Assetfragebogens auszufüllen:

- Umfassender Assetfragebogen für IT-Anwendungen
- Verkürzter Assetfragebogen für webbasierte Auskunftsdienste (z. B. LexisNexis, Compliance Catalyst, Beck Online)
- Verkürzter Assetfragebogen für analoge Assets (z. B. Dokumentenarchive, Personalaktenschränke)

Neben Angaben zum Asset werden auch Informationen u. a. zum Anbieter/Betreiber und Serverstandort sowie zur Informations- und IT-Sicherheit gestellt.

Falls notwendige Informationen zur Beantwortung bestimmter Fragen nicht vorliegen, muss der zuständige Asset-Eigentümer entsprechende Nachforschungen tätigen und eventuell mit dem Dienstleister/Anbieter, der Informations- und/oder IT-Sicherheit in Kontakt treten.

Nach Beantwortung des Assetfragebogens erfolgt die Auswertung durch die Data Privacy Organization (je Asset). Hierbei können insbesondere Datenschutz Compliance Risiken identifiziert, etwaige Rückfragen gestellt und erforderliche Handlungsbedarfe festgelegt werden. Die Identifizierung, Bewertung und Behandlung der Risiken sowie Nachverfolgung der erforderlichen Maßnahmen erfolgt ebenfalls toolgestützt (vgl. Ziffer 4.10 und 4.11).

5.3.2.4 Risikofragebogen

Über den Risikofragebogen erfolgt eine Identifikation, Beschreibung und Bewertung der Datenschutzrisiken der Verarbeitungstätigkeit unter Berücksichtigung der etwaig eingesetzten Assets und Lieferanten/Dienstleister. Bei diesen Datenschutzrisiken handelt es sich um Risiken, die für die von der Verarbeitungstätigkeit betroffenen Personen (z. B. Beschäftigte von Rheinmetall, Beschäftigte von Lieferanten/Dienstleister, Beschäftigte von Kunden B2B/B2C, Privatkunden) aufgrund der Verarbeitung ihrer personenbezogenen Daten bestehen (nicht zu verwechseln mit den Datenschutz Compliance Risiken, die bei datenschutzrechtlichen Verstößen für das Unternehmen bestehen).

Im Rahmen dieses Fragebogens wird außerdem eine sogenannte DSFA-Schwellwertanalyse durchgeführt. Hierbei wird u. a. anhand vorgeschriebener Fallgruppen ermittelt, ob eine Datenschutz-Folgenabschätzung (DSFA)¹⁸² für die betroffene Verarbeitungstätigkeit durchzuführen ist (vgl. Ziffer 4.12). Bei Verarbeitungstätigkeiten, die voraussichtlich ein hohes Risiko für die betroffenen Personen beinhalten, ist zwingend eine solche DSFA durchzuführen.

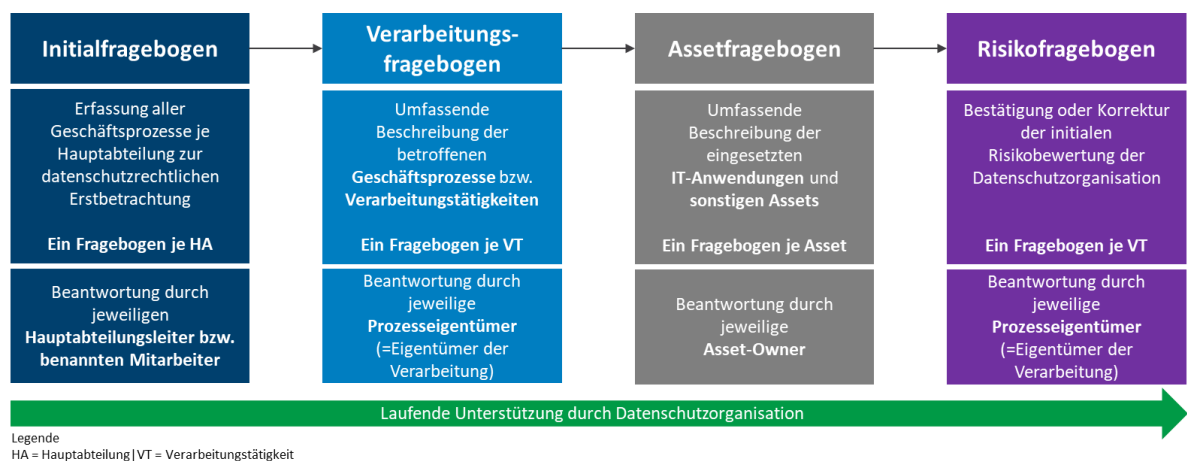
Ausgehend vom identifizierten Risiko sind zudem angemessene technische und organisatorische Maßnahmen (TOMs) mit Blick auf Verarbeitungstätigkeit, Asset und Dienstleister zu ergreifen (vgl. Ziffer 4.11). Die Festlegung angemessener TOMs erfolgt primär in Abstimmung mit der Informations- und IT-Sicherheit.

5.3.2.5 Datenverarbeitungsdienstleister(DVD)-Fragebogen

Für jeden identifizierten Datenverarbeitungsdienstleister (vgl. Ziffer 6) ist zudem ein DVD-Fragebogen durch den Prozesseigentümer (ggf. unter Rückgriff auf den jeweiligen Dienstleister) auszufüllen. Hier werden datenschutzrechtlich relevante Angaben zum Datenverarbeitungsdienstleister abgefragt.

Im Rahmen dieser Fragebögen erfolgt eine Bewertung der Kritikalität der Auftragsverarbeitung.

5.3.2.6 Grafische Kurzdarstellung des Standardprozesses¹⁸³



5.3.3 Dokumentation

Es müssen für jeden Verantwortlichen sowohl sämtliche Verarbeitungstätigkeiten in einer toolgestützten Verarbeitungsbeschreibung als auch Assets in einer toolgestützten Asset-Beschreibung dokumentiert werden. Darüber hinaus müssen alle Datenschutzrisiken je Verarbeitungstätigkeit toolgestützt dokumentiert und bewertet werden. Zudem sind alle Datenverarbeitungsdienstleister, die in seinen Verarbeitungstätigkeiten zum Einsatz kommen, toolgestützt zu dokumentieren.

Die Maßgaben für diese Dokumentation ergeben sich insbesondere aus dem vorherigen Ziffer 5.3.2.

Für die Dokumentation der Verarbeitungstätigkeiten, Assets und Datenverarbeitungsdienstleister sowie Datenschutzrisiken wird ein Tool, Fragebögen sowie geeignete Arbeitshilfen zur Verfügung gestellt.

Bei Fragen zur Dokumentation **können** die *Datenschutz-Koordinatoren* und die *Data Privacy Organization* kontaktiert werden.

5.3.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none"> Dokumentiert alle seine Verarbeitungstätigkeiten in einer toolgestützten Verarbeitungsbeschreibung.

¹⁸² Vgl. Art. 35 DSGVO.

¹⁸³ Der Dienstleisterfragebogen ist an dieser Stelle bewusst ausgeklammert.

Rolle	Verantwortung
	<ul style="list-style-type: none"> ▪ Dokumentiert und bestätigt/korrigiert toolgestützt alle Datenschutzrisiken je Verarbeitungstätigkeit auf Grundlage einer Initialbewertung durch die <i>Data Privacy Organization</i>. ▪ Dokumentiert toolgestützt alle Datenverarbeitungsdienstleister, die in seinen Verarbeitungstätigkeiten zum Einsatz kommen. ▪ Überprüft Geschäftsprozesse, um festzustellen, ob im Zusammenhang mit dem Geschäftsprozess personenbezogene Daten erhoben, verarbeitet, genutzt oder übermittelt werden (vgl. Ziffer 4.3). ▪ Beantwortet die Verarbeitungsfragebögen für seine Verarbeitungstätigkeiten innerhalb einer vorgegebenen, angemessenen Zeit. ▪ Beantwortet den Datenverarbeitungsdienstleister-Fragebogen für alle in seinen Verarbeitungstätigkeiten involvierten Datenverarbeitungsdienstleister innerhalb einer vorgegebenen, angemessenen Zeit. ▪ Bindet bei allen Fragen oder Unklarheiten zur Daten-/ Informations- und/oder IT-Sicherheit (einschließlich technischer und organisatorischer Maßnahmen) die jeweils zuständige <i>Informations- und/oder IT-Sicherheit ein</i>. ▪ Können sich bei Fragen zur Dokumentation an die <i>Datenschutz-Koordinatoren</i> und an die <i>Data Privacy Organization wenden</i>. ▪ Prüft regelmäßig und anlassbezogen, ob Veränderungen an seinen Verarbeitungstätigkeiten vorliegen, die in der Dokumentation (Verarbeitungsbeschreibung, Risikobewertung) entsprechend aufzunehmen sind. ▪ Dokumentiert alle Kontrollmaßnahmen.
Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Dokumentiert alle seine Assets in einer toolgestützten Asset-Beschreibung. ▪ Beantwortet Assetfragebogen für seine Assets innerhalb einer vorgegebenen, angemessenen Zeit beantworten. ▪ Bindet bei allen Fragen oder Unklarheiten zur Daten-/ Informations- und/oder IT-Sicherheit (einschließlich technischer und organisatorischer Maßnahmen) ist die jeweils zuständige <i>Informations- und/oder IT-Sicherheit ein</i>. ▪ Prüft regelmäßig und anlassbezogen, ob Veränderungen an seinen Assets vorliegen, die in der Dokumentation (Asset-Beschreibung) entsprechend aufzunehmen sind. ▪ Dokumentiert alle Kontrollmaßnahmen.
Hauptabteilungsleiter	<ul style="list-style-type: none"> ▪ Dokumentiert alle Geschäftsprozesse in ihrem Verantwortungsbereich. ▪ Dürfen für jeden Geschäftsprozess einen <i>Prozesseigentümer</i> benennen. Dieser Prozesseigentümer muss dokumentiert werden. Benennt der Hauptabteilungsleiter keinen Prozesseigentümer, so muss der Hauptabteilungsleiter die Aufgaben der <i>Prozesseigentümer</i> erfüllen (vgl. Ziffer 3.2.4.6). ▪ Beantwortet den Initialfragebogen innerhalb einer vorgegebenen, angemessenen Zeit (dies kann auch ein von ihm <i>benannter Beschäftigter</i> übernehmen). ▪ Prüft regelmäßig und anlassbezogen, ob neue Geschäftsprozesse oder Änderungen an bestehenden Geschäftsprozessen vorliegen, die zu dokumentieren und der <i>Data Privacy Organization</i> zu melden sind. ▪ Dokumentiert alle Kontrollmaßnahmen.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Unterstützt die <i>Prozesseigentümer</i> und <i>Asset-Eigentümer</i> bei der Dokumentation.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Stellt das Tool, die Fragebögen sowie geeignete Arbeitshilfen zur Verfügung. ▪ Berät die <i>Prozesseigentümer</i> und <i>Asset-Eigentümer</i> bei der Dokumentation. ▪ Prüft regelmäßig und anlassbezogen, ob Anpassungen an der Dokumentation und Bewertung von Verarbeitungstätigkeiten, Assets, Risiken und Datenverarbeitungsdienstleistern erforderlich sind. ▪ Dokumentiert alle Kontrollmaßnahmen.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Unterstützt bei allen Fragen oder Unklarheiten zur Daten-/ Informations- und/oder IT-Sicherheit (einschließlich technischer und organisatorischer Maßnahmen).
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.

Überblick der **Zuständigkeiten** für die Beantwortung der Fragebögen:

Fragebogen	Primäre Zuständigkeit	Alternative Zuständigkeit
Initialfragebogen	Hauptabteilungsleiter	<i>Alternativ:</i> Benannter Beschäftigter
Verarbeitungsfragebogen	Jeweiliger Prozesseigentümer	<i>Sofern nicht benannt:</i> Hauptabteilungsleiter
Assetfragebogen	Jeweiliger Asset-Eigentümer	<i>Sofern nicht benannt:</i> Leiter derjenigen (Haupt-) Abteilung, die das Asset fachlich verantwortet.
Risikofragebogen Bestätigung oder Korrektur der initialen Risikobewertung der Data Privacy Organization	Jeweiliger Prozesseigentümer	<i>Sofern nicht benannt:</i> Hauptabteilungsleiter
Datenverarbeitungsdienstleister (DVD)-Fragebogen	Jeweiliger Prozesseigentümer	<i>Sofern nicht benannt:</i> Hauptabteilungsleiter

6 Datenverarbeitungsdienstleister und gemeinsam Verantwortliche

6.1 Allgemeine Vorgaben

Werden personenbezogene Daten gemeinsam von verschiedenen Verantwortlichen (=Gesellschaften) verarbeitet oder wird eine Datenverarbeitung von einem oder mehreren Verantwortlichen (=Gesellschaften) auf einen Auftragsverarbeiter ausgelagert, so **müssen** durch den *zuständigen Prozess- oder Asset-Eigentümer* geeignete Datenschutzvereinbarungen abgeschlossen werden.

Die Datenverarbeitung liegt aufgrund der Datenmengen und anderer Faktoren zumeist nicht alleine bei dem Unternehmen, welches die Daten letztendlich verwendet. Häufig werden Dienstleister beauftragt, die die Daten erheben und weiterverarbeiten. Beispielsweise haben Unternehmen oft keine eigenen Server, um ihre Webseiten zu hosten. Vielmehr werden Agenturen beauftragt, eine Webseite zu gestalten und diese wiederum beauftragen Anbieter von Rechenzentren, um die Webseite zu hosten. Zudem besteht die Möglichkeit, sich gleich fremder Plattformen zu bedienen, wie z. B. Facebook.

Die DSGVO sieht für solche Konstellationen verschiedene Konstrukte vor, um die Rechte und Pflichten zu verteilen und auch, um die Haftung zu regeln. Zum einen besteht das Konstrukt der „Auftragsverarbeitung“¹⁸⁴, zum anderen das der „Gemeinsamen Verantwortlichkeit“¹⁸⁵. Es ist daher stets erforderlich, zu ermitteln, ob in einer Geschäftsbeziehung eine gemeinsame Verantwortlichkeit oder Auftragsverarbeitung vorliegt. Entsprechend der Bewertung sind weitere formelle Anforderungen zu erfüllen. Dienstleister, die als Auftragsverarbeiter oder gemeinsame Verantwortliche tätig sind, werden vorliegend auch als *Datenverarbeitungsdienstleister* bezeichnet.

Allerdings ist nicht jede Dienstleistungsbeziehung bzw. jeder Datenaustausch mit anderen Unternehmen zwingend als Auftragsverarbeitung oder gemeinsame Verantwortlichkeit anzusehen. Neben diesen beiden Konstrukten kann etwa auch eine reine Datenübermittlung an einen datenschutzrechtlich eigenständigen Verantwortlichen vorliegen (z. B. Übermittlung von Daten an einen Wirtschaftsprüfer, Steuerberater oder Rechtsanwalt). In solchen Fällen sind das datenübermittelnde Unternehmen und das datenempfangende Unternehmen getrennte (eigenständige) Verantwortliche. Für solche reinen Datenübermittlungen bedarf es zwar keiner gesonderten Datenschutzvereinbarung, dafür aber stets einer tauglichen Rechtsgrundlage.

Die genaue Bestimmung des konkreten Datenschutzverhältnisses im Einzelfall ist nicht immer einfach. Bei vielen Beauftragungen von Dienstleistern liegt zugleich eine Auftrags(daten)verarbeitung im datenschutzrechtlichen Sinne vor. Die Auftragsverarbeitung kann dabei nicht ohne Weiteres mit der zugrundeliegenden Dienstleistungsbeziehung gleichgesetzt werden. Vielmehr ist im Einzelfall zu überprüfen, welche Aspekte der Leistungserbringung Gegenstand einer Auftragsverarbeitung darstellen. Diese Elemente sind sodann in einer gesonderten Auftragsverarbeitungsvereinbarung (AVV)¹⁸⁶ zu regeln, die neben oder als Teil der Leistungsvereinbarungen (z. B. Dienstleistungsvertrag) bestehen.

Im Falle einer *gemeinsamen Verantwortlichkeit* ist in einer Vereinbarung über die gemeinsame Verantwortlichkeit (auch *Joint Control Agreement* genannt) insbesondere zu regeln, wer in welcher Weise für die Erfüllung der Pflichten aus der DSGVO (v. a. die Betroffenenrechte) zuständig ist.

6.2 Beauftragung von Auftragsverarbeitern

6.2.1 Einleitung

Sofern eine Auftragsverarbeitung vorliegt, ist sicherzustellen, dass ein Vertrag zur Auftragsverarbeitung (AVV) mit dem Auftragsverarbeiter geschlossen wird, der insbesondere den zahlreichen gesetzlichen Mindestanforderungen¹⁸⁷ genügt.

¹⁸⁴ Vgl. Art. 28 DSGVO.

¹⁸⁵ Vgl. Art. 26 DSGVO.

¹⁸⁶ Auch Auftragsverarbeitungsvertrag oder Vertrag zur Auftragsverarbeitung genannt.

¹⁸⁷ Vgl. Art. 28 DSGVO.

6.2.2 Beschreibung

Die Data Privacy Organization hält hierzu verschiedene Mustervereinbarungen vor. Auftraggeber ist dabei derjenige, der die personenbezogenen Daten an den Auftragnehmer liefert und diesem eine konkrete Weisung erteilt, wie die personenbezogenen Daten zu verarbeiten sind. Weicht der Auftragnehmer von dieser Weisung ab und verwendet die personenbezogenen Daten zu eigenen Zwecken, so wird der Auftragnehmer eigener Verantwortlicher. Die Bestimmung, ob eine Auftragsverarbeitung vorliegt oder nicht, hängt dabei von den tatsächlichen Umständen ab.

6.2.2.1 Auftragsverarbeitung

Zur Erbringung von Leistungen wird häufig auf spezialisierte Dienstleister zurückgegriffen. Beispiele hierfür sind:

- IT-Dienstleistungen,
- „Shared Services“-Dienstleistungen innerhalb eines Konzerns (z. B. Dienstreiseplanung),
- Assistance-Leistungen, wie Empfang oder Sicherheitsdienste.

Die Übernahme derartiger Tätigkeiten durch Dienstleister erfolgt in der Regel durch Auftragsverarbeitung, in einigen Fällen auch durch eigenverantwortlich tätige Dienstleister (Dritte).

Eine Datenübermittlung zur Verarbeitung im Auftrag liegt regelmäßig in den folgenden Konstellationen vor:

- Datenverarbeitung bei Lohn- und Gehaltsabrechnungen,
- Outsourcing personenbezogener Datenverarbeitung im Rahmen von Cloud-Computing,
- Beauftragung eines Callcenters zur Kundenkommunikation,
- Wartungsdienstleistungen, bei denen nicht ausgeschlossen werden kann, dass während der Wartung personenbezogene Daten zur Kenntnis gelangen,
 - Wartung von IT-Systemen,
 - Wartung von Telekommunikations-Anlagen,
- Entsorgung von Akten oder Datenträgern durch externe Unternehmen.

Keine Auftragsverarbeitung liegt z. B. beim Postversand durch die Post oder bei klassischen Bankgeschäften vor. Auch kann aus gesetzlichen Regelungen eine Auftragsverarbeitung ausgeschlossen sein, wie dies z. B. für Steuerberater gilt (§ 11 Steuerberatungsgesetz). Dort wird ausdrücklich vorgegeben, dass Steuerberater weisungsfrei handeln.

Diese Aufzählungen sind nicht abschließend, auch in weiteren Konstellationen kann der Abschluss eines Vertrages zur Auftragsverarbeitung erforderlich sein.

In Zweifelsfällen **muss** der *Data Privacy Officer* oder der *Datenschutzbeauftragte* durch den Einkauf oder beauftragenden Fachbereich miteinbezogen werden.

Wird eine Verarbeitung identifiziert, die ein Auftragsverarbeiter übernehmen soll, ist zunächst gem. Ziffer 5 die Verarbeitungsbeschreibung für die entsprechende Verarbeitung zu erstellen. In diesem Rahmen ist ebenfalls zumindest eine Schutzbedarfs- oder Risikoanalyse gem. Ziffer 4.10 durchzuführen, um risikoadäquat auf Basis des ermittelten Schutzbedarfes technische und organisatorische Maßnahmen mit dem Ziel der Risikoreduzierung für die Verarbeitung festzulegen und vertraglich zu vereinbaren. Bei einem sehr hohen Schutzbedarf oder bei hohen Risiken ist im Vorfeld eine Datenschutz-Folgenabschätzung (DSFA) durchzuführen (siehe Ziffer 4.11.2.4).

Es dürfen nur Auftragsverarbeiter eingesetzt werden, die hinreichend Garantien dafür bieten, dass sie ausreichende technische und organisatorische Maßnahmen für einen zuverlässigen Schutz der Daten bieten.¹⁸⁸ Diese Maßnahmen müssen geeignet sein, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.¹⁸⁹ Bei der Auswahl des Auftragsverarbeiters ist sicherzustellen, dass dieser die festgelegten technischen und organisatorischen Maßnahmen einhält. Hierzu sind im Rahmen einer Ausschreibung die Anforderungen an den Dienstleister zu formulieren und die technischen und organisatorischen Maßnahmen sind mittels einer Checkliste/eines Fragebogens zu erfragen oder ggfs. sogar vorzugeben.

¹⁸⁸ Vgl. Art. 28 Abs. 1 DSGVO.

¹⁸⁹ Vgl. Art. 32 Abs. 1 DSGVO.

Der Auftragsverarbeitungsvertrag **muss** schriftlich oder in elektronischer Form abgeschlossen werden. Für die Verträge zur Auftragsverarbeitung **sind grundsätzlich** die Rheinmetall-Musterverträge als Grundlage zu verwenden und entsprechend durch den beauftragenden Fachbereich auszufüllen.

Die technischen und organisatorischen Maßnahmen sind bezogen auf die Verarbeitung zu beschreiben und als Anlage zum Auftragsverarbeitungsvertrag beizufügen. Die technischen und organisatorischen Maßnahmen sind auf ihre Angemessenheit zu überprüfen. Dies richtet sich insbesondere nach dem Maßnahmenkatalog zu den technischen und organisatorischen Maßnahmen (siehe Ziffer 4.11). Hierfür ist im Regelfall vorab die Informationssicherheit einzubinden.

6.2.2.2 Auftragsverarbeiter aus Drittstaaten

Sofern sich der Auftragsverarbeiter außerhalb der Europäischen Union oder dem Europäischen Wirtschaftsraum befindet, sind weitere Anforderungen zu beachten. Insbesondere ist ein angemessenes Datenschutzniveau zu gewährleisten. Die hierfür geeigneten rechtlichen Instrumente sind in Ziffer 4.7 beschrieben. Der zuständige Data Privacy Officer ist bei entsprechenden Beauftragungen hinzuzuziehen.

Beim Einsatz von Auftragsverarbeitern (einschließlich Unterauftragsverarbeitern) aus Drittstaaten sind im Regelfall zusätzlich die sogenannten EU-Standarddatenschutzklauseln zwischen Datenexporteur und Datenimporteur abzuschließen.

6.2.2.3 Vertragsentwurf des Auftragnehmers

Soweit der Auftraggeber die Unterzeichnung eines eigenen Vertragsmusters oder Änderungen an Rheinmetall Mustervereinbarungen verlangt, ist sicherzustellen, dass dieser Vertrag zuvor Rheinmetall-seitig rechtlich geprüft wurde.

Die Entscheidung über die Unterzeichnung eines Vertragsentwurfs des Auftragnehmers **darf** nur nach Rücksprache mit der *Data Privacy Organization* getroffen werden. Sofern erforderlich, bindet der *Data Privacy Manager* die *Rechtsabteilung* und/oder den *Datenschutzbeauftragten* ein.

6.2.3 Dokumentation

Der Abschluss des Vertrages zur Auftragsverarbeitung ist zu dokumentieren. In dem genutzten Archiv- und/oder Vertragsmanagementsystem sind eine Kopie (z. B. ein Scan) des unterzeichneten Vertrages, die an den Auftragnehmer erteilten Weisungen zum Umgang mit den Daten und eine Liste der eingesetzten Unterauftragsverarbeiter (sofern diese nicht bereits Bestandteil des Vertrages sind), alle von Auftragsverarbeitern erhaltenen Mitteilungen (z. B. über eine Datenschutzverletzung) und ein Protokoll der Überprüfung der getroffenen technischen und organisatorischen Maßnahmen zu hinterlegen.

Der Dienstleister und ggf. etwaige Unterauftragsverarbeiter (z. B. Cloud-Dienstleister, Hoster) sind in die Liste der Empfänger in der Verfahrensbeschreibung (vgl. Ziffer 5) aufzunehmen. Je nach Art der Beauftragung sind die Datenschutzinformationen und Dienstleisterlisten (z. B. im Intranet, Internet oder analog) anzupassen (vgl. Ziffer 4.6).

Dem zuständigen Data Privacy Officer ist mindestens eine digitale Kopie des unterzeichneten Vertrages zur Auftragsverarbeitung unaufgefordert nach Vertragsschluss per E-Mail zu übersenden.

6.2.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer bzw. Asset-Eigentümer i.d.R. Auftraggeber der Dienstleistung	<ul style="list-style-type: none">▪ Ist für den Abschluss von Verträgen zur Auftragsverarbeitung (AVV) und EU-Standarddatenschutzklauseln (SDK) verantwortlich.▪ Schließt geeignete Verträge zur Auftragsverarbeitung (AVV) mit dem Auftragsverarbeiter (Datenverarbeitungsdienstleister) <u>vor Beginn</u> der Verarbeitung durch diesen Dienstleister ab.▪ Führt eine Liste der durch ihn eingesetzten Dienstleister und hält diese aktuell.▪ Steuert den Dienstleister und nimmt die aktive Vertragsverwaltung vor.

Rolle	Verantwortung
	<ul style="list-style-type: none"> ▪ Meldet Änderungen der Dienstleister oder neue Dienstleister an den Datenschutz-Koordinator und der Data Privacy Organization. ▪ Legt die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit bezogen auf eine Verarbeitung fest. ▪ Prüft regelmäßig, ob mit allen Auftragsverarbeitern die erforderlichen vertraglichen Regelungen (angemessene Auftragsverarbeitungsverträge) bestehen und ob die getroffenen technischen und organisatorischen Maßnahmen weiterhin geeignet sind, ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu gehört auch, falls erforderlich, eine Vorortprüfung. ▪ <u>Im Falle von weiteren Kontrollpflichten:</u> Stimmt diese mit der Data Privacy Organization oder dem Datenschutzbeauftragten ab und führt diese ggf. mit diesen gemeinsam durch.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Führt eine ausführliche Dienstleisterliste des Bereichs / der Abteilung und hält diese aktuell.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Stellt geeignete Vertragsmuster bereit und pfl egt diese. ▪ Stellt geeignete Tools zum Vorhalten einer zentralen Dienstleisterliste zur Verfügung und stellt über geeignete Vorgaben sicher, dass diese Dienstleisterliste aktuell ist. ▪ Unterstützt die Informationssicherheit bei Erstellung der Checklisten zu datenschutz-spezifischen Fragen. ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Unterstützt und überprüft die Datensicherheitsmaßnahmen auf Angemessenheit und stellt Vorgaben für geeignete Maßnahmen zur Verfügung. ▪ Stellt geeignete Checklisten/Fragebögen zur Prüfung der Eignung von Datenverarbeitungsdienstleistern bereit.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.¹⁹⁰

6.3 Gemeinsame Verantwortliche

6.3.1 Einleitung

Es ist sicherzustellen, dass bei einer gemeinsamen Verarbeitung vertraglich festgelegt wird, wer von den gemeinsam Verantwortlichen (involvierten Unternehmen) für die Erfüllung der jeweiligen Verpflichtungen aus der DSGVO zuständig ist. Im Falle einer gemeinsamen Verantwortlichkeit legen mindestens zwei Unternehmen die Zwecke und die Mittel der Verarbeitung gemeinsam fest.

Da der Abschluss einer solchen Vereinbarung hohe Anforderungen an die rechtliche Kompetenz stellt und im Einzelfall viel Gestaltungsspielraum besteht, **muss** durch den zuständigen Prozess- oder Asset-Eigentümer der zuständige *Data Privacy Officer*, die *Rechtsabteilung* oder der *Datenschutzbeauftragte* einbezogen werden.

Ein **Beispiel** für eine gemeinsame Verantwortlichkeit sind die sogenannten Facebook-Fanpages¹⁹¹ (z. B. eine Unternehmensauftritt auf Facebook). Aufgrund von gewissen Einstellungen, die der Fanpage-Betreiber (das Unternehmen) durchführt, legt dieser die Mittel und Zwecke gemeinsam mit Facebook (Betreiber der Social-Media-Plattform) fest. Gleichzeitig führt ein Fanpage-Betreiber die Internetnutzer auf Facebook, sodass Facebook zudem eigene Mittel und Zwecke verfolgen kann.

¹⁹⁰ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

¹⁹¹ Für Facebook-Fanpages wurde dies bereits gerichtlich vom EuGH entschieden. Gleiches dürfte allerdings auch für ähnliche Social-Media-Unternehmenspräsenzen gelten.

6.3.2 Beschreibung

Der Prozess **muss** durchgeführt werden, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel für eine Verarbeitung festlegen bzw. entscheiden.¹⁹²

Dies kann beispielsweise der Fall sein, wenn zwei oder mehrere gemeinsam Verantwortliche die Festlegung der Zwecke und Mittel zur Verarbeitung beabsichtigen. Dies trifft aber auch dann regelmäßig zu, wenn mehrere Unternehmen im Rheinmetall Konzern eine Verarbeitung oder ein technisches Verfahren (Asset) gemeinsam nutzen. In diesem Fall müssen die gemeinsam Verantwortlichen eine schriftliche Vereinbarung (sogenanntes *Joint Control Agreement*) treffen, die bestimmt, wer von ihnen welche Verpflichtungen der DSGVO erfüllt. Insbesondere muss geregelt werden, wer für die Wahrnehmung der Betroffenenrechte und der Informationspflichten zuständig ist. Die Vereinbarung muss in transparenter Form verfasst sein, d. h. für die gemeinsam Verantwortlichen sowie für die betroffene Person müssen aus der Vereinbarung die jeweiligen Zuständigkeiten klar erkennbar hervorgehen.¹⁹³

Die Vereinbarung muss die jeweils zugewiesenen tatsächlichen Funktionen und Beziehungen der gemeinsam Verantwortlichen gegenüber den betroffenen Personen gebührend widerspiegeln. Dabei ist mit tatsächlichen Funktionen die Aufgabenverteilung zwischen den gemeinsam Verantwortlichen und die jeweilige Entscheidungsbefugnis bezüglich der Festlegung der Zwecke und Mittel der Verarbeitung gemeint, während bei der Beziehung die Aufgabenverteilung hinsichtlich gesetzlicher Pflichten, die gegenüber der betroffenen Person zu erfüllen sind, darzustellen ist. Insgesamt sind die tatsächlichen Gegebenheiten detailliert zu beschreiben.¹⁹⁴

6.3.3 Dokumentation

Der Abschluss der Vereinbarung über die gemeinsame Verantwortlichkeit (Joint Control Agreement) ist zu dokumentieren. In dem genutzten Archiv- und/oder Vertragsmanagementsystem sind eine Kopie (z. B. ein Scan) der unterzeichneten Vereinbarung und alle vom gemeinsamen Verantwortlichen erhaltenen Mitteilungen (z. B. über eine Datenschutzverletzung zu hinterlegen.

Der andere gemeinsam Verantwortliche (z. B. der Dienstleister, die andere Konzerngesellschaft) ist in die Liste der Empfänger in der Verfahrensbeschreibung (vgl. Ziffer 5) aufzunehmen. Je nach Einzelfall sind die Datenschutzinformationen und Dienstleisterlisten (z. B. im Intranet, Internet oder analog) anzupassen (vgl. Ziffer 4.6).

Dem zuständigen Data Privacy Officer muss mindestens eine digitale Kopie der unterzeichneten Vereinbarung über die gemeinsame Verantwortlichkeit (Joint Control Agreement) unaufgefordert nach Vertragsschluss per E-Mail übersendet werden.

6.3.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer bzw. Asset-Eigentümer i.d.R. Auftraggeber der Dienstleistung	<ul style="list-style-type: none"> ▪ Ist für die Vereinbarung verantwortlich. ▪ Schließt geeignete Datenschutzvereinbarungen mit den übrigen gemeinsam Verantwortlichen <u>vor Beginn</u> der Verarbeitung ab. ▪ Stellt sicher, dass eine Vereinbarung geschlossen wird, die mindestens beschreibt, welche Parteien für welche Datenschutzaufgaben verantwortlich sind (insbesondere wer welchen Informationspflichten nachkommt und wer für die Wahrung/Erfüllung der Rechte der betroffenen Personen zuständig ist). ▪ Dokumentiert den Abschluss der Vereinbarung über die gemeinsame Verantwortlichkeit (Joint Control Agreement). ▪ Nimmt den anderen gemeinsam Verantwortlichen (z. B. der Dienstleister, die andere Konzerngesellschaft) in die Liste der Empfänger in der Verfahrensbeschreibung (vgl. Ziffer 5) auf.

¹⁹² Nach jüngster Entscheidungen des EuGH unterstehen z. B. Unternehmensseiten auf Facebook („Fanpages“) einer gemeinsamen Verantwortlichkeit zwischen Facebook und dem jeweiligen Unternehmen.

¹⁹³ Vgl. Art. 26 Abs. 1 DSGVO.

¹⁹⁴ Vgl. Art. 26 Abs. 2 DSGVO.

Rolle	Verantwortung
	<ul style="list-style-type: none"> ▪ Macht die wesentlichen Inhalt der Vereinbarung der betroffenen Person auf Anfrage zugänglich.¹⁹⁵ ▪ Bindet den zuständigen Data Privacy Officer, die Rechtsabteilung oder den Datenschutzbeauftragten rechtzeitig ein. ▪ Übersendet dem zuständigen Data Privacy Officer mindestens eine digitale Kopie der unterzeichneten Vereinbarung über die gemeinsame Verantwortlichkeit (Joint Control Agreement) unaufgefordert nach Vertragsschluss per E-Mail. ▪ Prüft regelmäßig, ob mit allen Auftragsverarbeitern die erforderlichen vertraglichen Regelungen (angemessene Auftragsverarbeitungsverträge) bestehen und ob die getroffenen technischen und organisatorischen Maßnahmen weiterhin geeignet sind, ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu gehört auch, falls erforderlich, eine Vorortprüfung. ▪ Leitet Betroffenenanfragen an den zuständigen Verantwortlichen weiter. ▪ Prüft regelmäßig, ob eine Sachlage vorliegt, aufgrund derer eine Vereinbarung einer gemeinsam Verantwortlichen getroffen werden muss. ▪ Prüft regelmäßig, ob die Voraussetzungen für die Vereinbarung einer gemeinsamen Verantwortlichkeit noch vorliegen und ob er seine Zuständigkeitsbereiche gemäß der Vereinbarung ordnungsgemäß erfüllt bzw. erfüllen kann. ▪ Führt je nach Vertragsabrede weitere Kontrollpflichten in Bezug auf die Erfüllung der Pflichten der anderen Verantwortlichen durch. ▪ <u>Im Falle von weiteren Kontrollpflichten:</u> Stimmt diese mit der Data Privacy Organization oder dem Datenschutzbeauftragten ab und führt diese ggf. mit diesen gemeinsam durch.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.¹⁹⁶

6.4 Tätigwerden als Auftragsverarbeiter

6.4.1 Einleitung

Wird ein Unternehmen im Rheinmetall Konzern als Auftragnehmer tätig und verarbeitet personenbezogene Daten im Auftrag eines Dritten (z. B. andere Konzerngesellschaft, externer Geschäftspartner), muss ein Vertrag zur Auftragsverarbeitung (AVV) mit diesem Dritten (Auftraggeber) abgeschlossen werden, der den zahlreichen gesetzlichen Mindestanforderungen entspricht.¹⁹⁷ Dies kann schriftlich oder in elektronischer Form erfolgen.

Dies ist regelmäßig bei konzerninternen Dienstleistungen der Fall, bei dem ein Konzernunternehmen für ein anderes Konzernunternehmen Verarbeitungsleistungen übernimmt (z. B. bei Shared Service wie dem Recruiting Center oder der Gehaltsabrechnung).

6.4.2 Beschreibung

Die *Data Privacy Organization* hält hierzu verschiedene Mustervereinbarungen vor. Auftraggeber ist dabei derjenige, der die personenbezogenen Daten an den Auftragnehmer liefert und diesem eine konkrete Weisung erteilt, wie die personenbezogenen Daten zu verarbeiten sind (z. B. Konzerngesellschaft A beauftragt die Payroll-Abteilung einer anderen Konzerngesellschaft B mit der Lohnabrechnung). Weicht der Auftragnehmer von dieser Weisung ab und verwendet die personenbezogenen Daten zu eigenen Zwecken, so wird der Auftragnehmer eigener Verantwortlicher. Die Bestimmung, ob eine Auftragsverarbeitung vorliegt oder nicht, hängt dabei von den tatsächlichen Umständen ab.

¹⁹⁵ Vgl. Art. 26 Abs. 2 S. 2 DSGVO.

¹⁹⁶ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

¹⁹⁷ Vgl. Art. 28 DSGVO.

6.4.2.1 Beauftragung

Bei der Beauftragung eines Unternehmens im Rheinmetall Konzern als Auftragnehmer muss ein Vertrag zur Auftragsverarbeitung schriftlich oder elektronisch abgeschlossen werden. Hierbei sind stets die Rheinmetall Mustervereinbarungen als Grundlage zu verwenden und entsprechend auszufüllen.

Soll ein Unternehmen im Rheinmetall Konzern als Auftragsverarbeiter eingesetzt werden, müssen hinreichende Garantien dafür geboten werden, dass ausreichende technische und organisatorische Maßnahmen für einen zuverlässigen Schutz der Daten bestehen.¹⁹⁸ Diese Maßnahmen müssen geeignet sein, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.¹⁹⁹

Als Basis dient u. a. die während der Erstellung der Verarbeitungsbeschreibung (vgl. Ziffer 5) erstellte Schutzbedarfsanalyse. Diese ist grundsätzlich vom Auftraggeber, aber mindestens gemeinsam zwischen Auftragnehmer und Auftraggeber durchzuführen. Die Anforderungen an geeignete technische und organisatorische Maßnahmen kommen vom Auftraggeber. Die Festlegung geeigneter technischer und organisatorischer Maßnahmen erfolgt gemeinsam. Hierbei ist der Maßnahmenkatalog zu den technischen und organisatorischen Maßnahmen zu berücksichtigen (vgl. Ziffer 4.11).

Im Falle von konzerninternen Verarbeitung (d. h. ein Konzernunternehmen ist Auftraggeber und das andere Konzernunternehmen ist Auftragnehmer der Verarbeitung) erstellt grundsätzlich der Auftragnehmer die Verarbeitungsbeschreibung und legt abhängig vom Risiko und Stand der Technik geeignete technische und organisatorische Maßnahmen fest. Der Auftraggeber prüft lediglich die Geeignetheit der Maßnahmen.

Außerdem sind zusätzlich stets die in dem Vertrag zur Auftragsverarbeitung enthaltenen Regelungen zu beachten.

6.4.2.2 Vertragsentwurf des Auftragnehmers

Soweit der Auftraggeber die Unterzeichnung eines eigenen Vertragsmusters oder Änderungen an der Rheinmetall Mustervereinbarung verlangt, ist sicherzustellen, dass diese Vereinbarung zuvor rechtlich geprüft wurde.

Die Entscheidung über die Unterzeichnung eines solchen Vertrages **darf nur** nach Rücksprache mit der *Data Privacy Organization* getroffen werden. Sofern erforderlich, bindet die *Data Privacy Organization* die *Rechtsabteilung* und/oder den *Datenschutzbeauftragten* ein.

6.4.3 Dokumentation

Der Abschluss des Vertrages zur Auftragsverarbeitung ist zu dokumentieren. In dem genutzten Archivsystem sind eine Kopie (z. B. ein Scan) des unterzeichneten Vertrages, die an den Auftragnehmer erteilten Weisungen zum Umgang mit den Daten, eine Liste von Unterauftragsverarbeitern (sofern diese nicht bereits Bestandteil des Vertrages sind), alle an den Auftraggeber versandten Mitteilungen (z. B. über eine Datenschutzverletzung) und ggfs. ein Protokoll der Überprüfung der getroffenen technischen und organisatorischen Maßnahmen zu hinterlegen.

6.4.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer bzw. Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Ist für den Abschluss von Verträgen zur Auftragsverarbeitung (AVV) und EU-Standarddatenschutzklauseln (SDK) verantwortlich. ▪ <u>Hinweis bei konzerninternen Beauftragungen (insbesondere bei Shared Services):</u> Der für die Dienstleistung zuständige Prozesseigentümer kann den Abschluss der erforderlichen Vereinbarungen mit den Konzerngesellschaften veranlassen. ▪ Schließt geeignete Verträge zur Auftragsverarbeitung (AVV) mit dem Auftragsverarbeiter (Datenverarbeitungsdienstleister) <u>vor Beginn</u> der Verarbeitung durch diesen Dienstleister ab. ▪ Führt eine Liste der durch ihn eingesetzten Dienstleister und hält diese aktuell. ▪ Steuert den Dienstleister und nimmt die aktive Vertragsverwaltung vor. ▪ Stellt sicher, dass die Anforderungen aus der Vereinbarung umgesetzt werden.

¹⁹⁸ Vgl. Art. 28 Abs. 1 DSGVO.

¹⁹⁹ Vgl. Art. 32 Abs. 1 DSGVO.

Rolle	Verantwortung
	<ul style="list-style-type: none"> ▪ Meldet Änderungen der Dienstleister oder neue Dienstleister an den Datenschutz-Koordinator und an die Data Privacy Organization. ▪ Legt die erforderlichen technischen und organisatorischen Maßnahmen zur Datensicherheit bezogen auf eine Verarbeitung fest. ▪ Prüft regelmäßig, ob mit allen Auftragsverarbeitern die erforderlichen vertraglichen Regelungen (angemessene Auftragsverarbeitungsverträge) bestehen und ob die getroffenen technischen und organisatorischen Maßnahmen weiterhin geeignet sind, ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Dazu gehört auch, falls erforderlich, eine Vorortprüfung.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Stellt geeignete Mustervereinbarungen bereit und pflegt diese. ▪ Unterstützt Informationssicherheit bei Erstellung der Checklisten zu datenschutzspezifischen Fragen. ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Unterstützt und überprüft die Datensicherheitsmaßnahmen auf Angemessenheit und stellt Vorgaben für geeignete Maßnahmen zur Verfügung. ▪ Hält eine regelmäßig aktualisierte Liste der technischen und organisatorischen Maßnahmen bezogen auf die Datenverarbeitungen durch den Rheinmetall Konzern vor.²⁰⁰ ▪ Stellt geeignete Checklisten/Fragebögen zur Prüfung der Eignung von Datenverarbeitungsdienstleistern bereit.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.²⁰¹

²⁰⁰ Die technischen und organisatorischen Maßnahmen sind im Einzelnen, bezogen auf die relevanten Kontrollen/Maßnahmen (Zutrittskontrolle, Zugriffskontrolle etc.), durch die durchführenden Stellen bei Rheinmetall zu pflegen (bspw. IT-Betrieb, Unternehmenssicherheit oder Facility Management). Aktualisierungen sind an die *Informationssicherheit* zu melden.

²⁰¹ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

7 Betroffenenrechte

7.1 Gestaltung des Prozesses bei Rheinmetall

7.1.1 Management von Betroffenenrechte-Anfragen

7.1.1.1 Identifikation der Anfrage einer betroffenen Person und des Verantwortlichen

Betroffene Personen können einen Antrag auf Geltendmachung ihrer Rechte sowohl telefonisch, postalisch, per Fax, per elektronischer Post (E-Mail) als auch persönlich stellen. Es ist keine besondere Form zur Antragstellung vorgeschrieben, weshalb Anträge betroffener Personen grundsätzlich über alle Kanäle angenommen und bearbeitet werden müssen.

Die *Beschäftigten* **müssen** die Anträge betroffener Personen ernst nehmen und diese zur Bearbeitung annehmen. Zudem **müssen** die *Beschäftigten* die betroffene Person und den zuständigen Verantwortlichen identifizieren.

Des Weiteren muss die betroffene Person ihre Rechte nicht genau bezeichnen, so dass entsprechende Anträge auszulegen sind und im Zweifel davon auszugehen ist, dass die betroffene Person ihre Rechte geltend machen möchte. Regelmäßig finden sich Vorlagen im Internet, um den Auskunftsanspruch nach den Artt. 15 ff. DSGVO geltend machen zu können. Eine solche Vorlage wird u.a. von der Verbraucherzentrale zur Verfügung gestellt. Da diese Muster den Gesetzeswortlaut wiederholen, sind diese gut geeignet, um sich einen Überblick über die herauszugebenden Daten zu verschaffen.

Ist der Adressat der Anfrage nicht der zuständige Verantwortliche, **muss** durch die *federführende Kontaktstelle* zunächst eine Freigabe zur Weitergabe der Anfrage an den zuständigen Verantwortlichen von der betroffenen Person eingeholt werden.

Sofern die Freigabe nicht durch die betroffene Person erteilt wird und es sich nicht um den zuständigen Verantwortlichen handelt, ist eine Negativauskunft zu erteilen und an den zuständigen Verantwortlichen zu verweisen.

Nachfolgende Besonderheiten sind jeweils bei der Identifikation eines Antrags einer betroffenen Person zu beachten:

7.1.1.2 Besonderheit: Persönliche Antragsstellung

Macht die betroffene Person ihre Rechte persönlich vor Ort geltend, so ist die Identität der betroffenen Person beispielsweise durch Vorlage eines geeigneten Ausweispapiers festzustellen. Dies gilt nicht, sofern sich die betroffene Person beispielsweise per E-Mail-Adresse zu einem Newsletter angemeldet hat, da eine Zuordnung von Person zu E-Mail-Postfach üblicherweise nicht in dieser Form vorgenommen wird. Im Rahmen dessen sind Name, Vorname, Geburtsdatum und Anschrift der Person schriftlich zu erfassen. Hierzu sollte die Musterdokumentation zu Betroffenenanfragen verwendet werden.

7.1.1.3 Besonderheit: Antrag per Telefon

Stellt eine betroffene Person einen Antrag telefonisch, so ist sie darauf aufmerksam zu machen, dass eine telefonische Auskunft nicht möglich ist. Eine angemessene Identifizierung der betroffenen Person ist hier nur sehr schwer möglich, zudem hat Rheinmetall hierzu keine geeigneten Verfahren implementiert. Daher ist die betroffene Person auf die schriftliche Antragsstellung hinzuweisen.

7.1.1.4 Besonderheit: Postalischer Antrag

Erfolgt die Antragstellung postalisch, ist das Datum des Posteingangs auf dem Schreiben zu vermerken (z. B. Posteingangsstempel). Das mit einem Posteingangsstempel versehene Schreiben ist anschließend mit einzuscannen und an die Data Privacy Organization sowie die federführende Kontaktstelle weiterzuleiten.

7.1.1.5 Besonderheit: Antrag per E-Mail

Macht die betroffene Person ihre Rechte per E-Mail geltend, so hat der Empfänger die E-Mail an die *Data Privacy Organization* und an die *federführende Kontaktstelle* weiterzuleiten. Die federführende Kontaktstelle hat den

Eingang der E-Mail geeignet zu dokumentieren (beispielsweise durch Speicherung in einem gesonderten Ordner). Kommt der Antrag von der bei Rheinmetall über die betroffene Person dokumentierten Email-Adresse, so dient diese Email-Adresse bei Anträgen, die keine sensiblen personenbezogenen Daten umfassen, als ausreichendes Identifikationsmerkmal.

7.1.2 Umgang mit Anträgen betroffener Personen

Im Umgang mit Anträgen betroffener Personen ist insbesondere die Prozessdarstellung zum Umgang mit Anträgen betroffener Personen zu beachten.

Im Einzelnen sind nachfolgende Punkte besonders zu beachten:

7.1.2.1 Fristennotierung

Die Betroffenenrechte unterliegen einer Frist.²⁰² Grundsätzlich ist die Anfrage „unverzüglich“ zu bearbeiten, spätestens jedoch innerhalb eines Monats. Die Unverzüglichkeit richtet sich auch nach der vorhandenen Datenmenge, die zunächst ermittelt werden muss. Die Höchstfrist von einem Monat ist dann auszuschöpfen, wenn die Datenbestände über die betroffene Person sehr umfangreich sind und die Beschaffung nicht ohne weiteres durchzuführen ist. Technische Maßnahmen sind zu treffen, um die Datenbeschaffung zu unterstützen. Die Data Privacy Organization erhält stets eine Benachrichtigung, wann der Antrag eingegangen ist und notiert in der Meldung eine Frist von einem Monat. Diese Frist wird der federführenden Kontaktstelle mitgeteilt (sollte das Fristende auf Samstag, Sonntag oder einen Feiertag fallen, gilt der nächste Arbeitstag als Ende der Monatsfrist). Fristbeginn ist der Tag, an dem der Antrag an den zuständigen Verantwortlichen gestellt wurde.

Die *Data Privacy Organization* muss die Höchstfrist in seiner Dokumentation notieren.

Grundsätzlich muss der Fachbereich als federführende Kontaktstelle die Bearbeitung von Anträgen vornehmen, der für die Betroffenenkategorie allgemein zuständig ist.

Das wären grundsätzlich für Beschäftigte der Personalbereich, für Lieferanten/Dienstleister der Einkauf, für Kunden der Vertrieb und für Adressaten von Werbung oder die Webseitenbesucher das Marketing.

Sollten die Datenmengen und die Datenbeschaffung zu umfangreich sein, um die Auskunftspflicht zu erfüllen, so kann die Monatsfrist verlängert werden. Dies erfordert allerdings eine entsprechende Begründung.

7.1.2.2 Unmittelbare Weiterleitung des Antrags an die Data Privacy Organization

Wird ein Antrag als Geltendmachung der Rechte einer betroffenen Person identifiziert, so hat der Beschäftigte, der den Antrag erhalten bzw. identifiziert hat, den Antrag (als Scan oder Weiterleitung der E-Mail) an die Data Privacy Organization und die federführende Kontaktstelle per E-Mail mit Betreff „WAHRNEHMUNG BETROFFENENRECHTE + DATUM“ weiterzuleiten.

Ergänzende Informationen sowie die Kontaktdaten des Data Privacy Managers bzw. Data Privacy Officers sind geeignet bekannt zu machen.

Sofern der *Data Privacy Manager* den Antrag erhält, hat dieser den Data Privacy Officer unverzüglich über den Eingang eines Antrags auf Geltendmachung der Betroffenenrechte zu informieren.

Die *Beschäftigten* müssen Anfragen betroffener Personen an die *Data Privacy Organization* und an die federführende Kontaktstelle weiterleiten.

7.1.2.3 Koordination und Einbeziehung der Fachbereiche

Die federführende Kontaktstelle dokumentiert den Erhalt des weitergeleiteten Antrags gemäß der Musterdokumentation zu Betroffenenanfrage und teilt dem Antragssteller (der betroffenen Person) nach Rücksprache mit der Data Privacy Organization den Eingang und dessen Bearbeitungsstand mit. Grundsätzlich sollte hierbei das Kommunikationsmittel der E-Mail gewählt werden, auch dann, wenn eine Kopie der Daten angefordert wird.

²⁰² Vgl. Art. 12 Abs. 3 DSGVO.

(diese sind in Form von PDF-Dokumenten mit geeignetem Zugriffsschutz bereitzustellen, z. B. durch Verschlüsselung mittels Cryptshare). Bei ausdrücklicher Anfrage auf dem Postweg ist dieser zu wählen und ggf. – sofern nicht vorhanden – die Anschrift zu erfragen.

Zuständig für die Beantwortung und Dokumentation ist die *federführende Kontaktstelle* (der für die Betroffenengruppe allgemein zuständige Fachbereich).

Soweit eine Identifikation des Antragstellers durch Empfänger des Antrags nicht eindeutig möglich ist (z.B. die E-Mail-Adresse lautet anonymous1234@anbieter.de und Frau Lieschen Müller bittet um Auskunft zu dieser E-Mail-Adresse), führt die federführende Kontaktstelle in Abstimmung mit der Data Privacy Organization ergänzende Maßnahmen zur Identifikation des Antragstellers durch. Eine Erfüllung der Betroffenenrechte kann erst nach Identifizierung der betroffenen Person und des zuständigen Verantwortlichen erfolgen.

Der Data Privacy Manager sollte den Datenschutzbeauftragten und den zuständigen Data Privacy Officer über den Eingang eines Antrags informieren.

Die *federführende Kontaktstelle* **muss** den Erhalt des Antrages dokumentieren und der betroffenen Person in geeigneter Weise antworten. Außerdem **muss** die federführende Kontaktstelle in Abstimmung mit der *Data Privacy Organization* ggf. weitergehende Identifikationsmaßnahmen durchführen.

Der *Data Privacy Manager* **sollte** –sofern vorhanden- den *Datenschutzbeauftragten* und *Data Privacy Officer* über den Eingang eines Antrages informieren.

Zur Beantwortung des Antrags der betroffenen Person werden mindestens folgende Fachbereiche eingebunden:

- Personalabteilung
- IT-Abteilung
- Fachbereich, dem gegenüber die Rechte der betroffenen Person geltend gemacht wurden.

Daneben kann es notwendig sein, dass weitere Fachbereiche eingebunden werden müssen, soweit im Rahmen der Bearbeitung des Antrags der betroffenen Person festgestellt wird, dass Datenübermittlungen / Datenweitergaben auch zu anderen Fachbereichen stattgefunden haben.

Ein Rückgriff auf die im Verzeichnis der Verarbeitungstätigkeiten geführten Verfahren zur Ermittlung weiterer involvierter Fachbereiche ist jederzeit möglich.

7.1.2.4 Beantwortung Antrag betroffener Person

Die Fachbereiche sind nach Einbeziehung durch die federführende Kontaktstelle oder die Data Privacy Organization zur Bereitstellung der ihren Fachbereich betreffenden Informationen zur Erfüllung des Antrags der betroffenen Person verantwortlich.

Die Prozess- und Asset-Eigentümer haben geeignete Maßnahmen zu ergreifen, damit den Rechten der betroffenen Person entsprochen werden kann. Zudem hat der Prozesseigentümer die ordnungsgemäße Erfüllung eines Betroffenenantrags sicherzustellen.

Im Einzelnen:

Zunächst ist durch die Personalabteilung festzustellen, ob es sich bei dem Antragsteller um einen derzeitigen oder ehemaligen Beschäftigten handelt.

Handelt es sich um einen (ehemaligen) Beschäftigten, so ist der Fachbereich, in welchem der Beschäftigte tätig war, durch die Personalabteilung als federführende Kontaktstelle oder die Data Privacy Organization zwingend einzubinden.

Die eingebundenen Fachbereiche identifizieren Verarbeitungstätigkeiten und die zur Durchführung der Verarbeitungstätigkeit unterstützenden Mittel (Assets wie beispielsweise IT-Anwendungen, Datenbanken), bei welchen Daten des Antragstellers verarbeitet werden / wurden und melden diese an die federführende Kontaktstelle (Personalabteilung) und an die Data Privacy Organization. Hierzu kann auf die bereitgestellten Vorlagen zurückgegriffen werden.

Zusätzlich muss seitens der Personalabteilung eine Kopie aller in der Personalverwaltungssoftware gespeicherten, personenbezogenen Daten bereitgestellt werden. Gleiches gilt für personenbezogene Daten, die im Zusammenhang mit der Betrieblichen Altersversorgung verarbeitet werden/wurden.

Die IT-Abteilung teilt Autorisierungen / Deautorisierung des Antragstellers bei zentral verwalteten IT-Systemen mit und prüft entsprechende IT-Systeme daraufhin, welche Daten zum Antragsteller in den IT-Systemen verarbeitet werden/wurden.

Soweit der Antragsteller nicht als (ehemaliger) Beschäftigter identifiziert wird und auch keine Zuordnung anhand des Anschreibens zu einem Fachbereich möglich ist, hat die IT-Abteilung alle Datenbank-Systeme nach den personenbezogenen Daten des Antragstellers zu durchsuchen und das Ergebnis der Überprüfung an die Data Privacy Organization zurückzumelden.

Anschließend sind, je nach geltend gemachtem Recht, die notwendigen Maßnahmen zur Erfüllung der Betroffenenanfrage in Abstimmung mit dem Data Privacy Organization oder Datenschutzbeauftragten zu treffen. Dies kann sowohl die Bereitstellung von Informationen zur Datenverarbeitung, die Berichtigung und/oder Löschung von Daten als auch etwas Anderes sein (siehe Ziffer 7.2 bis 7.7).

Der jeweilige Fachbereich ist für die Durchführung bzw. Umsetzung der Maßnahme(n) verantwortlich.

7.1.2.5 Erfüllung des Antrags der betroffenen Person

Nach Bereitstellung der notwendigen Informationen durch die Fachbereiche und Umsetzung geeigneter Maßnahmen zur Erfüllung der jeweiligen Rechte der betroffenen Person bereitet die federführende Kontaktstelle das jeweilige Antwortschreiben in Abstimmung mit der Data Privacy Organization vor und stellt dieses dem Datenschutzbeauftragten zur Kenntnisnahme zur Verfügung.

Die Ausfertigung und den Versand des Antwortschreibens stellt die federführende Kontaktstelle in Abstimmung mit der Data Privacy Organization sicher.

Wurde der Antrag von der betroffenen Person elektronisch gestellt, so erfolgt die Beantwortung durch ein geeignetes verschlüsseltes Verfahren, soweit eine eindeutige Zuweisung der verwendeten E-Mail-Adresse zum Antragsteller möglich ist. In allen anderen Fällen erfolgt die Beantwortung per Briefversand als Einschreiben (Einwurf).

7.1.2.6 Dokumentation

Anträge und Reaktionen auf die Anträge sind zur Abwehr von Rechtsansprüchen und zur Erfüllung der gesetzlichen Nachweispflichten in der Dokumentation zur Betroffenenengruppe drei Jahre aufzubewahren.

Die Unterlagen sind zudem der Data Privacy Organization zuzusenden.

7.1.3 Rollen und Verantwortung

Rolle	Verantwortung
Beschäftigter	<ul style="list-style-type: none">▪ Kennt die Rechte betroffener Personen.▪ Kann Anträge betroffener Personen identifizieren.▪ Leitet Anträge betroffener Personen unmittelbar an die Data Privacy Organization weiter.▪ Unterstützt als Beschäftigter des Fachbereichs bei der Erfüllung von Betroffenenrechten.
Federführende Kontaktstelle der jeweiligen Betroffenenengruppe	<ul style="list-style-type: none">▪ Dokumentiert Betroffenenanfragen in geeigneter Weise.▪ Konsolidiert Rückmeldungen der Prozesseigentümer zur Erfüllung des Antrags.▪ Fertigt Antwortschreiben an und stellt - soweit erforderlich - den Versand sicher.▪ Informiert die Data Privacy Organization nach Eingang von Betroffenenanfragen.▪ Informiert die Data Privacy Organization über den Fortschritt der Erfüllung des Antrags.
Data Privacy Officer	<ul style="list-style-type: none">▪ Unterstützt bei allen Fragen im Zusammenhang mit der Erfüllung der Betroffenenrechte.▪ Definiert Prozess zum Umgang mit Betroffenenanfragen.▪ Stellt Implementierung des Prozesses zum Umgang mit Betroffenenanfragen und Schulung der Beschäftigten sicher.

Rolle	Verantwortung
	<ul style="list-style-type: none"> ▪ Nimmt das Vorhandensein eines Antrags auf Geltendmachung von Rechten einer betroffenen Person sowie deren Bearbeitungsstand in den Compliance Monatsbericht auf. ▪ Informiert Datenschutzbeauftragten nach Eingang von Betroffenenanfragen.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Unterstützt den Fachbereich im Zusammenhang mit der Erfüllung der Betroffenenrechte. ▪ Dokumentiert Betroffenenanfragen in geeigneter Weise. ▪ Prüft Antrag der betroffenen Person auf Plausibilität. ▪ Teilt betroffener Person Eingang und Stand der Bearbeitung mit. ▪ Überprüft in geeigneter Weise die Identität der betroffenen Person (soweit notwendig). ▪ Leitet Antrag betroffener Person an die Prozesseigentümer zur Prüfung und Rückmeldung weiter. ▪ Unterstützt die Prozesseigentümer bei der Ermittlung der Daten zu betroffener Person. ▪ Informiert Data Privacy Officer nach Eingang von Betroffenenanfragen. ▪ Informiert Data Privacy Officer über Fortschritt der Erfüllung des Antrags. ▪ Stellt geeignete Hilfsmittel zur Verfügung.
Datenschutzbeauftragter²⁰³	<ul style="list-style-type: none"> ▪ Berät die Data Privacy Organization und den Prozesseigentümer hinsichtlich der Erfüllung der Rechte betroffener Personen. ▪ Überprüft regelmäßig den Prozess zum Umgang mit Betroffenenrechten. ▪ Wirkt bei aufsichtsbehördlichen Verfahren in Zusammenhang mit Beschwerden betroffener Personen mit.
Prozesseigentümer bzw. Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Prüft, ob personenbezogene Daten zu Antragsteller vorhanden sind. ▪ Meldet Ergebnis zurück <ul style="list-style-type: none"> – Soweit personenbezogene Daten vorhanden: <ul style="list-style-type: none"> ➔ Meldet konkrete Daten und Zwecke der Datenverarbeitung. – Soweit keine personenbezogenen Daten vorhanden: <ul style="list-style-type: none"> ➔ Teilt mit, dass keine personenbezogenen Daten zum Antragsteller vorhanden sind. ▪ Erfüllt die Rechte der betroffenen Person in Abstimmung mit der Data Privacy Organization. ▪ Stellt die ordnungsgemäße Erfüllung der Rechte der betroffenen Person für seinen Verantwortungsbereich sicher. ▪ Stellt notwendige Ressourcen zur Erfüllung der Rechte der betroffenen Person zur Verfügung. ▪ Prüft regelmäßig, ob ausreichende technische und organisatorische Maßnahmen zur Erfüllung der Betroffenenrechte getroffen wurden, durch die eine Geltendmachung in geeigneter Form erfolgen kann.
IT-Abteilung	<ul style="list-style-type: none"> ▪ Unterstützt die Fachbereiche bei der Identifikation personenbezogener Daten zur betroffenen Person in IT-Systemen. ▪ Unterstützt und recherchiert bei notwendiger Einbindung des IT-Dienstleisters. ▪ Unterstützt bei der Umsetzung der Rechte der betroffenen Person in Abstimmung mit der Data Privacy Organization. ▪ Meldet konkrete personenbezogene Daten betroffener Person und Zwecke der Datenverarbeitung zurück.
Geschäftsführung	<ul style="list-style-type: none"> ▪ Stellt der Data Privacy Organization Mittel zur Erfüllung der Anforderungen zur Verfügung. ▪ Stellt sicher, dass involvierte Hauptabteilungen ihrer Verpflichtung nachkommen.

²⁰³ Soweit eine gesetzliche Verpflichtung zur Benennung eines Datenschutzbeauftragten besteht. Andernfalls werden die Aufgaben des Datenschutzbeauftragten durch den Data Privacy Manager oder Data Privacy Officer übernommen.

7.2 Auskunftswesen

7.2.1 Einleitung

Die betroffene Person hat das Recht, Auskunft über die zu ihr gespeicherten personenbezogenen Daten zu verlangen. Dazu gehören sowohl die gespeicherten personenbezogenen Daten als auch weitere festgelegte Informationen zu der Verarbeitung ihrer Daten (siehe Ziffer 4.6).

7.2.2 Beschreibung

7.2.2.1 Regelfall

Der Prozess ist durchzuführen, wenn die betroffene Person einen Antrag auf Auskunft über die von ihr gespeicherten personenbezogenen Daten stellt. Zunächst ist der Antragsteller zu identifizieren, wobei unter Umständen weitere Informationen einzuholen und alle vertretbaren Mittel auszuschöpfen sind (siehe Ziffer 7.1.1.1).²⁰⁴ Die zur Identifikation erhaltenen zusätzlichen Informationen über die betroffene Person dürfen ausschließlich zum Zweck der Identifizierung verwendet werden und sind nach der Identifizierung unverzüglich zu löschen. Insbesondere ist festzustellen für welchen Verantwortlichen (welches Unternehmen im Rheinmetall Konzern) die Anfrage gestellt wird.

Bittet die betroffene Person allgemein um Auskunft nach Art. 15 DSGVO, ohne die Anforderung genauer zu spezifizieren, kann die Auskunft in zwei Stufen erfolgen.

- **Übersicht über gespeicherte Daten**

Die betroffene Person erhält eine Erstauskunft (Übersicht) über die von ihr gespeicherten Daten.

- **Datenschutzinformationen**

Zusätzlich zu der Erstauskunft über die gespeicherten Daten müssen der betroffenen Person folgende Informationen bereitgestellt werden: Verarbeitungszwecke, Kategorien personenbezogener Daten, die verarbeitet werden, Empfänger bzw. Kategorien von Empfängern, die diese Daten bereits erhalten haben oder künftig erhalten werden, geplante Speicherdauer (falls möglich, andernfalls die Kriterien für die Festlegung der Speicherdauer), Information über Rechte auf Berichtigung, Löschung oder Einschränkung der Verarbeitung oder das Widerspruchsrecht gegen diese Verarbeitung, Beschwerderecht der betroffenen Person bei der Aufsichtsbehörde, Herkunft der Daten (soweit diese nicht bei der betroffenen Person selbst erhoben wurden), das Bestehen einer automatisierten Entscheidungsfindung einschließlich Profiling mit aussagekräftigen Informationen über die dabei involvierte Logik sowie die Tragweite und die angestrebten Auswirkungen solcher Verfahren und im Falle eines Datentransfers in ein Drittland auch die geeigneten Garantien für den Datentransfer (z. B. vereinbarte Standard-Datenschutzklauseln oder verbindliche interne Datenschutzvorschriften).²⁰⁵ Dazu erhält die betroffene Person, wenn verfügbar, die Datenschutzinformationen zur jeweiligen Gesellschaft und die Betroffenengruppe, der der Antragsteller angehört.

- **Anschreiben bei Verarbeitung einer großen Menge von personenbezogenen Daten**

Sollte eine Gesellschaft eine große Menge von Informationen über die betroffene Person verarbeiten, so kann von der betroffenen Person verlangt werden, dass sie ihr Auskunftersuchen präzisiert. Die betroffene Person wird in einem Schreiben dazu aufgefordert, dass sie die Informationen oder die Verarbeitungsvorgänge benennt, auf die sich das Auskunftersuchen bezieht, sodann wird die Auskunft erteilt.

²⁰⁶

7.2.2.2 Ausnahmen zum Auskunftswesen

Ausnahmsweise kann die Pflicht zur Erteilung der Auskunft entfallen. Dies ist insbesondere in folgenden Fällen gegeben:²⁰⁷

- Die Auskunft beeinträchtigt voraussichtlich die Verwirklichung von Forschungs- oder Statistikzwecken;
- das Bekanntwerden der Daten gefährdet die öffentliche Sicherheit oder Ordnung;

²⁰⁴ Vgl. Art. 12 Abs. 6 i.V.m Art. 11 DSGVO sowie ErwGr. 64 DSGVO.

²⁰⁵ Informationen nach Art. 15 Abs. 1 und Abs. 2 DSGVO.

²⁰⁶ Siehe hierzu ErwGr. 63 DSGVO.

²⁰⁷ Ausschlussgründe nach § 34 Abs. 1 BDSG.

- die Daten sind nur deshalb gespeichert, weil sie aufgrund gesetzlicher oder satzungsmäßiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen.

Bei der Entscheidung über das Entfallen einer Informationspflicht **muss** der *Data Privacy Officer* oder der *Datenschutzbeauftragte* zu Rate gezogen werden. Eine solche Entscheidung **muss** dokumentiert werden.

7.2.2.3 Zurverfügungstellung einer Kopie der Daten

Auf Verlangen der betroffenen Person ist ihr eine Kopie der personenbezogenen Daten, die Gegenstand der Verarbeitung sind, zur Verfügung zu stellen.²⁰⁸ Dies kann beispielsweise durch eine Datei im PDF-Format oder in Form von Screenshots mit geeignetem Zugriffsschutz (z. B. durch Verschlüsselung mittels Cryptshare) bei einer präzisierten Anfrage erfolgen. Durch die Zurverfügungstellung der Kopie dürfen nicht die Rechte und Freiheiten anderer Personen (Geschäftsgeheimnisse oder Rechte am geistigen Eigentum anderer, wie beispielsweise Urheberrechte) beeinträchtigt werden.²⁰⁹

Der *Data Privacy Officer* oder der *Datenschutzbeauftragte* **können** zu Rate gezogen werden, sofern im konkreten Fall die Beeinträchtigung von Rechten und Freiheiten weiterer Personen möglich erscheint.

Beeinträchtigung weiterer Personen können immer dann gegeben sein, wenn auch die personenbezogenen Daten weiterer Personen in der Datenkopie enthalten sind.

7.2.2.4 Entgeltlichkeit

7.2.2.4.1 Regelfall

Die erste Kopie der Daten muss der betroffenen Person kostenlos zur Verfügung gestellt werden. Für alle weiteren Kopien, die die betroffene Person mit geringem zeitlichen Abstand beantragt, kann ein angemessenes Entgelt auf Grundlage der Verwaltungskosten verlangt werden.²¹⁰

7.2.2.4.2 Ausnahmefall

Bei offenkundig unbegründeten oder exzessiven Anträgen kann einerseits für die Information ein angemessenes Entgelt verlangt oder ein Tätigwerden auf den Antrag hin verweigert werden, sofern in den konkreten Vorschriften keine spezielleren Vorgaben zu finden sind. Es ist ein Nachweis für den offenkundig unbegründeten oder exzessiven Charakter des Antrags zu erbringen. Dies ist entsprechend zu dokumentieren.

Um die einzelnen Bereiche vor übermäßigen Anfragen zu schützen, müssen unbegründete oder exzessive Anfragen identifiziert werden. Für nachweislich unbegründete oder exzessive Anfragen kann folglich eine Kostenrechnung erstellt oder die Auskunft verweigert werden. Die Begründungspflicht für die Verweigerung ist stets zu beachten, außerdem ist auf die Rechtsschutzmöglichkeit hinzuweisen.

Bei Verdacht auf unbegründete und exzessive Anfragen **muss** der *Data Privacy Officer* oder der *Datenschutzbeauftragte* miteinbezogen werden.

7.2.3 Dokumentation

Die Bearbeitung des Antrags ist zu dokumentieren und durch die federführende Kontaktstelle im genutzten Archivsystem zu hinterlegen. Konkret müssen hierzu insbesondere die Zeitpunkte der Antragsstellung sowie der Erledigung des Antrags, das Verfahren der Identifizierung und der Gegenstand der Beauskunftung dokumentiert werden. Sofern der betroffenen Person eine Kopie der Daten zur Verfügung gestellt wurde, ist auch dieser Umstand zu dokumentieren.

7.2.4 Rollen und Verantwortung

Siehe hierzu Ziffer 7.1.3.

²⁰⁸ Vgl. Art. 15 Abs. 3 DSGVO.

²⁰⁹ Vgl. Art. 15 Abs. 4 DSGVO.

²¹⁰ Vgl. Art. 15 Abs. 3 S. 2 DSGVO.

7.3 Recht auf Berichtigung der Daten

7.3.1 Einleitung

Die betroffene Person hat das Recht, zu beantragen, dass ihre personenbezogenen Daten im Falle ihrer Unrichtigkeit berichtigt werden oder die Vervollständigung unvollständiger personenbezogener Daten vorgenommen wird. Unabhängig vom Recht der betroffenen Person eine Berichtigung unrichtiger Daten zu verlangen, existiert nach den Datenschutz-Grundsätzen im Rheinmetall Konzern die Pflicht, durch geeignete und angemessene technische und organisatorische Maßnahmen die Richtigkeit von personenbezogenen Daten zu gewährleisten (vgl. Ziffer 4.8).

7.3.2 Beschreibung

7.3.2.1 Berichtigung von unrichtigen Daten

Eine Berichtigung ist durchzuführen, wenn die betroffene Person einen Antrag auf Berichtigung stellt. Eine Berichtigung ist abzugrenzen von einer einfachen Änderung: Ein neuer Sachverhalt (z. B. Mitteilung einer neuen Adresse) ist keine Berichtigung. Es muss sich um eine unrichtige Information/Angabe handeln, die korrigiert wird (z. B. ein falsch geschriebener Name).²¹¹

Liegen falsche Daten vor, müssen diese Daten berichtigt werden. Dies kann durch eine Veränderung sowie durch eine Löschung der betreffenden Daten geschehen. Bei der Umsetzung sind die Auswirkungen der Berichtigung bei gemeinsamen Datenverarbeitungen zu berücksichtigen.

7.3.2.2 Vervollständigung unvollständiger Daten

Der Prozess ist durchzuführen, wenn die betroffene Person einen Antrag auf Vervollständigung stellt und die betreffenden Daten unter Berücksichtigung des Verarbeitungszwecks unvollständig sind. Eine Unvollständigkeit liegt vor, wenn die Daten für sich genommen richtig sind, aber im Hinblick auf den Verarbeitungszweck ein unzutreffendes Bild der Person ergeben²¹² und der mit der Verarbeitung verfolgte Zweck somit nicht erreicht werden kann. Dies ist beispielsweise der Fall, wenn einem Paketzustelldienst erforderliche Adressinformationen fehlen. Dies hätte zur Folge, dass das Paket anhand fehlender Adressinformationen nicht zugestellt werden kann und somit der Datenverarbeitungszweck nicht erreicht wird.

Liegt eine Unvollständigkeit vor, müssen die Daten, soweit wie für den Verarbeitungszweck erforderlich, ergänzt werden bzw. vervollständigt.²¹³

7.3.2.3 Unterrichtung

Der betroffenen Person sind alle Maßnahmen, die auf einen Antrag hin im Rahmen einer Berichtigungspflicht bzw. Vervollständigungspflicht ergriffen werden, mitzuteilen.²¹⁴ Für die Unterrichtung ist keine Form vorgeschrieben; allerdings muss die Nachweisbarkeit sichergestellt werden (vgl. Ziffer 7.3.3).

Die Berichtigung bzw. die Vervollständigung muss außerdem allen anderen Empfängern der betreffenden personenbezogenen Daten mitgeteilt werden.²¹⁵ Diese Pflicht entfällt, wenn die Mitteilung entweder unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. Die betroffene Person ist zudem über die Empfänger dieser Mitteilung zu informieren, soweit sie dies verlangt.²¹⁶

²¹¹ Vgl. Art. 16 S. 1 DSGVO.

²¹² Vgl. Art. 16 S. 2 DSGVO.

²¹³ Vgl. Art. 16 S. 2 DSGVO.

²¹⁴ Vgl. Art. 12 Abs. 3 S.1 DSGVO.

²¹⁵ Vgl. Art. 19 S. 1 DSGVO und Art. 5 Abs. 1 lit. e DSGVO.

²¹⁶ Vgl. Art. 19 S. 2 DSGVO.

7.3.3 Dokumentation

Die Berichtigung sowie die Vervollständigung werden in den dazu genutzten Verarbeitungen und Assets durchgeführt. In dem genutzten Archivsystem ist der Inhalt und Umstand der Erfüllung der zugehörigen Informationspflicht zu hinterlegen. Konkret muss hierzu insbesondere dokumentiert werden, wann der Antrag gestellt wurde, welche personenbezogenen Daten berichtigt und vervollständigt wurden und wie der Benachrichtigungspflicht nachgekommen wurde.

7.3.4 Rollen und Verantwortung

Siehe hierzu Ziffer 7.1.3.

7.4 Recht auf Löschung

7.4.1 Einleitung

Es ist sicherzustellen, dass die personenbezogenen Daten der betroffenen Person auf Antrag gelöscht werden können. In diesem Fall werden die personenbezogenen Daten unkenntlich gemacht. Wurden die personenbezogenen Daten öffentlich gemacht, sind andere Verantwortliche unter bestimmten Voraussetzungen zusätzlich über das Lösungsverlangen der betroffenen Person zu informieren (Recht auf „Vergessenwerden“).

Zusätzlich besteht die Pflicht des Verantwortlichen, personenbezogenen Daten zu löschen. Das ist in den Datenschutz-Grundsätzen für die Verarbeitung personenbezogener Daten verankert (vgl. Ziffer 4.8).²¹⁷

Um eine fristwahrende Löschung gewährleisten zu können, sind für Verfahren – soweit möglich – automatisierte Lösungskonzepte bzw. Lösungsregeln zu erstellen; in übrigen Fällen werden manuelle Lösungskonzepte erstellt.

7.4.2 Beschreibung

7.4.2.1 Löschung von Daten

Die Löschung ist vorzunehmen, wenn die betroffene Person einen Antrag gestellt hat oder eine der hier aufgezählten Fallgruppen vorliegt.²¹⁸ Eine Fallgruppe liegt beispielsweise vor, wenn die Daten für den Zweck der Verarbeitung nicht mehr notwendig sind (vgl. Ziffer 4.8).²¹⁹

Ist eine der Fallgruppen gegeben, müssen die personenbezogenen Daten gelöscht werden. Die Daten sind gelöscht, wenn sie zerstört sind oder es praktisch unmöglich ist, den zuvor in den zu löschenden Daten verkörpert Personenbezug wahrzunehmen oder herzustellen (die personenbezogenen Daten sind dann anonymisiert). Abzugrenzen davon ist die Pseudonymisierung. Auch in diesem Fall wird der Personenbezug entfernt, kann allerdings über einen Schlüssel wiederhergestellt werden.

Der Prozesseigentümer und der Asset-Eigentümer müssen Vorkehrungen treffen, die die Löschung der personenbezogenen Daten gewährleisten.

Für solche Verarbeitungen, die personenbezogene Daten außerhalb von zentralen Lösungen betreffen (sogenannte unstrukturierte Daten), sind von den jeweiligen zuständigen Stellen des Verantwortlichen Regelungen zu treffen, die die geforderte Löschung personenbezogener Daten organisatorisch sicherstellen.

7.4.2.2 Information anderer Verantwortlicher – Recht auf „Vergessenwerden“

Der Prozess ist durchzuführen, wenn die erforderlichen Voraussetzungen gemäß Ziffer 7.4.2.1 vorliegen und die personenbezogenen Daten durch Unternehmen im Rheinmetall Konzern öffentlich bekannt gemacht worden sind.²²⁰

²¹⁷ Vgl. detaillierter hierzu die Ausführungen zu Art. 5 Abs. 1 lit. e DSGVO.

²¹⁸ Vgl. zu den Fallgruppen: Art. 17 Abs. 1 lit. a bis lit. f DSGVO.

²¹⁹ Vgl. Art. 17 Abs. 1 lit. a DSGVO.

²²⁰ Vgl. Art. 17 Abs. 2 DSGVO.

Liegen die Voraussetzungen vor, müssen durch den Prozess- und Asset-Eigentümer angemessene Maßnahmen, die auch technischer Art sein können, getroffen werden, um die weiteren Verantwortlichen, die die personenbezogenen Daten verarbeiten, über das Lösungsverlangen zu informieren.

7.4.2.3 Ausnahmen zur Löschung von Daten

In bestimmten Fällen können eine Löschung und eine Information anderer Verantwortlicher ausnahmsweise ausgeschlossen sein. Dies liegt beispielsweise dann vor, wenn gesetzliche Aufbewahrungspflichten zu erfüllen oder die Daten zur Abwehr von Rechtsansprüchen gegenüber dem Verantwortlichen erforderlich sind.²²¹

Entsprechende Sachverhalte sind zu den jeweiligen Verarbeitungen zu dokumentieren.

Die Entscheidung über das Entfallen einer Löschpflicht **darf** nur nach Rücksprache mit dem *Data Privacy Officer* oder dem *Datenschutzbeauftragten* getroffen werden.

7.4.2.4 Unterrichtung

Die Löschung **muss** durch den *Prozesseigentümer* allen anderen Empfängern der personenbezogenen Daten mitgeteilt werden, sofern die Daten öffentlich gemacht wurden.

Diese Pflicht entfällt, wenn die Mitteilung entweder unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist.²²² Die betroffene Person ist zudem über die Empfänger dieser Mitteilung zu informieren, soweit sie dies verlangt.²²³

7.4.3 Dokumentation

Die Erfüllung der Löschungspflicht und der Informationspflicht (auch an andere Verantwortliche) ist zu dokumentieren. Zu den Verarbeitungen sind die getroffenen Maßnahmen zur Umsetzung der Datenlöschungen zu dokumentieren. Der Inhalt und Umstand der Erfüllung der Informationspflicht ist zu hinterlegen. Konkret müssen hierzu insbesondere, falls vorliegend, der Zeitpunkt der Antragsstellung, die vorgenommene Art und Weise der Löschung,²²⁴ die erfolgte Information sowie die getroffenen Maßnahmen zur Information Dritter über das Lösungsverlangen dokumentiert werden.

7.4.4 Rollen und Verantwortung

Siehe hierzu Ziffer 7.1.3.

7.5 Einschränkung der Verarbeitung

7.5.1 Einleitung

Es ist sicherzustellen, dass die Verarbeitung der personenbezogenen Daten der betroffenen Person auf Antrag eingeschränkt werden kann. In diesem Fall werden die Daten in einer Art und Weise markiert, dass ihre künftige Verarbeitung nur in begründeten Ausnahmefällen möglich ist.

Auch von sich aus und ohne Verlangen muss die Verarbeitung eingeschränkt werden, wenn eine Speicherung, jedoch nicht mehr die weitere Verarbeitung zulässig ist.²²⁵

²²¹ Vgl. Art. 17 Abs. 3 Ziffer a) – e) DSGVO, sowie § 35 BDSG.

²²² Vgl. Art. 19 S. 1 DSGVO.

²²³ Vgl. Art. 19 S. 2 DSGVO.

²²⁴ Dies kann bspw. durch das Lösprotokoll erfolgen.

²²⁵ Vgl. Art. 5 Abs. 1 lit. c und e DSGVO.

7.5.2 Beschreibung

7.5.2.1 Regelfall: Einschränkung der Verarbeitung

Der Prozess ist durchzuführen, wenn die betroffene Person einen Antrag auf Einschränkung der Verarbeitung stellt.²²⁶ Gründe für die Einschränkung der Verarbeitung können sein:

- Die Richtigkeit der Daten wird bestritten,
- die Verarbeitung ist unrechtmäßig und die betroffene Person lehnt die Löschung ab,
- der Verantwortliche benötigt die Daten nicht länger, doch die betroffene Person benötigt sie zur Geltendmachung ihrer Rechtsansprüche,
- die betroffene Person widerspricht der Verarbeitung aus berechtigtem Interesse und es steht noch nicht fest, ob die berechtigten Gründe des Verantwortlichen für eine Weiterverarbeitung gegenüber denen der betroffenen Person überwiegen.²²⁷

Der *Data Privacy Officer* und der *Datenschutzbeauftragte* **können** bei der Entscheidung über eine Einschränkung der Verarbeitung hinzugezogen werden.

Wird dem Antrag der betroffenen Person stattgegeben, müssen die Daten in einer Weise markiert werden, die ihre künftige Verarbeitung einschränkt. Zu geeigneten Methoden siehe Ziffer 4.8.4. Die Markierung der Daten hat schnellstmöglich, in jedem Fall aber innerhalb eines Monats nach Eingang des Antrags, zu erfolgen.²²⁸

7.5.2.2 Unterrichtung

Der betroffenen Person sind alle Maßnahmen, die auf ihren Antrag zu Einschränkung der Verarbeitung hin ergriffen werden, mitzuteilen.²²⁹ Für die Unterrichtung ist keine Form vorgeschrieben; allerdings ist die Nachweisbarkeit zu gewährleisten (siehe Ziffer 7.5.3).

Wird die Einschränkung der Verarbeitung, die auf Antrag einer betroffenen Person erfolgt ist, aufgehoben, so muss die betroffene Person vorab hierüber informiert werden.²³⁰ Die Unterrichtung muss in geeigneter Form, beispielsweise in der Schriftform, erfolgen und entsprechend dokumentiert werden.

Zusätzlich müssen die Einschränkung der Verarbeitung sowie deren Aufhebung auch allen anderen Empfängern von personenbezogenen Daten mitgeteilt werden.²³¹ Diese Pflicht entfällt, wenn die Mitteilung entweder unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden ist. Die betroffene Person ist zudem über die Empfänger dieser Mitteilung zu informieren, soweit sie dies verlangt.²³²

Wird dem Antrag der betroffenen Person nicht stattgegeben, dann ist darüber mit der maßgeblichen Begründung zu informieren.

7.5.3 Dokumentation

Die Bearbeitung des Antrags ist zu dokumentieren. In dem genutzten Archivsystem ist der Inhalt und Umfang der Erfüllung der Einschränkung zu hinterlegen. Konkret müssen hierzu insbesondere der Zeitpunkt der Antragsstellung sowie die vorgenommene Art der Einschränkung bzw. deren Ablehnung dokumentiert werden.

7.5.4 Rollen und Verantwortung

Siehe hierzu Ziffer 7.1.3.

²²⁶ Die Voraussetzungen sind in Art. 18 Abs. 1 DSGVO zu finden.

²²⁷ Vgl. Art. 18 Abs. 1 lit. b DSGVO.

²²⁸ Vgl. Art. 12 Abs. 3 S. 1 DSGVO.

²²⁹ Vgl. Art. 12 Abs. 3 S.1 DSGVO.

²³⁰ Vgl. Art. 18 Abs. 3 DSGVO.

²³¹ Vgl. Art. 19 S. 1 DSGVO.

²³² Vgl. Art. 19 S. 2 DSGVO.

7.6 Datenportabilität

7.6.1 Einleitung

Es ist sicherzustellen, dass der betroffenen Person auf Antrag die sie betreffenden und durch sie bereitgestellten personenbezogenen Daten unter bestimmten Voraussetzungen zur Verfügung gestellt werden. Dies geschieht durch eine Übermittlung in einem strukturierten, gängigen und maschinenlesbaren Format (z.B. PDF-Datei) entweder an die betroffene Person selbst oder an einen anderen Anbieter.

7.6.2 Beschreibung

7.6.2.1 Regelfall: Anspruch auf Datenportabilität

Der Prozess ist durchzuführen, wenn die betroffene Person einen Antrag auf die Übertragung ihrer Daten stellt und alle erforderlichen Voraussetzungen vorliegen. Der Antrag muss sich auf personenbezogene Daten beziehen, die die betroffene Person selbst betreffen. Zusätzlich muss die Verarbeitung auf einer Einwilligung oder einem Vertrag beruhen und mithilfe eines automatisierten Verfahrens erfolgt sein.²³³

Es sind nur die Daten zu übertragen, die die betroffene Person selbst bereitgestellt hat. Dazu ist zu ermitteln, welche Daten die betroffene Person zur Verfügung gestellt hat (z. B. Antragsformulare, Webformulare). Davon umfasst sind vorrangig die „Rohdaten“, also alle personenbezogenen Daten, die die betroffene Person unmittelbar selbst mitgeteilt hat, und keine verarbeiteten Daten bzw. Ergebnisse der Verarbeitung oder Dokumente.

Bittet die betroffene Person allgemein um Übermittlung der Daten in einem maschinenlesbaren Format, ohne die Anforderung genauer zu spezifizieren, erfolgt die Datenübertragung in zwei Stufen.

Stufe 1

- Übersicht über gespeicherte Daten:
Die betroffene Person erhält eine erste Datenübertragung (Übersicht) über die von ihr gespeicherten Daten. Die Inhalte der Übermittlung werden vorher in den Fachbereichen festgelegt und können ggf. über eine technische Schnittstelle (z. B. Cryptshare) durch die jeweiligen Personen je nach Rolle und Unternehmen abgerufen werden.
- Anschreiben:
Die betroffene Person wird in einem Anschreiben darüber informiert, dass es sich um eine Übersicht der gespeicherten Daten handelt, mit der Bitte das Anliegen zu präzisieren, falls weitere konkrete Datenkategorien gewünscht sind.

Stufe 2

- Präzisiert die betroffene Person im Nachgang ihren Antrag, sind ihr zusätzlich die gewünschten Informationen zur Verfügung zu stellen. Die Zusammenstellung erfolgt individuell im jeweils zuständigen Fachbereich. Auch hier wird ein Anschreiben hinzugefügt. Bei der Datenübertragung sind die Rechte dritter Personen zu berücksichtigen und führen ggfs. zu Einschränkungen der Inhalte.
- Präzisiert die betroffene Person direkt, welche Daten sie haben möchten, sind ihr die Übersicht der personenbezogenen Daten, die weiteren präzise angeforderten Daten sowie ein entsprechendes Anschreiben zur Verfügung zu stellen. Bei der Auskunft sind die Rechte dritter Personen zu berücksichtigen und führen ggf. zu Einschränkungen der Inhalte.
- Die Daten sind in einem strukturierten, gängigen, maschinenlesbaren und interoperablen Format inkl. Metadaten an die betroffene Person oder direkt an einen anderen Anbieter zu übermitteln.²³⁴ Dies sind v. a. am Markt bekannte und oft genutzte Datei-Formate wie beispielsweise pdf-a oder csv.

²³³ Vgl. Art. 20 Abs. 1 DSGVO.

²³⁴ Vgl. Art. 20 Abs. 1 DSGVO und ErwGr 68 S.1 DSGVO.

7.6.2.2 Ausnahmen zur Datenportabilität

In bestimmten Fällen ist die Pflicht zur Datenübermittlung ausgeschlossen, beispielsweise wenn hierdurch die Rechte und Freiheiten einer anderen Person beeinträchtigt werden.²³⁵ In diesem Fall muss ein eingeschränkter Datensatz bereitgestellt werden.

Sofern Anhaltspunkte für das Vorliegen eines solchen Ausnahmefalls erkennbar sind, **muss** die *Data Privacy Organization* oder der *Datenschutzbeauftragte* miteinbezogen werden.

7.6.2.3 Technische Machbarkeit

Die Direktübermittlung der Daten an einen anderen Anbieter ist nur durchzuführen, wenn dies technisch machbar ist.²³⁶ Dazu gehört insbesondere auch die technische Sicherheit der Übermittlung. Ist eine Direktübermittlung technisch nicht machbar, sind die Daten direkt an die betroffene Person zu übermitteln.

7.6.3 Dokumentation

Die Erfüllung der Datenübertragung ist zu dokumentieren. In dem genutzten Archivsystem ist der Inhalt und Umstand der Erfüllung der Datenübertragungspflicht zu hinterlegen. Konkret müssen hierzu insbesondere der Zeitpunkt der Antragsstellung, das Format der übermittelten Daten sowie die vorgenommene Art der Übermittlung dokumentiert werden.

7.6.4 Rollen und Verantwortung

Siehe hierzu Ziffer 7.1.3.

7.7 Widerspruch gegen die Verarbeitung

7.7.1 Einleitung

Die betroffene Person hat das Recht, aus Gründen, die sich aus ihrer besonderen Situation ergeben, der Verarbeitung ihrer Daten in bestimmten Fällen zu widersprechen. Das Recht kann sie jederzeit ausüben.

7.7.2 Beschreibung

7.7.2.1 Widerspruch der Verarbeitung

Die betroffene Person hat das Recht, der Verarbeitung ihrer Daten zu widersprechen. Dies gilt für die Zwecke der Verarbeitung, die gestützt sind auf

- das berechtigte Interesse des Verantwortlichen oder
- die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt, oder in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde.

Der Widerspruch muss sich auf Daten beziehen, die die betroffene Person selbst betreffen. Der Widerspruch muss aus Gründen erfolgen, die sich aus ihrer besonderen Situation ergeben, dies gilt auch für ein auf diese Bestimmungen gestütztes Profiling.²³⁷ Hinsichtlich der von der betroffenen Person vorgebrachten Gründe ist eine individuelle Interessenabwägung notwendig, ob der Verantwortliche berechtigte Gründe für die Verarbeitung nachweisen kann, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen (Interessensabwägung):

- Überwiegen die Interessen der betroffenen Person, dürfen die Daten der betroffenen Person für diesen Zweck nicht mehr verarbeitet werden.²³⁸
- Überwiegen die Interessen des Verantwortlichen, kann der Widerspruch abgelehnt werden. Bei der Interessensabwägung ist hier ein strenger Maßstab anzulegen.

²³⁵ Die Ausnahmen richten sich nach Art. 20 Abs. 3 S. 2 und Abs. 4 DSGVO.

²³⁶ Vgl. Art. 20 Abs. 2 DSGVO.

²³⁷ Vgl. Art. 21 Abs. 1 S. 1 DSGVO, Art. 6 Abs. 1 lit. e oder lit. f DSGVO.

²³⁸ Siehe hierzu die Darstellung zu Art. 17 DSGVO.

In beiden Fällen ist die betroffene Person über die Maßnahmen zu unterrichten.

7.7.2.2 Ausnahmen zum Widerspruch der Verarbeitung

In bestimmten Fällen kann der Widerspruch zur Verarbeitung ausgeschlossen sein, beispielsweise dann, wenn die Weiterverarbeitung der Daten zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.²³⁹

Zudem besteht das Widerrufsrecht auch dann nicht, wenn nachgewiesen werden kann, dass zwingende schutzwürdige Gründe für die Verarbeitung vorliegen, die die Interessen und Freiheiten der betroffenen Person überwiegen.

Das Widerspruchsrecht besteht außerdem nicht, wenn die Datenverarbeitung zusätzlich zu den oben genannten Voraussetzungen noch auf einer zusätzlichen Rechtsgrundlage, beispielsweise die Erfüllung einer rechtlichen Verpflichtung, basiert.

7.7.2.3 Widerspruch der Direktwerbung

Der Widerspruch der Verarbeitung der Daten zur Direktwerbung kann ohne Angabe von Gründen erfolgen und ist unmittelbar, d. h. ohne Interessensabwägung, durchzuführen. Die Daten der betroffenen Person dürfen dann nicht mehr für Werbezwecke verwendet werden. Beinhaltet die Direktwerbung ein Profiling, so gilt der Werbeverzicht auch für dieses Profiling.²⁴⁰

Es ist zu beachten, dass bei erfolgtem Widerspruch ein Lösungsrecht der betroffenen Person hinsichtlich dieses Verarbeitungsvorganges und somit auch eine Löschpflicht besteht, soweit keine Ausnahme von dieser Löschpflicht besteht.²⁴¹

Der Widerspruch der Direktwerbung wird üblicherweise in sogenannten Robinsonlisten in dem für die Werbung zuständigen Fachbereich dokumentiert.

7.7.2.4 Widerspruch bei Verarbeitung zu Forschungszwecken oder zu statistischen Zwecken

Werden personenbezogenen Daten für wissenschaftliche oder geschichtliche Forschungen oder für statistische Zwecke verarbeitet²⁴², kann die betroffene Person aus besonderen persönlichen Gründen widersprechen, es sei denn, die Datenverarbeitung ist zur Erfüllung einer Aufgabe im öffentlichen Interesse erforderlich.²⁴³

7.7.2.5 Hinweispflicht und Unterrichtung

Auf das Widerspruchsrecht muss gemäß den Ausführungen in den Ziffern 7.7.2.1 und in 7.7.2.3 rechtzeitig und verständlich hingewiesen werden.²⁴⁴ Außerdem ist das Widerspruchsrecht optisch hervorzuheben, da es in einer von den anderen Informationen getrennten Form dargestellt werden muss.²⁴⁵ Als Beispiel für eine optische Hervorhebung dienen die in diesem Dokument zu findenden blauen Kästen. Der betroffenen Person sind alle Maßnahmen, die im Rahmen eines Widerspruchs ergriffen werden, mitzuteilen. Dies gilt für Bestätigungen sowie Ablehnungen von Widersprüchen.²⁴⁶

7.7.2.6 Form des Widerspruchs

Der Antrag der betroffenen Person muss zum Ausdruck bringen, dass die Verarbeitung der Daten beendet werden soll. Für den Widerspruch ist keine bestimmte Form erforderlich.²⁴⁷

²³⁹ Vgl. Art. 21 Abs. 1 S. 2 DSGVO.

²⁴⁰ Vgl. Art. 21 Abs. 2 DSGVO.

²⁴¹ Vgl. Art. 17 Abs. 1 lit. c DSGVO und die Ausnahmen der Löschpflicht in Art. 17 Abs. 3 DSGVO.

²⁴² Vgl. Art. 89 Abs. 1 DSGVO.

²⁴³ Vgl. Art. 21 Abs. 6 HS. 2 DSGVO.

²⁴⁴ Vgl. Art. 21 Abs. 4 DSGVO.

²⁴⁵ Vgl. Art. 21 Abs. 4 letzter Halbsatz DSGVO.

²⁴⁶ Vgl. Art. 13 Abs. 2 lit. b und Art. 14 Abs. 2 lit. c DSGVO.

²⁴⁷ Nach ErwGr. 59 DSGVO soll der betroffenen Person die Möglichkeit der elektronischen Antragsstellung eingeräumt werden. Dies gilt insbesondere, wenn die Verarbeitung der Daten elektronisch erfolgt.

7.7.3 Dokumentation

Die Abhilfe des Widerspruchs ist zu dokumentieren. In dem genutzten Archivsystem sind der Inhalt des Widerspruchs und die Unterrichtung der betroffenen Person zu den ergriffenen Maßnahmen zu hinterlegen. Konkret müssen hierzu insbesondere der Zeitpunkt des Widerspruchs, die Antwort und ggf. die vorgenommene Beendigung der Verarbeitung sowie die Erfüllung der Hinweispflichten dokumentiert werden.

Es sind die Auswirkungen eines berechtigten Widerspruchs auf die Verarbeitung zu überprüfen. Die Auswirkungen sind in der Verfahrensbeschreibung zu dokumentieren (siehe Ziffer 5).

Gibt ein Unternehmen im Rheinmetall Konzern einem Widerspruch nicht statt, muss dieses Unternehmen jederzeit nachweisen können, dass

- „zwingende schutzwürdige Gründe“ vorliegen, die die Interessen, Rechte und Freiheiten der betroffenen Person überwiegen oder
- die Erforderlichkeit der Verarbeitung für die Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen erforderlich ist.

Um den Nachweis führen zu können, sind die erfolgte Abwägung oder die in Anspruch genommenen Rechtsansprüche im Archivsystem zu dokumentieren.

7.7.4 Rollen und Verantwortung

Siehe hierzu Ziffer 7.1.3.

8 Datenschutzvorfälle

8.1 Einleitung

Ein Datenschutzvorfall ist eine „Verletzung des Schutzes personenbezogener Daten“²⁴⁸ sowie ein Verstoß gegen Vorschriften aus der DSGVO oder aus anderen nationalen Datenschutzgesetzen (z. B. BDSG).

Jeder potentielle Datenschutzvorfall ist unverzüglich der Datenschutz-Organisation zu melden: Eine Datenschutzverletzung, da diese gegebenenfalls meldepflichtig ist und ein Datenschutzverstoß, weil dieser zu Datenschutz Compliance Risiken für den Verantwortlichen mit nicht unerheblichen Konsequenzen wie z. B. Geldbußen, Schadensersatz führen kann.

Während ein Datenschutzverstoß nicht unbedingt meldepflichtig sein muss, ist eine Verletzung des Schutzes personenbezogener Daten (Datenschutzverletzung) bei einem potentiellen Risiko (nicht bloß geringfügig) für betroffene Personen (Regelfall) an die zuständige Aufsichtsbehörde zu melden (Meldepflicht).

Datenschutzaufsichtsbehörden veröffentlichen teilweise ihre Maßnahmen sowie Meldungen der Unternehmen. Sie sind zudem bei Auskunftersuchen verpflichtet, Informationen an den Antragssteller herauszugeben. Somit ist jede Meldung an eine Datenschutzaufsichtsbehörde potentiell öffentlichkeitswirksam.

Die Richtlinie zum Notfall- und Krisenmanagement des Rheinmetall Konzerns sieht vor, dass Incidents/Vorfälle, die potentiell öffentlichkeitswirksam (u. a. negative Presse, Bußgelder, Meldung an die Aufsichtsbehörde) sind, an den operativen Leiter des Krisenstabs gemeldet werden **müssen**. Somit ist jede Datenschutzverletzung an den operativen Leiter des Krisenstabs zu melden.

Die Behandlung einer Datenschutzverletzung als Incident wird durch die Rheinmetall Incident Organization (RIO) gesteuert. Die RIO hat hierbei datenschutzrechtliche Anforderungen zu erfüllen und wird durch die Data Privacy Organization unterstützt.

Besteht darüber hinaus auch ein hohes Risiko für die Rechte und Freiheiten betroffener Personen, sind diese neben der Aufsichtsbehörde ebenfalls zu benachrichtigen (Benachrichtigungspflicht). Einzelheiten hierzu sind den Ziffern 8.2 bis 8.6 zu entnehmen.

Unabhängig von einer Melde- oder Benachrichtigungspflicht **müssen** alle Datenschutzvorfälle intern unverzüglich an die zuständigen *Data Privacy Officer* gemeldet werden (Interne Meldeverpflichtung) und durch die *Data Privacy Organization* dokumentiert werden.

Alle Stellen im Rheinmetall-Konzern müssen im Rahmen der Aufklärung und Meldung von Datenschutzverletzungen und Datenschutzverstößen mit der RIO und der Data Privacy Organisation zusammenarbeiten und alle geforderten Informationen unmittelbar beschaffen und zur Verfügung stellen, insbesondere wenn eine Datenschutzverletzung potentiell meldepflichtig ist.

8.2 Meldung an die Aufsichtsbehörde und an die betroffene Person | 72 Stunden

Der Prozess ist durchzuführen, wenn eine Verletzung des Schutzes personenbezogener Daten bekannt wird.

Eine Verletzung des Schutzes personenbezogener Daten ist eine Verletzung der Sicherheit, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung (Verlust der Verfügbarkeit und Integrität) oder zur unbefugten Offenlegung von bzw. zum unbefugten Zugang zu personenbezogenen Daten (Verlust der Vertraulichkeit) führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden.²⁴⁹ Dies ist beispielsweise bei einem Hackerangriff oder unter Umständen auch beim Verlust eines unverschlüsselten Datenträgers der Fall.

Es sollte sofort festgestellt werden können, ob eine Datenschutzverletzung vorliegt, um daraufhin umgehend die Aufsichtsbehörde und die betroffenen Personen unterrichten zu können.²⁵⁰

²⁴⁸ Vgl. Art. 4 Nr. 12 DSGVO.

²⁴⁹ Vgl. Art. 4 Nr. 12 DSGVO.

²⁵⁰ Vgl. ErwGr. 87 DSGVO.

Liegt eine potentiell meldepflichtige Verletzung des Schutzes personenbezogener Daten vor, **müssen** durch die *RIO* zunächst die Verantwortlichen ermittelt werden, d. h. die Unternehmen im Rheinmetall Konzern, welche von dem Datenschutzvorfall betroffen sind.

Beschäftigte müssen in der Lage sein, Datenschutzverletzungen zu identifizieren. Eine vollständige, sichere Kenntnis der Datenschutzverletzung ist nicht erforderlich, vielmehr reicht eine hohe Wahrscheinlichkeit einer Datenschutzverletzung aus, um die Meldepflicht auszulösen.

Die Beschäftigten **müssen** durch die *Data Privacy Organization* angemessen geschult werden, zudem **müssen** zur Meldung von Datenschutzverletzungen geeignete Prozessbeschreibungen durch die *Unternehmenssicherheit* sowie Vordrucke/Templates und Verfahrensanweisungen²⁵¹ durch die *Data Privacy Organization* bereitgestellt werden.

Die *IT-Security und Informationssicherheit* **müssen** angemessene technische und organisatorische Maßnahmen zur Entdeckung, Meldung und Behandlung von Verletzungen des Schutzes personenbezogener Daten vorhalten und betreiben, zudem **müssen** durch die Unternehmenssicherheit Verfahren zur Erfüllung der Meldepflichten getroffen werden, durch die eine Meldung bei der Aufsichtsbehörde sowie an die betroffenen Personen in geeigneter Weise erfolgen kann.

Dies kann beispielsweise durch Einrichtung eines Incident-Managements und durch eine Überwachung von IT-Systemen im Hinblick auf sicherheitsrelevante Zugriffe erfolgen, die auch Maßnahmen zur Beseitigung von Datenschutzverletzungen und Risiken vorsieht und Möglichkeiten von Systemaufzeichnungen zur Dokumentation der Datenschutzverletzung bietet.

Sofern eine Datenschutzverletzung festgestellt wird, ist zu prüfen, ob die festgestellte Datenschutzverletzung zu einem Risiko oder sogar zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt. Dies ist der Fall, wenn die Datenschutzverletzung beispielsweise zu einem physischen, materiellen oder immateriellen Schaden für natürliche Personen führt (wie etwa der Verlust der Kontrolle über ihre personenbezogenen Daten oder Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder -betrug, finanzielle Verluste, unbefugte Aufhebung der Pseudonymisierung, Rufschädigung, Verlust der Vertraulichkeit von einem Berufsgeheimnis unterliegenden Daten oder andere erhebliche wirtschaftliche oder gesellschaftliche Nachteile für die betroffene Person).²⁵² Im Rahmen der Verarbeitungsbeschreibung (vgl. Ziffer 4.10) ist eine sogenannte Schwellwertanalyse bzw. Risikoanalyse vorgesehen. Um festzustellen, ob ein Risiko für die Rechte und Freiheiten natürlicher Personen besteht, kann die Schwellwertanalyse aus der Verarbeitungsbeschreibung ebenfalls ein Anhaltspunkt sein. Grundsätzlich ist aber das Risiko in Bezug auf den Einzelfall zu prüfen (vgl. Ziffer 4.10).

Für die Meldung an die Aufsichtsbehörde sind die Anforderungen an den Grad des Risikos gering. Es löst grundsätzlich jedes nicht auszuschließende Risiko für die Rechte und Freiheiten einer natürlichen Person die Meldepflicht²⁵³ aus.

Bei einem nicht auszuschließenden Risiko für die Rechte und Freiheiten natürlicher Personen **muss** schnellstmöglich, in jedem Fall innerhalb von **72 Stunden** ab Kenntniserlangung der Verletzung diese der Aufsichtsbehörde gemeldet sowie geeignete Maßnahmen zur Risikominimierung getroffen werden.

Die Meldung wird durch die *Data Privacy Organization* vorbereitet und durch die zuständige(n) *Geschäftsführung(en)* freigegeben. Die Meldung erfolgt nach Freigabe der Geschäftsführung(en) durch die zuständigen Data Privacy Officer. Zudem ist der Datenschutzbeauftragte als Anlaufstelle für die Datenschutzaufsichtsbehörden über die Meldung zu informieren.

Die *RIO* **muss** alle für die Meldung erforderlichen Informationen ermitteln (lassen) und der *Data Privacy Organization* zur Verfügung stellen.

Die Meldung muss die folgenden Mindestangaben enthalten:

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, soweit möglich mit Angabe der Kategorien und der ungefähren Zahl der betroffenen Personen, der betroffenen Datenkategorien und der ungefähren Zahl der betroffenen personenbezogenen Datensätze;

²⁵¹ Vgl. Richtlinie zum Notfall- und Krisenmanagement und mitgeltende Dokumente.

²⁵² Vgl. hierzu auch ErwGr. 85 DSGVO.

²⁵³ Vgl. Art. 33 DSGVO.

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

Können diese Informationen nicht alle zur gleichen Zeit zur Verfügung gestellt werden, müssen sie schnellstmöglich nachgereicht werden.²⁵⁴ Sofern die Meldung verspätet ist, sind ferner Gründe für die Verzögerung anzugeben.

Ergibt die Risikobewertung ein hohes Risiko für die betroffene Person, ist zusätzlich eine Benachrichtigung an die betroffene Person erforderlich. Die Benachrichtigung muss in klarer sowie einfacher Sprache die Verletzung beschreiben und die folgenden Mindestangaben enthalten:

- den Namen und die Kontaktdaten des Datenschutzbeauftragten oder einer sonstigen Anlaufstelle für weitere Informationen;
- eine Beschreibung der wahrscheinlichen Folgen der Verletzung des Schutzes personenbezogener Daten;
- eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung der Verletzung des Schutzes personenbezogener Daten und ggf. Maßnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.²⁵⁵

Kann nicht ausgeschlossen werden, dass eine Verletzung der Rechte und Freiheiten von betroffenen Personen vorliegt, sollte eine Meldung an die Aufsichtsbehörde und ggf. zusätzlich eine Benachrichtigung der betroffenen Person erfolgen.

Bei der Entscheidungsfindung **müssen** der *Data Privacy Officer* und der *Datenschutzbeauftragte* beratend miteinbezogen werden, die Entscheidung zur Meldung obliegt der Geschäftsführung.

8.3 Datenschutzverletzung im Rahmen von Auftragsverarbeitungsverhältnissen

8.3.1 Externer Auftragsverarbeiter

Bei externen Auftragsverarbeitern ist zu achten, dass im Auftragsverarbeitungsvertrag eine Regelung zur unverzüglichen Meldung von Verarbeitungsunregelmäßigkeiten aufgenommen wurde, sodass der gesetzlichen Meldepflicht nachgekommen werden kann (siehe Ziffer 6.2).

8.3.2 Rheinmetall Gesellschaft als Auftragsverarbeiter

Werden die Daten im Rahmen eines Auftragsdatenverarbeitungsvertrages verarbeitet, besteht bei Bekanntwerden einer Verletzung lediglich eine Meldepflicht gegenüber dem Verantwortlichen (=dem Auftraggeber), jedoch nicht gegenüber der Aufsichtsbehörde. Die Meldung an den Verantwortlichen (=Auftraggeber) muss schnellstmöglich (unverzüglich) erfolgen.²⁵⁶

8.4 Entfallen der Meldepflicht

Die Pflicht zur Meldung an die Aufsichtsbehörde entfällt, wenn festgestellt wird, dass die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.²⁵⁷ Die Darstellungen zur Feststellung des Risikos gelten entsprechend. Dies ist insbesondere dann der Fall, wenn technische und organisatorische Maßnahmen ergriffen worden sind, die den Zugriff auf die personenbezogenen Informationen verhindern oder unmöglich machen (z. B. Verschlüsselung der Daten, vollständige Anonymisierung).

²⁵⁴ Vgl. Art. 33 Abs. 1, Abs. 2 und Abs. 4 DSGVO und Art. 55 DSGVO.

²⁵⁵ Vgl. Art. 34 Abs. 1, Abs. 2 DSGVO.

²⁵⁶ Vgl. Art. 33 Abs. 2 DSGVO, ggf. enthält der zugrundeliegende Vertrag zur Auftragsverarbeitung konkretisierende Regelungen.

²⁵⁷ Vgl. Art. 33 Abs. 1 S.1 DSGVO.

Die Feststellung, ob eine Meldung oder Benachrichtigung entfallen **kann, darf** nur nach Beratung durch die *Data Privacy Organization* erfolgen.

8.5 Dokumentation

Die Erfüllung der Meldepflicht ist zu dokumentieren. In dem genutzten Archivsystem sind Inhalt und Umstand der Erfüllung der Meldepflicht zu hinterlegen. Bei der Meldung an die Aufsichtsbehörde müssen die Verletzung des Schutzes personenbezogener Daten einschließlich aller im Zusammenhang stehenden Fakten sowie deren Auswirkungen und die ergriffenen Abhilfemaßnahmen dokumentiert werden. Diese Dokumentation muss der Aufsichtsbehörde die Überprüfung der Einhaltung der gesetzlichen Anforderungen ermöglichen.²⁵⁸ Im intern genutzten Archivsystem ist mindestens Folgendes zu dokumentieren: die Interne Meldung, die Risikoanalyse, die Risikobewertung, ggf. die Meldung an die Aufsichtsbehörde sowie ggf. eine Benachrichtigung an die betroffene Person.

Die Dokumentation ist für drei Jahre aufzubewahren. Die Aufbewahrungsfrist beginnt nach Abschluss des Datenschutzvorfalls bzw. nach Abschluss des Verfahrens bei der zuständigen Aufsichtsbehörde.

Bei der Verarbeitung im Rahmen eines Auftragsdatenvertrages muss eine entsprechende Dokumentation durch den Auftragsverarbeiter erfolgen, die dem Verantwortlichen zur Verfügung gestellt wird.²⁵⁹

8.6 Rollen und Verantwortung

Rolle	Verantwortung
Beschäftigter	<ul style="list-style-type: none"> ▪ Kennt die Prozesse, Vordrucke/Templates und Verfahrensanweisungen zur Meldung von Datenschutzverletzungen.
Identifizierende Person „Erst-Melder“	<ul style="list-style-type: none"> ▪ Identifiziert den Verdacht einer Datenschutzverletzung. ▪ Meldet den Verdacht einer Verletzung <u>unverzüglich</u> (spätestens nach zwei Stunden) an den jeweiligen Datenschutz-Koordinator und Hauptabteilungsleiter. Falls kein Datenschutz-Koordinator benannt oder dieser nicht erreichbar ist, muss der zuständige Data Privacy Officer informiert werden.
Erstmelde-Stelle i.d.R. Datenschutz-Koordinator oder der Hauptabteilungsleiter	<ul style="list-style-type: none"> ▪ Ist die Person, die den Vorfall intern an den Data Privacy Officer und ggf. an den zuständigen Krisenstab gem. der Notfall- und Krisenmanagement Richtlinie meldet. ▪ Meldet das ausgefüllte Musterdokument zu Datenschutzverletzungen <u>schnellstmöglich</u>, spätestens jedoch innerhalb von 24 Stunden ab Bekanntwerden der Verletzung. ▪ Bindet den Data Privacy Officer ein, um bestehende Melde- und Benachrichtigungspflichten zu bewerten.
Hauptabteilungsleiter	<ul style="list-style-type: none"> ▪ Prüft regelmäßig, ob ausreichende technische und organisatorische Maßnahmen zur Entdeckung von der Verletzung des Schutzes personenbezogener Daten und zur Erfüllung der Meldepflichten getroffen wurden, durch die eine Meldung bei der Aufsichtsbehörde sowie an die betroffenen Personen in geeigneter Weise erfolgen kann. ▪ Stellt sicher, dass alle relevanten Informationen zusammengetragen und <u>unverzüglich</u> der zuständige Krisenstab gem. der Notfall- und Krisenmanagement Richtlinie sowie der zuständige Data Privacy Officer informiert werden. ▪ Steht bei Rückfragen in Bezug auf den Datenschutzvorfall zur Verfügung. ▪ Führt die Risikobewertung gemeinsam mit dem Krisenstab und dem Data Privacy Officer durch. ▪ Kann einen Beschäftigten benennen, der bei Rückfragen zum Datenschutzvorfall zur Verfügung steht und zu Assets und Verarbeitungen umfassende Kenntnisse hat.
(Haupt)Abteilungen	<ul style="list-style-type: none"> ▪ Kommen ihrer Verpflichtung aus den Verfahrensanweisungen und Anforderungen aus den Prozessen nach. ▪ Unterstützen den Krisenstab sowie den Data Privacy Officer bei der Bewertung einer Melde- und Benachrichtigungspflicht.

²⁵⁸ Vgl. Art. 33 Abs. 5 DSGVO.

²⁵⁹ Vgl. Art. 28 Abs. 3 S. 2 lit. f DSGVO.

Rolle	Verantwortung
Data Privacy Officer	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Nimmt die Meldung in Abstimmung mit der Geschäftsführung vor. ▪ Falls es sich bei dem Data Privacy Officer und dem Datenschutzbeauftragten um dieselbe Person handelt, so kann die Meldung alternativ auch durch den Data Privacy Manager erfolgen. Dies geschieht in enger Abstimmung zwischen den genannten Rollen.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Stellt sicher, dass Beschäftigte zu Datenschutzverletzungen entsprechend geschult werden. ▪ Stellt geeigneter Prozesse, Vordrucke/Templates und Verfahrensanweisungen zur Meldung von Datenschutzverletzungen bereit. ▪ Meldet Datenschutzverletzung, die potentiell zu einer Meldepflichtung an die zuständige Datenschutzaufsichtsbehörde führen, an die RIO. ▪ Dokumentiert den gesamten Ablauf des Datenschutzvorfalls bzw. die Datenschutzverletzung.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät und überwacht die Einführung solcher Verfahren und Vorgehensweisen. ▪ Hat in Bezug auf die Feststellung der Voraussetzungen der Meldepflicht keine durchführende Rolle.²⁶⁰ ▪ Obliegt per Gesetz die Zusammenarbeit mit der Aufsichtsbehörde.²⁶¹
Informationssicherheit	<ul style="list-style-type: none"> ▪ Stellt geeignete Prozesse, Vordrucke/Templates und Verfahrensanweisungen zur Meldung von Datenschutzverletzungen bereit. ▪ Stellt sicher, dass ausreichende technische und organisatorische Maßnahmen zur Entdeckung von Verletzungen des Schutzes personenbezogener Daten bestehen und dies im ISMS verankert ist.
Rheinmetall Incident Organization (RIO)	<ul style="list-style-type: none"> ▪ Wird unter Umständen gemäß Richtlinie zum Notfall- und Krisenmanagement vom Leiter des Stabs einberufen und von der Erstmelde-Stelle unterrichtet. ▪ Wird grundsätzlich einberufen, wenn potentiell eine Meldung an die Aufsichtsbehörde zu erfolgen hat. ▪ Die Einberufung hängt zudem von den Kriterien der Notfall- und Krisenmanagement Richtlinie ab.

²⁶⁰ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

²⁶¹ Vgl. Art. 39 Abs. 1 lit. d DSGVO.

9 Verpflichtung von Beschäftigten

9.1 Einleitung

Den Beschäftigten im Rheinmetall Konzern ist der unbefugte Umgang mit personenbezogenen Daten untersagt.

Die Beschäftigten **müssen** bei der Aufnahme ihrer Tätigkeit bei einem Unternehmen im Rheinmetall Konzern durch die einstellende Personalabteilung auf Vertraulichkeit beim Umgang mit personenbezogenen Daten verpflichtet werden.

Das gilt auch für alle Personen, die im Rahmen ihres Vertrages mit einem Unternehmen im Rheinmetall Konzern potentiellen Zugriff auf personenbezogene Daten erhalten könnten.

Für diese unterschiedlichen Personengruppen werden bei Bedarf jeweilige Verpflichtungen als Templates vorgesehen, die inhaltlich auch mit einer Verpflichtung auf spezielle Geheimhaltungspflichten (z. B. § 203 Strafgesetzbuch, § 35 SGB I Sozialgeheimnis, Bankgeheimnis) und auf betriebliche Geheimhaltungsvorschriften kombiniert werden können. Die Formulare umfassen ein Merkblatt mit grundlegenden Hinweisen zu den Inhalten der Verpflichtung sowie Verweise auf zugehörige Rechtsgrundlagen. Templates werden durch die Data Privacy Organization zur Verfügung gestellt.

Die Einrichtung von Berechtigungen für den Zugriff auf Verarbeitungen mit personenbezogenen Daten im Rheinmetall Konzern setzt eine solche Verpflichtung der zu berechtigenden Person voraus.

9.2 Beschreibung

Beschäftigte erhalten zusammen mit ihren Vertragsunterlagen die *Verpflichtung auf die Vertraulichkeit für Beschäftigte*, welcher ein Merkblatt mit grundlegenden Hinweisen zum Datenschutz beigelegt ist. Der Vordruck ist vom Beschäftigten zu unterschreiben. Beschäftigte, die in mehreren Unternehmen im Rheinmetall Konzern eingesetzt werden, müssen diese Erklärung nur einmal unterschreiben. Die Verpflichtung ist als Nachweis in die Personalakte zu legen. Die Erklärung umfasst auch die Verpflichtung auf spezielle Geheimhaltungspflichten. Die einstellende Personalabteilung ist grundsätzlich dafür zuständig, die Verpflichtungserklärung einzuholen und zu dokumentieren.

Andere Beschäftigte (z. B. Arbeitnehmer in Arbeitnehmerüberlassung) erhalten die Verpflichtung auf die Vertraulichkeit für ihre jeweilige Rolle. Dieses Formular ist von jeder im Rahmen eines Vertragsverhältnisses beschäftigten Einzelperson zu unterschreiben. Die Verpflichtung ist Bestandteil der Vertragsunterlagen für den Einsatz dieser Personen. Die Erklärung sollte auch die Verpflichtung auf spezielle Geheimhaltungspflichten sowie auf die betrieblichen Geheimhaltungsvorschriften enthalten. Die einstellende Personalabteilung ist grundsätzlich dafür zuständig, die Verpflichtungserklärung einzuholen und zu dokumentieren.

Externe (z. B. Berater) - soweit sie nicht einem besonderen Berufsgeheimnis unterliegen wie Wirtschaftsprüfer, Anwälte, Steuerberater usw. - erhalten ebenfalls diese Verpflichtung. Der Vordruck ist von diesen zu unterschreiben. Die Verpflichtung ist Bestandteil der Vertragsunterlagen für den Einsatz von Externen. Die Erklärung sollte auch die Verpflichtung auf spezielle Geheimhaltungspflichten sowie auf die betrieblichen Geheimhaltungsvorschriften umfassen. Zudem kann bereits mit externen Unternehmen im Dienstleistungsvertrag vereinbart werden, dass sie ihre Beschäftigten selber in dem geforderten Umfang schriftlich auf die Vertraulichkeit verpflichten und dies bei Bedarf nachweisen. Dies ist beim Abschluss des Vertrages mit dem Geschäftspartner stichprobenartig durch den Prozesseigentümer bzw. Asset-Eigentümer zu überprüfen. Die Prüfung ist zu dokumentieren.

9.3 Dokumentation

Die unterschriebenen Verpflichtungserklärungen sind in der Personalakte oder zusammen mit den jeweiligen Vertragsunterlagen zu dokumentieren.

9.4 Rollen und Verantwortung

Rolle	Verantwortung
Personalabteilung bzw. Prozesseigentümer	▪ Obliegt die Durchführung und Dokumentation der Verpflichtung von (neuen) Beschäftigten.

Rolle	Verantwortung
	<ul style="list-style-type: none"> ▪ Prüft regelmäßig, ob die Verpflichtungserklärung im Beschäftigtenverhältnis aktuell ist und die gesetzlichen Anforderungen erfüllt und ob geeignete Verpflichtungserklärungen im Beschäftigtenverhältnis vorliegen. ▪ Stellt sicher, dass die Verpflichtung vor Aufnahme der Tätigkeit unterzeichnet wird.
Prozesseigentümer & Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Obliegt die Durchführung und Dokumentation der Verpflichtung von Vertragsnehmer (u. a. Dienstleister und Berater). ▪ Kann als Auftraggeber dem jeweiligen Einkäufer die Durchführung der Verpflichtung übertragen. ▪ Stellt sicher, dass die Verpflichtung vor Aufnahme der Tätigkeit unterzeichnet wird. ▪ Prüft das Vorliegen einer entsprechenden Verpflichtungserklärung bei der Erteilung von Berechtigungen für den Zugriff auf Verarbeitungen oder Assets mit personenbezogenen Daten im Rheinmetall Konzern. ▪ Dokumentiert die Verpflichtung bei den Vertragsunterlagen.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Verwaltet die Muster und hält die Muster der Verpflichtungen aktuell. ▪ Stellt die Formulare zu den Verpflichtungen im Gate oder auf ggfs. dafür vorgesehenen Laufwerk-Verzeichnissen zur Verfügung. ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.

10 Schulung und Awareness

10.1 Einleitung

Die Beschäftigten, die personenbezogene Daten verarbeiten, sind durch geeignete Maßnahmen mit den Vorschriften und mit den jeweiligen besonderen Erfordernissen des Datenschutzes vertraut zu machen. Maßnahmen zur Sensibilisierung der Beschäftigten im datenschutzkonformen Umgang mit personenbezogenen Daten stellen im Rheinmetall Konzern entsprechende Schulungen dar.

Jeder Beschäftigte muss die datenschutzrechtlichen Grundsätze im täglichen Berufsalltag beachten und einhalten.

10.2 Beschreibung

Alle Beschäftigten erhalten zeitnah, jedoch mindestens im ersten Jahr nach der Einstellung eine Einweisung in den Datenschutz. In der Regel findet die Einweisung als Web-Schulung bzw. E-Learning statt. Die Bereitstellung von sogenannten E-Learnings soll nach Möglichkeit über die zentrale Lern-Management-Plattform erfolgen. Neu eingestellte Beschäftigte, die keinen Zugang zu Web-Schulungen und E-Learnings haben, müssen ebenfalls zeitnah, jedoch mindestens im ersten Jahr nach Einstellung an einer Präsenzs Schulung teilnehmen.

Wenn im Ausnahmefall weder Web- noch Präsenzs Schulungen genutzt werden können, wird Informationsmaterial als druckbare Unterlage im Gate oder auf dafür ggf. vorgesehenen Laufwerk-Verzeichnissen zur Verfügung gestellt. Für Beschäftigte ohne technischen Zugang zum Informationsmaterial muss sichergestellt werden, dass die Informationen den betroffenen Beschäftigten entsprechend bereitgestellt werden.

Um die Kenntnisse der Beschäftigten zum Thema Datenschutz aktuell zu halten, finden Wiederholungsschulungen und weitergehende Präsenzs Schulungen in regelmäßigen Abständen statt. Das E-Learning wird verbindlich für alle aktiven mit der Verarbeitung personenbezogener Daten betrauten Personen in regelmäßigen Abständen organisiert.

Aufgrund unterschiedlicher Aufgabenbereiche ist die Intensität der Verarbeitung personenbezogener Daten nicht für alle Beschäftigten gleich. Daher wird zudem zwischen allgemeinen, für alle Beschäftigten verbindlichen und fachbereichsspezifischen Schulungen unterschieden. Beschäftigtengruppen mit speziellem Informationsbedarf zu Themen des Datenschutzes können bei Bedarf mit thematisch entsprechend zugeschnittenen Schulungsinhalten nach Abstimmung versorgt werden.

In der Regel finden zielgruppenspezifische Schulungen als Präsenzs Schulungen statt, um den Lernerfolg sicherzustellen und den Beschäftigten die Gelegenheit für Rückfragen und Klärungen zu geben. Alternativ kann die Einweisung durch Nutzung entsprechender Schulungsinhalte über eine Lern-Management- Plattform online oder durch die Nutzung anderer Medien, z.B. in Form einer Web-Schulung, erfolgen. Die Schulung muss mindestens die Grundlagen des Datenschutzes beinhalten. Dabei werden die Begriffsdefinitionen, gesetzliche Regelungen und die Grundsätze für die Verarbeitung personenbezogener Daten allgemein dargestellt. Es wird zudem auf die gesetzlichen Dokumentationspflichten zum Nachweis ordnungsgemäßer Datenverarbeitungen hingewiesen.

Unabhängig von einer regelmäßigen Schulung in Form eines E-Learnings erfolgt eine Sensibilisierung der Beschäftigten durch geeignete anlassbezogene und anlasslose Informations- und Awareness-Maßnahmen (z. B. Videos und Beiträge im Gate oder geeignete Präsenztermine).

Die Data Privacy Organization muss ein angemessenes Schulungs- und Awareness-Konzept erstellen und pflegen.

10.3 Dokumentation

Die Durchführungen von Schulungen im ersten Jahr nach der Einstellung, fachbereichsspezifische Schulungen sowie Wiederholungsschulungen von Beschäftigten sind zu dokumentieren. Ein Nachweis der Teilnahme muss in der Personalakte des Beschäftigten abgelegt werden.

10.4 Rollen und Verantwortung

Rolle	Verantwortung
Hauptabteilungsleiter	<ul style="list-style-type: none"> ▪ Stellt gemeinsam mit der Personalabteilung sicher, dass die Informationen für Beschäftigte ohne technischen Zugang zum Informationsmaterial entsprechend zur Verfügung gestellt werden.
Personalentwicklung	<ul style="list-style-type: none"> ▪ Organisiert die Durchführungen von Schulungen nach der Einstellung, fachbereichsspezifische Schulungen sowie Wiederholungsschulungen und ist für deren Durchführung verantwortlich. ▪ Überprüft die Teilnahme an den Schulungen. ▪ Gewährleistet durch geeignete Maßnahmen die Teilnahme an verpflichtenden Schulungen. ▪ Stellt ein Learning Management System zur Verfügung.
Personalabteilung	<ul style="list-style-type: none"> ▪ Stellt gemeinsam mit dem Hauptabteilungsleiter sicher, dass die Informationen für Beschäftigte ohne technischen Zugang zum Informationsmaterial entsprechend zur Verfügung gestellt werden. ▪ Dokumentiert die Teilnahme der Beschäftigten an den entsprechenden Schulungen in der Personalakte oder einem Learning Management System.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Führt Präsenz- und Web-Schulungen durch, um den Beschäftigten die Gelegenheit für Rückfragen und Klärungen zu geben. ▪ Kann die Schulung ebenfalls durch entsprechend qualifiziertes Schulungspersonal durchführen lassen. ▪ Stellt Informationsmaterial als druckbare Unterlage im Gate oder auf dafür ggf. vorgesehenen Laufwerk-Verzeichnissen zur Verfügung, wenn im Ausnahmefall weder Web- noch Präsenzs Schulungen genutzt werden können. ▪ Stellt Schulungsinhalte zur Verfügung. ▪ Kann bei Bedarf und in Abstimmung thematisch entsprechend zugeschnittene Schulungsinhalte je Beschäftigtengruppe bereitstellen. ▪ Prüft die ordnungsgemäße Durchführung von Schulungen sowie die Dokumentation der Teilnahme an diesen.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Kontrolliert die ordnungsgemäße Durchführung der Schulung. ▪ Berät und überwacht die durch den Verantwortlichen vorgenommenen Maßnahmen in Bezug auf Schulungen. ▪ Führt eigene Schulungen durch.

11 Sonstiges und besondere Verarbeitungssituationen

11.1 Umgang mit Beschäftigtendaten²⁶²

11.1.1 Einleitung

Es ist sicherzustellen, dass die Verarbeitung personenbezogener Daten von Beschäftigten nur in dem erlaubten Umfang und zu den erlaubten Zwecken erfolgt. In der Regel dient die Verarbeitung personenbezogener Daten von Beschäftigten, dem Zwecke des Beschäftigungsverhältnisses, darüber hinaus kann es jedoch auch für andere Zwecke notwendig sein, die Daten von Beschäftigten zu verarbeiten.

11.1.2 Beschreibung

11.1.2.1 Regelfall: Personenbezogene Daten von Beschäftigten

Die nachfolgend beschriebenen Tätigkeiten sind durchzuführen, wenn eine Verarbeitung personenbezogener Daten von Beschäftigten beabsichtigt wird. Die Verarbeitung personenbezogener Daten eines Beschäftigten darf nur auf einer der im Gesetz benannten Fälle beruhen und es müssen geeignete Maßnahmen getroffen werden, durch die eine Verarbeitung unter Beachtung der Datenschutzgrundsätze gewährleistet wird.²⁶³ Beschäftigte sind u.a. Arbeitnehmerinnen und Arbeitnehmer, einschließlich Leiharbeiterinnen und Leiharbeitern im Verhältnis zum Entleiher, sowie Auszubildende.²⁶⁴

In folgenden Fällen ist eine Verarbeitung der Daten von Beschäftigten erlaubt:

- für die Zwecke des Beschäftigungsverhältnisses,
- für die Aufdeckung von Straftaten im Arbeitsverhältnis,
- bei Vorliegen einer geeigneten Einwilligung,
- bei Vorliegen einer geeigneten Kollektivvereinbarung (z. B. Tarifvertrag oder Betriebsvereinbarung).

11.1.2.2 Zwecke des Beschäftigungsverhältnisses

Eine Verarbeitung personenbezogener Daten von Beschäftigten ist zulässig, wenn sie für Zwecke des Beschäftigungsverhältnisses erforderlich ist. Dies ist der Fall, wenn eine Verarbeitung für die Entscheidung über die Begründung, für die Durchführung und für die Beendigung des Beschäftigungsverhältnisses oder für die Ausübung oder Erfüllung der sich aus Gesetz, Tarifvertrag oder Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten notwendig ist. Beispiele hierfür sind Datenverarbeitungsvorgänge zum Zwecke der Lohn- und Gehaltsabrechnung oder die Einstellung von neuen Beschäftigten oder Auszubildenden.²⁶⁵

11.1.2.3 Aufdeckung von Straftaten

Eine Verarbeitung personenbezogener Daten von Beschäftigten ist zulässig, wenn tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung der Straftat zwingend erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt. Eine vorsorgliche Verarbeitung oder die Verarbeitung zum Zwecke der Verdachtserforschung sind grundsätzlich unzulässig.²⁶⁶ Bei der Interessenabwägung ist sicherzustellen, dass Art und Ausmaß der Verarbeitung im Hinblick auf den Anlass der Verarbeitung nicht in einem Missverhältnis zueinanderstehen.²⁶⁷

²⁶² Vgl. Art. 88 DSGVO, § 26 BDSG.

²⁶³ Vgl. § 26 Abs. 8 BDSG für die Definition des Beschäftigten.

²⁶⁴ Vgl. § 26 Abs. 8 BDSG.

²⁶⁵ Vgl. § 26 Abs. 1 S. 1 BDSG.

²⁶⁶ Vgl. Datenschutzkonferenz (DSK), *Kurzpapier Nr. 14 (2020)*, S. 2.

²⁶⁷ Vgl. § 26 Abs. 1 S. 2 BDSG.

Es **müssen** seitens der ermittelnden Stelle (z. B. Personalabteilung, Compliance-Abteilung, Informationssicherheit) geltende Betriebsvereinbarungen berücksichtigt werden. Der zuständige *Datenschutzbeauftragte* und der zuständige *Data Privacy Officer* **müssen** vor Beginn der Ermittlungen hinzugezogen werden.

11.1.2.4 Einwilligung

Im Beschäftigungsverhältnis kommt eine wirksame Einwilligung nur in Ausnahmefällen in Betracht.²⁶⁸ Die Einwilligung des Beschäftigten muss in Textform und freiwillig erteilt worden sein. Eine andere Form der Erteilung ist nur in gesondert gelagerten Fällen möglich. Von der freiwilligen Erteilung ist im Regelfall auszugehen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder der Arbeitgeber und die beschäftigte Person gleichgelagerte Interessen verfolgen, wie beispielsweise die Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder die Erlaubnis zur Privatnutzung der betrieblichen IT-Systeme.

Bei der Beurteilung der Freiwilligkeit müssen insbesondere Faktoren wie die Abhängigkeit des Beschäftigten sowie die Umstände und der Zeitpunkt der Einwilligungserteilung berücksichtigt werden. Die Einwilligung darf nicht aufgrund einer Drucksituation erteilt werden. Beispielsweise ist die betroffene Person vor Abschluss eines Beschäftigungsverhältnisses einem höheren Druck ausgesetzt als nach dessen Abschluss.²⁶⁹ Liegt eine Einwilligung vor, muss die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht in Textform aufgeklärt werden.²⁷⁰ Zuständig sind der Asset- und Prozesseigentümer.

Es **können** zur Bewertung der Freiwilligkeit der Erteilung einer Einwilligung die *Data Privacy Organization* oder der zuständige *Datenschutzbeauftragte* miteinbezogen werden.

11.1.2.5 Kollektivvereinbarung

Eine Verarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses ist auf der Grundlage von Kollektivvereinbarungen zulässig.²⁷¹

Bei der Erstellung von kollektivrechtlichen Vereinbarungen bezogen auf Verarbeitungen personenbezogener Daten **muss** der zuständige *Datenschutzbeauftragte* und der zuständige *Data Privacy Officer* durch den verantwortlichen *Prozesseigentümer/Personalbereich* hinzugezogen werden.

11.1.2.6 Ausnahmefall: Besondere Kategorien personenbezogene Daten von Beschäftigten

Der Prozess ist durchzuführen, wenn eine Verarbeitung besonderer Kategorien personenbezogener Daten von Beschäftigten beabsichtigt wird. Eine solche Verarbeitung ist zulässig, wenn sie für Zwecke des Beschäftigungsverhältnisses erforderlich ist. Dies ist der Fall, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes notwendig ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt.

Bei einer Einwilligung zur Verarbeitung besonderer Kategorien personenbezogener Daten gelten die gleichen Grundsätze wie in Ziffer 4.5.3.2, jedoch sind an die Beurteilung der Freiwilligkeit strengere Maßstäbe zu setzen.

Die *Prozess-* und *Asset-Eigentümer* **können** zur Bewertung der Freiwilligkeit der Erteilung einer Einwilligung die *Data Privacy Organization* und *Datenschutzbeauftragten* miteinbeziehen.

11.1.2.7 Protokollierung von Beschäftigtendaten aus Gründen der Daten-/Informationssicherheit

Personenbezogene Daten, die zum Zweck der Daten-/Informationssicherheit oder zur Sicherstellung eines ordnungsgemäßen Betriebes einer Datenverarbeitungsanlage gespeichert werden, **dürfen** grundsätzlich nur für diese Zwecke verwendet werden.

²⁶⁸ Vgl. Datenschutzkonferenz (DSK), *Kurzpapier Nr. 14 (2020)*, S. 1-2.

²⁶⁹ Vgl. § 26 Abs. 2 DSGVO.

²⁷⁰ Vgl. § 26 Abs. 2 S. 4 BDSG sowie Verweis auf das Widerrufsrecht nach Art. 7 Abs. 3 DSGVO.

²⁷¹ Vgl. § 26 Abs. 4 S. 2 BDSG sowie Verweis auf die Schutzkriterien nach Art. 88 Abs. 2 DSGVO.

Geltende Betriebsvereinbarungen sind zu berücksichtigen.

11.1.3 Dokumentation

Die Verarbeitung personenbezogener Daten von Beschäftigten ist zu dokumentieren. Konkret müssen die einschlägige Fallgruppe, die Einhaltung der jeweiligen Anforderungen, die Art der verarbeiteten Daten, der Verarbeitungszweck und die getroffenen Maßnahmen zur Beachtung der Datenschutzgrundsätze dokumentiert werden. In der Regel wird die Verarbeitung hierzu in das Verzeichnis von Verarbeitungstätigkeiten aufgenommen (siehe Ziffer 5). Außerdem kann es sein, dass ggf. eine Datenschutz-Folgenabschätzung vorab durchzuführen ist (siehe hierzu Ziffer 4.11.2.4).

11.1.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer & Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Gewährleistet die Einhaltung der Datenschutzgrundsätze beim Umgang mit Beschäftigtendaten. ▪ Dokumentiert das Verfahren im Verzeichnis von Verarbeitungstätigkeiten. ▪ Überprüft regelmäßig, ob technische und organisatorische Maßnahmen getroffen wurden, um die Rechte und Freiheiten der betroffenen Person bei einer Verarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten zu wahren. ▪ Prüft, ob die getroffenen Maßnahmen geeignet sind, um die Anforderungen an die Verarbeitung von Beschäftigtendaten zu genügen.
Hauptabteilungsleiter	<ul style="list-style-type: none"> ▪ Stellt die Einhaltung datenschutzrechtlicher Grundsätze beim Umgang mit Beschäftigtendaten sicher.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Unterstützt und berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Unterstützt und berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.²⁷²

11.2 Videoüberwachung (Deutschland)

11.2.1 Einleitung

Soll eine Beobachtung mittels optisch-elektronischen Einrichtungen („Videoüberwachung“) etabliert werden oder besteht ein solches System bereits, so ist sicherzustellen, dass hierbei die strengen und ausdifferenzierten rechtlichen Vorgaben beachtet werden.

In jedem Fall **muss** ein solches System in enger Abstimmung mit dem zuständigen *Datenschutzbeauftragten* und der Data Privacy Organization entwickelt werden.

Jede Videoüberwachung stellt grundsätzlich einen Eingriff in das Persönlichkeitsrecht der betroffenen Personen dar. Sei es, weil die Kontrolle über das eigene Bild nicht mehr vollständig gegeben ist oder weil auch unverdächtige Personen im Wissen um die Aufzeichnung ihr Verhalten entsprechend anpassen (sogenannter „Überwachungsdruck“). Dies gilt im besonderen Maße für die Videoüberwachung von Beschäftigten am Arbeitsplatz.

Eine Videoüberwachung liegt auch schon dann vor, wenn das Videomaterial nicht aufgezeichnet (gespeichert), sondern nur „live“ auf einen Monitor übertragen wird (sogenannter „Fern- oder Echtzeitbeobachtung“). Durch eine Aufzeichnung des Videomaterials entsteht eine zusätzliche Beeinträchtigung der betroffenen Personen.

²⁷² Art. 39 Abs. 1 lit. b DSGVO.

11.2.2 Beschreibung

11.2.2.1 Offene Videoüberwachung

11.2.2.1.1 Zulässige Videoüberwachung

Bei einer „offenen“ Videoüberwachung handelt es sich um eine nach außen erkennbare Videoüberwachung, typischerweise durch eine sichtbar angebrachte Videokamera und/oder einem klaren Hinweis auf eine stattfindende Videoüberwachung (z. B. durch ein Schild am Eingang eines Gebäudes).

Die offene Videoüberwachung ist grundsätzlich zulässig, wenn sie zur Wahrnehmung des Hausrechts (des Unternehmens) oder zur Wahrnehmung berechtigter Interessen (z. B. Prävention oder Aufdeckung von Straftaten oder arbeitsrechtlichen Verfehlungen) für konkret festgelegte Zwecke erforderlich ist. Dabei dürfen schutzwürdige Interessen der betroffenen Personen (gegen die Videoüberwachung) nicht gegenüber dem Interesse des Verantwortlichen (Unternehmen) an der Videoüberwachung überwiegen.²⁷³ Es ist zudem sicherzustellen, dass die Videoüberwachung sowie der Name und die Kontaktdaten des Verantwortlichen durch geeignete Maßnahmen zum frühestmöglichen Zeitpunkt erkennbar gemacht werden.²⁷⁴

Es gelten daher für jede offene Videoüberwachung durch Unternehmen die folgenden generellen Anforderungen:

- Die Videoüberwachung dient der Wahrnehmung konkret festgelegter, **berechtigter Interessen** (einschließlich des Hausrechts) des Unternehmens.
- Die Videoüberwachung ist **erforderlich**, sprich es gibt kein „milderes“ Mittel, das genauso gut geeignet ist, wie die Videoüberwachung (z. B. Pförtner am Eingang statt einer Kamera).
- **Interessenabwägung:** Die berechtigten Interessen des Unternehmens an der Videoüberwachung müssen gegenüber den berechtigten Interessen der betroffenen Personen (insbesondere Beschäftigten) gegen die Videoüberwachung überwiegen.
- **Transparenz:** Die Videoüberwachung und die wesentlichen Informationen zu der damit verbundenen Verarbeitung der personenbezogenen Daten müssen den betroffenen Personen erkennbar gemacht werden (z. B. durch einen klar erkennbaren Aushang).

11.2.2.1.2 Videoüberwachung von öffentlich zugänglichen und öffentlich nicht zugänglichen Räumen

Es ist weiterhin zwischen der Videoüberwachung öffentlich zugänglicher Räume und nicht öffentlich zugänglicher Räume zu unterscheiden. Öffentlich zugänglich sind nur solche Räume bzw. Bereiche, die ihrem Zweck nach dazu bestimmt sind, von einer unbestimmten Zahl oder nach nur allgemeinen Merkmalen bestimmten Personen betreten und genutzt zu werden. Dies ist beispielsweise bei Orten wie der Rezeption, dem Eingangsbereich, dem Parkhaus oder Verkaufsflächen in Warenhäusern der Fall, die für jedermann zugänglich sind.

Räumlichkeiten bzw. Bereiche, die nur für bestimmte Personen zugänglich sind bzw. sein sollen (z. B. nur für Beschäftigte des Unternehmens), sind nicht öffentlich zugänglich (z. B. Büros, Produktionsflächen, Lagerräume).

11.2.2.1.3 Videoüberwachung von Beschäftigten

Die Videoüberwachung von Beschäftigten bzw. am Arbeitsplatz unterliegt besonders strengen Anforderungen.²⁷⁵ Können Beschäftigte von Videoüberwachung betroffen sein, sind v. a. auch geeignete Abstimmungen mit der Mitbestimmung zu treffen. Im Rahmen der Interessenabwägung sind anerkannte Gründe für eine zulässige Videoüberwachung ein besonderes Sicherheitsbedürfnis sowie das Interesse des Arbeitgebers daran, von Arbeitnehmern begangene Straftaten aufzuklären. Hierfür geltende Betriebsvereinbarungen sind zu berücksichtigen.

²⁷³ Bei der Interessenabwägung sind insb. die Kriterien nach Art. 6 Abs. 1 lit. f DSGVO und im Beschäftigtenkontext nach § 26 BDSG zu berücksichtigen. Die normierten Inhalte des § 4 Abs. 1 BDSG können bei der Interessenabwägung herangezogen werden (vgl. BVerwG, Urteil v. 27.03.2019, BVerwG 6 C 2.18).

²⁷⁴ Vgl. Art. 13 DSGVO und § 4 Abs. 2 BDSG.

²⁷⁵ Neben der DSGVO gelten hier die besonderen Regelungen des § 26 BDSG und v. a. die Rechtsprechung der deutschen Arbeitsgerichte.

Videoüberwachungen von Beschäftigten können sich sowohl auf öffentliche (z. B. gleichzeitige Videoüberwachung von Kunden und Personal in Verkaufsflächen) als auch auf nicht-öffentliche (z. B. Büros) Räume beziehen.

Eine ständige Videoüberwachung, die zu einer lückenlosen Beobachtung des Arbeitsplatzes führen würde, der sich der Beschäftigte nicht entziehen kann und die deshalb einen „Überwachungsdruck“ schafft, kann weder auf das Direktionsrecht noch auf das Hausrecht des Arbeitgebers gestützt werden. Die Videoüberwachung ist hier nur dann erlaubt, wenn das Kontrollinteresse des Arbeitgebers gegenüber dem Persönlichkeitsrecht der Beschäftigten überwiegt. Dazu genügt es in der Regel nicht, dass der Arbeitgeber schlicht überprüfen will, ob und wie gearbeitet wird. Vielmehr müssen besonders schutzwürdige Interessen des Arbeitgebers beeinträchtigt sein, etwa durch gegen ihn gerichtete Straftaten (z. B. Diebstahl, Beschädigungen, Unterschlagung, Verrat von Betriebs- und Geschäftsgeheimnissen. Schutz von Beschäftigten in Gefahrenzonen), die das schutzwürdige Interesse der betroffenen Person, nicht einem ständigen Überwachungsdruck ausgesetzt zu sein, deutlich überwiegen. Auch ist zu unterscheiden, ob die Videoüberwachung öffentliche oder nicht öffentliche Räume erfasst.

11.2.2.2 Verdeckte Videoüberwachung

Bei einer „verdeckten“ Videoüberwachung handelt es sich um eine heimliche, nach außen bzw. durch die betroffenen Personen nicht erkennbare Videoüberwachung (z. B. durch versteckte Kameras ohne Hinweise).

Eine verdeckte Videoüberwachung ist (insbesondere bei öffentlichen Räumen) aufgrund der gesetzlichen Informations- und Transparenzpflichten²⁷⁶ grundsätzlich nicht zulässig. Ausnahmsweise kann eine verdeckte Videoüberwachung von Beschäftigten allerdings nach der Rechtsprechung unter sehr engen Voraussetzungen möglich sein.²⁷⁷ Eine verdeckte Videoüberwachung ist ausnahmsweise nur dann zulässig, wenn „der konkrete Verdacht einer strafbaren Handlung oder einer schweren Verfehlung zugunsten des Arbeitgebers besteht, weniger einschneidende Mittel zur Aufklärung des Verdachts ergebnislos ausgeschöpft worden sind, die verdeckte Videoüberwachung damit das praktisch einzig verbleibende Mittel darstellt und sie insgesamt nicht unverhältnismäßig ist.“²⁷⁸ Eine verdeckte Videoüberwachung zu präventiven Zwecken ohne konkreten Verdacht (eine abstrakte Gefahr genügt nicht) ist unzulässig. Es ist außerdem stets zu prüfen, ob statt einer Videoüberwachung andere Formen der Ermittlungen innerhalb des Unternehmens gleich effektiv sind (z. B. die Befragung anderer Beschäftigter, ggf. auch von Kunden oder von Lieferanten).

Eine ausnahmsweise zulässige verdeckte Videoüberwachung sollte mit dem Betriebsrat abgestimmt und auf einen kurzen Zeitraum und möglichst engen räumlichen wie personellen Kreis beschränkt werden.

11.2.2.3 Speicherung und Speicherdauer des Videomaterials

Eine Speicherung der durch die Videoüberwachung erhobenen Daten ist nur zulässig, wenn sie zum Erreichen des verfolgten Zwecks (der berechtigten Interessen) erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der betroffenen Person überwiegen. So können bestimmte Zwecke schon mit einer bloßen Echtzeitüberwachung (z. B. Monitor des Pförtners) auch ohne Speicherung des Videomaterials erreicht werden.

Die Daten der Videoüberwachung sind unverzüglich zu löschen, wenn sie zur Erreichung der Zwecke, für die sie erhoben wurden, nicht mehr notwendig sind oder schutzwürdige Interessen der betroffenen Personen einer weiteren Speicherung entgegenstehen. Ob eine Sicherung des Materials notwendig ist, sollte grundsätzlich innerhalb von ein bis zwei Tagen geklärt werden können (z. B. Feststellung von Diebstahl oder Schäden). Unter Berücksichtigung der Grundsätze der „Datenminimierung“²⁷⁹ und „Speicherbegrenzung“²⁸⁰ sollte demnach grundsätzlich nach 48 Stunden eine Löschung erfolgen.²⁸¹ In begründeten Einzelfällen kann jedoch auch eine

²⁷⁶ Vgl. insb. Art. 13 DSGVO.

²⁷⁷ Siehe hierzu die Grundsatzurteile des Bundesarbeitsgerichts BAG, Beschluss vom 29.06.2004 – 1 ABR 21/03 und BAG, Urteil vom 20.10.2016 – 2 AZR 395/15 sowie des Europäischen Gerichtshofs für Menschenrechte EGMR, Urteil vom 01.09.2018 – 1874/13, 8567/13.

²⁷⁸ BAG, Urteil vom 20.10.2016 – 2 AZR 395/15.

²⁷⁹ Vgl. Art. 5 Abs. 1 lit. c DSGVO.

²⁸⁰ Vgl. Art. 5 Abs. 1 lit. e DSGVO.

²⁸¹ So die klare Position der deutschen Aufsichtsbehörden, vgl. Datenschutzkonferenz (DSK), Kurzpapier Nr. 15 zur Videoüberwachung vom 17.12.2018, S. 3.

darüber hinausgehende Speicherdauer zulässig sein. Unter Berücksichtigung von Wochenenden, Feiertagen und Brückentagen können ausnahmsweise auch bis zu einer Woche zulässig sein.

Je länger die Speicherfrist ist, desto höher ist der Argumentationsaufwand in Bezug auf die Rechtmäßigkeit und Erforderlichkeit. Das gilt insbesondere, wenn sie **mehr als 72 Stunden** beträgt.²⁸²

Die Speicherdauer muss stets klar definiert und für jeden bestimmten Zweck einzeln festgelegt werden. Es liegt in der Verantwortung des Verantwortlichen, den Aufbewahrungszeitraum im Einklang mit den Grundsätzen der Erforderlichkeit und Verhältnismäßigkeit festzulegen und die Einhaltung der Bestimmungen der DSGVO nachzuweisen. Wird ein Schaden festgestellt, kann das Videomaterial (der relevante Ausschnitt) grundsätzlich länger gespeichert werden, um rechtliche Schritte gegen den Verdächtigen einleiten zu können.²⁸³

11.2.2.4 Ausschluss Videoüberwachung

Die Videoüberwachung in einem gegen Einblick besonders geschützten Raum, beispielsweise der Toilettenbereich oder die Umkleiden, ist verboten und ggfs. sogar strafbar.²⁸⁴

11.2.2.5 Transparenz und Informationspflicht

Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, muss diese entsprechend informiert werden (gilt insbesondere für Dritte in öffentlichen Räumen).²⁸⁵ Bei Beschäftigten ist stets davon auszugehen, dass sie durch den Arbeitgeber (sogar in Echtzeit) identifiziert und zugeordnet werden können, weshalb hier immer die Informationspflichten²⁸⁶ greifen (siehe hierzu auch den Prozess zu den Informationspflichten, vgl. Ziffer 4.6). Diese Informationspflichten können z. B. durch einen geeigneten (vollständigen) Aushang am Ort der Videoüberwachung²⁸⁷ oder durch Aushändigung der relevanten Datenschutzinformationen an die Beschäftigten erfüllt werden.

Die Informationspflicht kann im seltenen Ausnahmefall einer verdeckten Videoüberwachung entfallen, beispielsweise wenn durch die Information die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigt werden und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.²⁸⁸

Zuständig für den Einsatz von Videoüberwachungsmaßnahmen ist grundsätzlich die Unternehmenssicherheit.

Bei der Beurteilung des Einsatzes einer Videoüberwachung **muss** die *Data Privacy Organization* hinzugezogen werden.

11.2.2.6 Verwendung der Videodaten

Die Verwendung der Videodaten mit möglichem Bezug zu Beschäftigten unterliegt den Regelungen, die mit den Betriebsverfassungsorganen abgestimmt sind. Die Verwendung von Videodaten aus öffentlich zugänglichen Räumen erfolgt u.a. nach Rücksprache mit dem zuständigen *Data Privacy Officer* oder dem zuständigen *Datenschutzbeauftragten*.

Die Verwendung der Videodaten bei akutem Handlungsbedarf muss durch die Unternehmenssicherheit geregelt werden, z. B. bei Gefahr im Verzug, obliegt i. d. R. dem *Sicherheitsdienst/Objektschutz*, **muss** eigens dokumentiert werden und erfordert die Information u. a. des zuständigen *Data Privacy Officers* und des zuständigen *Datenschutzbeauftragten*.

²⁸² So der Europäische Datenschutzausschuss (EDSA), Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte vom 29.01.2020, S. 30.

²⁸³ Europäische Datenschutzausschuss (EDSA), Leitlinien 3/2019 zur Verarbeitung personenbezogener Daten durch Videogeräte vom 29.01.2020, S. 30.

²⁸⁴ Vgl. § 201 a StGB.

²⁸⁵ Vgl. § 4 Abs. 4 BDSG.

²⁸⁶ Vgl. Art. 13 DSGVO.

²⁸⁷ Datenschutzkonferenz (DSK), Kurzpapier Nr. 15 zur Videoüberwachung vom 17.12.2018, S. 3.

²⁸⁸ Vgl. § 32 Abs. 1 Nr. 4 BDSG. Zu beachten sind zudem die Ausschlussstatbestände zu Art. 13 und 14 DSGVO sowie § 32 Abs. 1 BDSG.

11.2.3 Dokumentation

Die Videoüberwachung ist in einem Konzept zu dokumentieren. In der Dokumentation sind Inhalt und Umstand der Videoüberwachung zu hinterlegen. Konkret müssen hierzu für jede Kamera insbesondere die Blickwinkel, die überwachten Räume, der konkrete Zweck der Überwachung einschließlich der Abwägung der widerstreitenden Interessen, welche Abhilfemaßnahmen erwogen und getroffen wurden, die Erfüllung der Hinweis- und Informationspflicht sowie die Löschung der durch die Videoüberwachung erhobenen Daten dokumentiert werden.

Im Übrigen handelt es sich bei nahezu jeder Videoüberwachung um eine Verarbeitung personenbezogener Daten, für die eine entsprechende Datenschutzdokumentation zu erstellen ist (vgl. Ziffer 5).

11.2.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer & Asset-Eigentümer <i>(i.d.R. Unternehmenssicherheit/Werkschutz)</i>	<ul style="list-style-type: none"> ▪ Stellt sicher, dass die Anforderungen des Datenschutzes bei der Durchführung der Videoüberwachung beachtet werden. ▪ Dokumentiert die Überwachung in einem Konzept. ▪ Dokumentiert das Verfahren im Verzeichnis von Verarbeitungstätigkeiten. ▪ Prüft, ob der Anlass und die Durchführung der Videoüberwachung noch erforderlich ist. ▪ Prüft, ob die getroffenen Abhilfemaßnahmen weiterhin geeignet sind. ▪ Prüft, ob die erforderlichen Datenschutzinformationen an geeigneten Stellen vorhanden (z. B. Hinweisschilder) und die Videoüberwachungskonzepte aktuell sind. ▪ Muss vor einer etwaigen Verwendung von Videodaten (z. B. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen) den zuständige Data Privacy Officer einbinden.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.²⁸⁹

11.3 Automatisierte Entscheidungen im Einzelfall (einschließlich Profiling)

11.3.1 Einleitung

Es ist sicherzustellen, dass eine automatisierte Entscheidung (d. h. ohne menschliches Einwirken), die gegenüber der betroffenen Person eine rechtliche Wirkung entfaltet oder sie in ähnlicher Weise erheblich beeinträchtigt, nur unter besonderen Voraussetzungen erfolgt. Auch das bilden von Profilen (Profiling) unterliegt entsprechenden Anforderungen.

Ist die Einführung eines Verfahrens zur automatisierten Entscheidung geplant oder sollen Profile von Betroffenen erstellt werden (Profiling), **muss** geprüft werden, ob eine Datenschutz-Folgenabschätzung (DSFA) durchgeführt werden (siehe Ziffer 4.11.2.4) **muss**.²⁹⁰ Der *Prozesseigentümer* **muss** den zuständige *Data Privacy Officer* rechtzeitig miteinbeziehen.

11.3.2 Beschreibung

11.3.2.1 Erläuterung: Vollautomatisierte Entscheidung und Profiling

Grundsätzlich kommt nach derzeitigen Erkenntnissen die automatisierte Entscheidung bei Rheinmetall nicht vor. Sollten automatisierte Entscheidungen vorkommen wird die Data Privacy Organization entsprechende Richtlinien zum datenschutzkonformen Umgang erlassen.

„Profiling“ bezeichnet jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine

²⁸⁹ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

²⁹⁰ Vgl. Art. 35 Abs. 3 lit. a DSGVO.

natürliche Person beziehen, zu bewerten. Dies dient insbesondere dazu, Aspekte bezüglich der Arbeitsleistung, wirtschaftlichen Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen.

11.3.3 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none"> ▪ Muss den zuständigen Data Privacy Officer miteinbeziehen, sofern die Einführung eines Verfahrens zur automatisierten Entscheidung oder Profiling geplant ist.
Datenschutz-Koordinator	<ul style="list-style-type: none"> ▪ Prüft und unterstützt den Prozesseigentümer, bei der Prüfung, Kontrolle und Dokumentation entsprechender Verarbeitungen.
Data Privacy Officer	<ul style="list-style-type: none"> ▪ Erlässt eine entsprechende Richtlinie. ▪ Unterstützt und berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.²⁹¹

11.4 Wissenschaftliche oder historische Forschungszwecke und statistische Zwecke

11.4.1 Einleitung

Es ist sicherzustellen, dass bei einer Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken bestimmte Mindestanforderungen erfüllt werden.

11.4.2 Beschreibung

11.4.2.1 Regelfall

Dieser Prozess ist eine Spezifizierung der allgemeinen Vorgaben für die Verarbeitung personenbezogener Daten. Er ist durchzuführen, wenn eine Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken beabsichtigt wird. Im Regelfall wird die statistische Verarbeitung von Unternehmensdaten den Anlass zur Bearbeitung geben.

Es muss durch angemessene technische und organisatorische Maßnahmen sichergestellt werden, dass die Rechte und Freiheiten der betroffenen Person gewahrt werden. Dafür muss im Kern geregelt werden, dass die Personenbeziehbarkeit in den statistischen Daten nur im Rahmen der zulässigen Zweckbestimmungen vorhanden sein darf und auch nur so lange, wie sie dafür erforderlich ist.. Dies kann beispielsweise durch eine Pseudonymisierung oder Anonymisierung erfolgen, wenn eine solche Maßnahme nicht dem Zweck der Verarbeitung entgegensteht.²⁹² Wird die statistische Verarbeitung mittels anonymisierter Daten durchgeführt, sind diese für den Datenschutz mangels Personenbezugs der Daten nicht mehr relevant.

„Statistische Zwecke“ umfassen jeden für die Durchführung statistischer Untersuchungen und die Erstellung statistischer Ergebnisse erforderlichen Vorgang der Erhebung und Verarbeitung personenbezogener Daten.²⁹³ Unter Statistik wird allgemein der methodische Umgang mit empirischen Daten verstanden. Im Zusammenhang mit den statistischen Zwecken wird vorausgesetzt, dass die Ergebnisse der Verarbeitung zu statistischen Zwecken keine personenbezogenen Daten, sondern aggregierte Daten sind und diese Ergebnisse oder personenbezogenen Daten nicht für Maßnahmen oder Entscheidungen gegenüber einzelnen natürlichen Personen verwendet werden.²⁹⁴

²⁹¹ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

²⁹² Vgl. Art. 89 Abs. 1 DSGVO.

²⁹³ Vgl. ErwGr. 162 DSGVO.

²⁹⁴ Vgl. ErwGr. 162 DSGVO.

Die Daten **müssen** durch geeignete Maßnahmen seitens des *Prozesseigentümers* anonymisiert werden, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist und keine berechtigten Interessen der betroffenen Person entgegenstehen.²⁹⁵

Zudem können auch die Rechte der betroffenen Personen auf Datenauskunft und auf Einschränkung der Verarbeitung in diesem Fall begrenzt sein.²⁹⁶ Dies ist dann der Fall, wenn sie voraussichtlich die Verwirklichung der Statistikzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Beschränkung für die Erfüllung der Statistikzwecke notwendig ist.

Statistische Zwecke enden dort, wo eine Zuordnung der statistischen Ergebnisdaten zu einer konkreten Person erfolgt. Es ist sicherzustellen, dass in den Ergebnisdaten kein Personenbezug mehr vorhanden ist. Falls im Rahmen des statistischen Prozesses Personenbezüge entstehen, dürfen diese nicht gegenüber diesen Personen für Maßnahmen oder Entscheidungen verwendet werden, solange hierfür keine zulässige Zweckbestimmung und Erforderlichkeit gegeben ist. Die aggregierten Ergebnisse einer statistischen Verarbeitung können z. B. für die Tarifierung oder für das Risikomanagement verwendet werden. Sollen die Ergebnisse einer Statistik oder daraus entwickelte Tarife jedoch konkret auf eine einzelne Person angewendet werden, müssen für die Verwendung der hierfür benötigten personenbezogener Daten die allgemeinen Rechtfertigungstatbestände²⁹⁷ herangezogen werden²⁹⁸.

11.4.2.2 Ausnahmefall: Besondere Kategorien personenbezogener Daten

Eine Verarbeitung besonderer Kategorien personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken ist ohne Einwilligung der betroffenen Person zulässig, wenn die Verarbeitung zu den genannten Zwecken erforderlich ist, die Interessen des Verantwortlichen gegenüber den Interessen der betroffenen Person überwiegen und der Verantwortliche angemessene und spezifische Maßnahmen zur Wahrung der Interessen der betroffenen Person getroffen hat.²⁹⁹ Solche Maßnahmen sind u. a.:

- Technische und organisatorische Maßnahmen (TOM), die sicherzustellen, dass die Verarbeitung datenschutzkonform erfolgt,
- Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind (z. B. Änderungshistorie, Protokollierung),
- Sensibilisierung der an Verarbeitungsvorgängen Beteiligten,
- Benennung eines Datenschutzbeauftragten,
- Strenge Beschränkung des Zugangs zu den personenbezogenen Daten,
- Pseudonymisierung personenbezogener Daten,
- Verschlüsselung personenbezogener Daten,
- Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschließlich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen,
- zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der TOM oder
- spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke sicherzustellen, dass die Verarbeitung datenschutzkonform erfolgt.

Eine solche Entscheidung **darf nicht** ohne Rücksprache mit dem zuständigen *Data Privacy Officer* oder *Datenschutzbeauftragten* getroffen werden.

11.4.3 Dokumentation

Die Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken ist zu dokumentieren. Konkret

²⁹⁵ Vgl. § 27 Abs. 3 BDSG auch zum Vorgehen bis zum Zeitpunkt der Anonymisierung der Daten.

²⁹⁶ Vgl. Art. 89 Abs. 3 DSGVO, § 27 Abs. 2 DSGVO, § 28 Abs. 2, 3, 4.

²⁹⁷ Insb. Art. 6 und 9 DSGVO.

²⁹⁸ Vgl. ErwGr. 162 DSGVO.

²⁹⁹ Vgl. § 27 Abs. 1 BDSG sowie § 22 Abs. 2 S. 2 BDSG.

müssen hierzu insbesondere der Zweck der Verarbeitung und die getroffenen TOM zur Wahrung der Rechte und Freiheiten der betroffenen Person im Verzeichnis von Verarbeitungstätigkeiten dokumentiert werden.

Werden besondere Kategorien personenbezogener Daten zu den oben genannten Zwecken verarbeitet, so sind das Erfordernis der Verarbeitung und die getroffenen angemessenen und spezifischen Maßnahmen zu dokumentieren.

11.4.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer bzw. Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Hält die Mindestanforderungen der Verarbeitung personenbezogener Daten zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken sowie die Voraussetzungen der Verarbeitung besonderer Kategorien personenbezogener Daten ein. ▪ Dokumentiert das Verfahren im Verzeichnis von Verarbeitungstätigkeiten. ▪ Prüft regelmäßig, ob TOM ergriffen wurden, um die Rechte und Freiheiten der betroffenen Person bei einer Verarbeitung personenbezogener Daten und besonderer Kategorien personenbezogener Daten zu wahren. ▪ Prüft regelmäßig, ob die getroffenen Maßnahmen geeignet sind, um den oben dargestellten Anforderungen Rechnung zu tragen.
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Unterstützt und berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Berät bei Bedarf zur Einführung solcher Verfahren und Vorgehensweisen. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.

11.5 Zusammenarbeit mit der Datenschutz-Aufsichtsbehörde

11.5.1 Einleitung

Es ist sicherzustellen, dass auf Anfrage eine Zusammenarbeit mit den Aufsichtsbehörden bei der Erfüllung ihrer Aufgaben erfolgt.

Der *Data Privacy Officer* und der Datenschutzbeauftragte **müssen** bei jeder Kontaktaufnahme der Datenschutz-Aufsichtsbehörden unverzüglich informiert werden.

11.5.2 Beschreibung

11.5.2.1 Zusammenarbeit mit der Datenschutz-Aufsichtsbehörde

Wendet sich die Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben an ein Unternehmen im Rheinmetall Konzern als Verantwortlichen oder Auftragsverarbeiter, so muss diese hierbei unterstützt werden. Die Unterstützung erfolgt auf Grundlage der Kooperationspflicht gegenüber der Aufsichtsbehörde. Diese kann beispielsweise darin bestehen, der Aufsichtsbehörde alle angefragten Informationen bereitzustellen oder Untersuchungen in Form von Datenschutzüberprüfungen zu dulden.³⁰⁰

Soweit die Aufsichtsbehörde eine Frist zur Erfüllung der Anforderung setzt, **muss** eine Reaktion binnen dieser Frist erfolgen.

11.5.2.2 Überschreitung der aufsichtsrechtlichen Kompetenzen

Die Zusammenarbeit mit der Aufsichtsbehörde ist nur erforderlich, soweit diese zur Erfüllung ihrer Aufgaben tätig wird. Sollten Zweifel an der Rechtmäßigkeit des aufsichtsbehördlichen Verlangens bestehen, ist der zuständige Data Privacy Officer oder Datenschutzbeauftragte zu informieren. Dies gilt z.B. bei drohender Verletzung von anderen Verschwiegenheits- oder Geheimhaltungspflichten.

³⁰⁰ Siehe Art. 58 Abs. 1 DSGVO zu den Befugnissen der Aufsichtsbehörde.

11.5.3 Dokumentation

Die erfolgte Zusammenarbeit mit der Aufsichtsbehörde ist zu dokumentieren. In dem genutzten Archivsystem sind das Datum und der Inhalt der Anfrage der Aufsichtsbehörde sowie die jeweils erfolgte Reaktion zu dokumentieren.

11.5.4 Rollen und Verantwortung

Rolle	Verantwortung
Adressat der Anfrage / kontaktierte Stelle i.d.R. Adressat/Empfänger der E-Mail/des Briefs	<ul style="list-style-type: none"> Ist verantwortlich für die Zusammenarbeit mit der Aufsichtsbehörde. Leitet entsprechende Anfragen unverzüglich an den Datenschutzbeauftragten und den Data Privacy Officer weiter.
Data Privacy Officer	<ul style="list-style-type: none"> Prüft, ob geeignete technische und organisatorische Maßnahmen vorhanden sind, um eine effektive Zusammenarbeit mit der Aufsichtsbehörde zu gewährleisten. Organisiert interne Zuständigkeiten so, dass innerhalb der gesetzten Frist eine geeignete Reaktion an die Aufsichtsbehörde erfolgen kann. Unterstützt den Datenschutzbeauftragten vollumfänglich. Dokumentiert die erfolgte Zusammenarbeit mit der Aufsichtsbehörde gemeinsam mit dem Datenschutz-Koordinator.
Datenschutzbeauftragter	<ul style="list-style-type: none"> Obliegt per Gesetz die Zusammenarbeit mit der Aufsichtsbehörde.³⁰¹

11.6 Vorherige Konsultation

11.6.1 Einleitung

Steht als Ergebnis der DSFA fest, dass die geplante Datenverarbeitung ein hohes Risiko für Betroffene zur Folge hat, das der Verantwortliche nicht durch geeignete Maßnahmen eindämmen kann, **muss** die zuständige Aufsichtsbehörde konsultiert werden.

11.6.2 Beschreibung

11.6.2.1 Regelfall

Sollte die zuständige Aufsichtsbehörde zum Zweck der Konsultation kontaktiert werden, müssen dieser in einer informierten Stellungnahme die folgenden Informationen zur Verfügung gestellt werden:

- Angaben zu den Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter, falls der Verantwortliche die Verarbeitung nicht eigenständig vornimmt,
- Zweck und Mittel der beabsichtigten Verarbeitung,
- die zum Schutz der Rechte und Freiheiten der betroffenen Personen gemäß der DSGVO vorgesehenen Maßnahmen und Garantien,
- Kontaktdaten des Datenschutzbeauftragten, falls ein solcher benannt wurde sowie
- die Dokumentation der durchgeführten Datenschutz-Folgenabschätzung,
- Je nach Einzelfall können weitere Informationen mitzuteilen sein (Beispiel: Verträge oder Programm-codes).³⁰²

Die Aufsichtsbehörde hat nach Eingang der Mitteilung acht Wochen Zeit, um eine Stellungnahme abzugeben.³⁰³

³⁰¹ Art. 39 Abs. 1 lit d DSGVO.

³⁰² Informationen nach Art. 36 Abs. 3 DSGVO.

³⁰³ Vgl. Art. 36 Abs. 2 DSGVO.

11.6.2.2 Ausnahmefall: Verlängerte Frist zur Stellungnahme

Die Frist der Stellungnahme kann um bis zu sechs Wochen verlängert werden, wenn die geplante Verarbeitung einen höheren Grad an Komplexität aufweist. Über diese Verlängerung muss die Aufsichtsbehörde den Verantwortlichen vier Wochen nach Eingang der Konsultation unterrichten und eine Begründung beifügen.³⁰⁴

11.6.3 Dokumentation

Die Durchführung der vorherigen Konsultation ist zu dokumentieren. Dies erfolgt in dem Verzeichnis der Verarbeitungstätigkeiten zu der jeweiligen Verarbeitung und umfasst insbesondere den Inhalt und den Zeitpunkt der Mitteilung an die Aufsichtsbehörde sowie die Reaktion.

11.6.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer	<ul style="list-style-type: none"> ▪ Prüft mit dem Data Privacy Officer die Ergebnisse der durchgeführten DSFA in Hinblick auf eine vorherige Konsultation und initiiert sowie dokumentiert die Entscheidung zur jeweiligen DSFA. ▪ Kann den Datenschutzbeauftragten auffordern, die Konsultation mit der Aufsichtsbehörde vorzunehmen. ▪ Dokumentiert die Durchführung der vorherigen Konsultation im Verzeichnis von Verarbeitungstätigkeiten zur entsprechenden Verarbeitung.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Obliegt per Gesetz die Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Datenverarbeitung zusammenhängenden Fragen. Hierzu zählt auch die vorherige Konsultation der Aufsichtsbehörde.³⁰⁵ ▪ Kann nach Anforderung durch den Prozesseigentümer die Konsultation mit der Aufsichtsbehörde vornehmen.
Data Privacy Officer	<ul style="list-style-type: none"> ▪ Unterstützt und berät den Prozesseigentümer bei der Vorbereitung und Durchführung der Konsultation

11.7 Verhaltensregeln

11.7.1 Einleitung

Es ist sicherzustellen, dass Verhaltensregeln zur Förderung der Durchführung datenschutzrechtlicher Regelungen, welche auch als "Code of Conduct" bezeichnet werden, befolgt werden. Verhaltensregeln erfahren in der Regel eine planmäßige Fortschreibung und Weiterentwicklung.

11.7.2 Beschreibung

Für die Branchen, in denen der Rheinmetall Konzern tätig ist, gibt es einen solchen Code of Conduct nicht.

11.7.3 Rollen und Verantwortung

Rolle	Verantwortung
Data Privacy Organization	<ul style="list-style-type: none"> ▪ Prüft regelmäßig, ob ein „Code of Conduct“ für das jeweilige Unternehmen Gültigkeit erlangt hat.
Data Privacy Officer	<ul style="list-style-type: none"> ▪ Beobachtet und berät bei Bedarf zum Umgang mit einem „Code of Conduct“.
Datenschutzbeauftragter	<ul style="list-style-type: none"> ▪ Beobachtet und berät bei Bedarf zum Umgang mit einem „Code of Conduct“. ▪ Ist überwachend tätig, er hat keine durchführende Rolle.³⁰⁶

³⁰⁴ Vgl. Art. 36 Abs. 2 DSGVO.

³⁰⁵ Art. 39 Abs. 1 lit. e DSGVO.

³⁰⁶ Vgl. Art. 39 Abs. 1 lit. b DSGVO.

11.8 Webseiten und Social-Media-Auftritte

11.8.1 Einleitung

Bei Gestaltung und Betrieb von Webseiten und Social-Media-Auftritten (nachfolgend auch kurz „Internetpräsenzen“) müssen stets die datenschutzrechtlichen Anforderungen berücksichtigt werden. Hierfür ist es unerlässlich, ein klares und vollständiges Bild über die verschiedenen Verarbeitungen personenbezogener Daten auf den jeweiligen Internetpräsenzen zu erlangen. Durch die Integration verschiedener technischer Funktionen bzw. Dienste (v. a. von Drittanbietern wie z. B. Google, Twitter und Facebook) auf Webseiten finden oftmals Verarbeitungstätigkeiten statt, die nicht auf Anhieb ersichtlich sind. Dies betrifft insbesondere auch den Einsatz von sogenannten Cookies und anderen Tracking Tools, die häufig personenbezogene Daten der Webseitenbesucher erfassen (z. B. Analyse der Webseitenutzung inklusive IP-Adresse) und an Drittanbieter (z. B. Google in den USA) übermitteln. Inzwischen unterliegt der Einsatz solcher Cookies/Tracking Tools besonders strengen datenschutzrechtlichen Vorgaben. Bei Social-Media-Auftritten (z. B. Unternehmensseite auf Facebook) liegt zudem in bestimmten Fällen eine sogenannte gemeinsame datenschutzrechtliche Verantwortlichkeit³⁰⁷ zusammen mit dem Social-Media-Plattformbetreiber (z. B. Facebook) vor.

Außerdem bedarf jede Internetpräsenz einer präzisen, transparenten, verständlichen sowie vollständigen Datenschutzhinweise, die den Besuchern jederzeit leicht zugänglich ist und ein klares Bild über die verschiedenen Verarbeitungen ihrer personenbezogenen Daten auf der jeweiligen Internetpräsenz vermittelt.³⁰⁸

11.8.2 Beschreibung

11.8.2.1 Datenschutzkonforme Gestaltung von Webseiten

11.8.2.1.1 Überblick wesentlicher Aspekte

Für die datenschutzkonforme Gestaltung von Webseiten sind zahlreiche Aspekte zu berücksichtigen. Hierzu stellt die Data Privacy Organization geeignete Checklisten zur Verfügung.

Der *Prozesseigentümer* **muss** die erforderlichen Informationen entsprechend den Checklisten der *Data Privacy Organization* zur Verfügung stellen und die Vorgaben zur datenschutzkonformen Gestaltung einhalten.

11.8.2.1.2 Einsatz von Cookies

Cookies sind Textdateien, die auf dem Endgerät (Computer, Smartphone) des Webseitenbesuchers gespeichert werden und die z. B. eine Individualisierung/Anpassung der Webseite an bestimmte Präferenzen, eine automatische Wiedererkennung der Person beim nächsten Besuch, eine ordnungsgemäße Funktion der Webseite oder eine Analyse der Benutzung der Webseite ermöglichen. Mithilfe von Cookies können Website-Betreiber (First-Party-Cookies) oder Dritte (Third-Party-Cookies) bestimmte Informationen vom Endgerät des Besuchers auslesen. Individuelle Kennungen (IDs) ermöglichen es insbesondere, den Nutzer wiederzuerkennen, teilweise über unterschiedliche Webseiten und Geräte hinweg.

Seit der neusten Rechtsprechung³⁰⁹ gilt für die meisten Cookies ein Einwilligungserfordernis. Lediglich der Einsatz von Cookies, die für die korrekte Funktion einer Webseite unbedingt notwendig sind, können noch weiterhin ohne aktive Einwilligung des Webseitenbesuchers platziert werden (sogenannte notwendige Cookies bzw. Funktionscookies). Für alle anderen Cookies (insbesondere Analyse-, Tracking- und Werbecookies) gilt nunmehr die Pflicht, eine vorherige aktive Einwilligung (Opt-in) vom Webseitenbesucher (z. B. über eine aktive Auswahl in einem Cookie-Banner) einzuholen. Das Nichtabwählen eines voreingestellten Ankreuzkästchens (Opt-out) gilt hierbei nicht als wirksame aktive Einwilligung. Dabei spielt es auch keine Rolle, ob mit den Cookies tatsächlich personenbezogene Daten erhoben werden. Es zählt allein die Platzierung eines Cookies auf dem Endgerät des Besuchers.³¹⁰ Hierzu stellt die Data Privacy Organization geeignete Checklisten zur Verfügung.

³⁰⁷ Vgl. Art. 26 DSGVO.

³⁰⁸ Vgl. Art. 12-14 DSGVO.

³⁰⁹ Vgl. BGH, Urteil vom 28. Mai 2020 - I ZR 7/16 - Cookie-Einwilligung II; EuGH, Urteil vom 1. Oktober 2019, C-673/17 - Planet49.

³¹⁰ Die Cookie-Regelungen beruhen primär auf dem Telemediengesetz (TMG) bzw. der europäischen ePrivacy-Richtlinie und nur sekundär auf der DSGVO.

Der *Prozesseigentümer* **muss** die erforderlichen Informationen entsprechend den Checklisten der *Data Privacy Organization* zur Verfügung stellen und die Vorgaben zur datenschutzkonformen Gestaltung einhalten.

11.8.2.1.3 Exkurs: Web Analytics und Tracking

Google Analytics ist beispielsweise ein Trackingtool des US-amerikanischen Unternehmens Google und gehört zu den am weitesten verbreiteten Tools für Webseiten-Betreiber. Mit Hilfe dieser Tools lassen sich umfassende statistische Auswertungen der Webseitennutzung vornehmen. Diese Tools untersuchen u. a. die Herkunft der Webseiten-Besucher, ihre Verweildauer und Interaktionen auf einzelnen Webseiten (inkl. Unterseiten) sowie die Nutzung von Suchmaschinen und erlaubt damit insbesondere eine bessere Erfolgskontrolle von Werbekampagnen sowie Reichweitenmessungen. Beim Einsatz von Tools zur Webanalyse (Web Analytics) werden immer personenbezogene Daten der Webseitenbesucher (insbesondere Nutzungsdaten und sonstige gerätespezifische Daten, die einem bestimmten Nutzer zugeordnet werden können) erfasst.³¹¹

Aufgrund des komplexen Verarbeitungsumfangs und der Datenübermittlungen an das US-amerikanische Unternehmen Google ist der Einsatz von Google Analytics datenschutzrechtlich höchst problematisch und nur unter sehr engen Voraussetzungen möglich.

Vom Einsatz von Google Analytics im Rheinmetall Konzern wird **dringend abgeraten**.

Soll Web Analytics zum Einsatz kommen, so **muss** der zuständige *Data Privacy Officer* frühzeitig eingebunden werden.

Eine datenschutzfreundlichere Alternative zu Web Analytics stellt das kostenlose Webanalyse-Tool *Matomo* (vormals Piwik) dar.

11.8.2.1.4 Einbindung des Datenschutzes

Aufgrund des Umfangs und der Komplexität wird auf eine vertiefte Darstellung weiterer datenschutzrechtlicher Einzelheiten zur Webseitengestaltung in diesem Handbuch verzichtet.

Bei der Gestaltung von neuen Webseiten sowie bei nicht bloß redaktionellen Änderungen an bestehenden Webseiten **muss** stets der zuständige *Data Privacy Officer* eingebunden werden. Dies gilt insbesondere auch für die Erstellung, Überarbeitung und Aktualisierung der erforderlichen Datenschutzinformationen (vgl. Ziffer 4.6).

11.8.2.2 Datenschutzkonforme Gestaltung von Social-Media-Auftritten

Neben den üblichen datenschutzrechtlichen Anforderungen ist bei Social-Media-Auftritten insbesondere zu prüfen, welches Datenschutzverhältnis zum jeweiligen Social-Media-Anbieter (z. B. Facebook, LinkedIn, Xing, Twitter) besteht.

Nach aktueller Rechtsprechung und Position der Datenschutzaufsichtsbehörden sind speziell die Inhaber von sogenannten „Facebook-Fanpages“ (einschließlich Unternehmensauftritte auf Facebook) für die durch Facebook erfolgende Datenverarbeitung datenschutzrechtlich mitverantwortlich, denn der Inhaber ermöglicht durch den Betrieb der Fanpage Facebook erst den Zugriff auf die Daten der Fanpage-Besucher (unerheblich ist dabei, ob der Besucher ein Facebook-Konto besitzt oder nicht). Folglich liegt in solchen Konstellationen eine gemeinsame Verantwortlichkeit³¹² zwischen Facebook und dem Inhaber des Unternehmensauftritts auf Facebook vor.³¹³ Der Umstand, dass ein Betreiber einer Fanpage die von Facebook eingerichtete Plattform nutzt, um die dazugehörigen Dienstleistungen in Anspruch zu nehmen, könne – so der EuGH – diesen nämlich nicht von der Beachtung seiner Verpflichtungen im Bereich des Schutzes personenbezogener Daten befreien.³¹⁴ Kritisch ist insbesondere

³¹¹ Vgl. Datenschutzkonferenz (DSK), Hinweise zum Einsatz von Google Analytics im nichtöffentlichen Bereich vom 12.05.2020, S. 2.

³¹² Vgl. Art. 26 DSGVO.

³¹³ Vgl. EuGH, Urteil vom 05.06.2018 - C-210/16 (Facebook Fanpages); BVerwG 6 C 15.18 - Urteil vom 11. September 2019; DSK, Positionierung zur Verantwortlichkeit und Rechenschaftspflicht bei Facebook-Fanpages sowie der aufsichts-behördlichen Zuständigkeit v. 01.04.2019.

³¹⁴ EuGH, Urteil vom 05.06.2018 - C-210/16 (Facebook Fanpages), Rn. 40.

ist das Tracking von nicht „Facebook-Nutzern“ bei Besuch der Fanpage. Hierzu stellt die Data Privacy Organization geeignete Checklisten zur Verfügung.

Sollten Social-Media-Auftritte zum Einsatz kommen, **muss** der *Data Privacy Officer* durch den *Prozesseigentümer* eingebunden werden.

Der *Prozesseigentümer* **muss** die erforderlichen Informationen entsprechend den Checklisten der *Data Privacy Organization* zur Verfügung stellen und die Vorgaben zur datenschutzkonformen Gestaltung einhalten.

Social-Media-Auftritte **dürfen** nur nach expliziter Freigabe durch die zuständige Geschäftsführung eingesetzt werden.

Aufgrund des Umfangs und der Komplexität wird auf eine vertiefte Darstellung weiterer datenschutzrechtlicher Einzelheiten zur Gestaltung von Social-Media-Auftritten in diesem Handbuch verzichtet. Ein Betrieb von Social-Media-Auftritten ist ohne ein Datenschutz Compliance Risiko im Hinblick auch auf Drittlandtransfers derzeit nicht möglich.

Bei der Gestaltung von neuen Social-Media-Auftritten sowie bei nicht bloß redaktionellen Änderungen an bestehenden Social-Media-Auftritten **muss** stets die *Data Privacy Organization* eingebunden werden. Dies gilt insbesondere auch für die Erstellung, Überarbeitung und Aktualisierung der erforderlichen Datenschutzinformationen (vgl. Ziffer 4.6).

11.8.3 Dokumentation

Zum einen müssen alle Verarbeitungstätigkeiten im Zusammenhang mit Webseiten und Social-Media-Auftritten datenschutzrechtlich dokumentiert und in das Verzeichnis der Verarbeitungstätigkeiten aufgenommen werden (vgl. Ziffer 5). Hier sind auch die getroffenen technischen und organisatorischen Maßnahmen zu dokumentieren.

Zum anderen müssen die Einzelheiten der Verarbeitungstätigkeiten im Zusammenhang mit Webseiten und Social-Media-Auftritten in den jeweiligen Datenschutzinformationen in präziser, transparenter und verständlicher Weise aufgenommen und den Besuchern der Webseite bzw. Social-Media-Auftritt leicht zugänglich gemacht werden (vgl. Ziffer 4.6).

Darüber hinaus müssen alle eingesetzten Cookies in einer Übersicht aufgeführt und jeweils mit folgenden Informationen versehen werden: Bezeichnung, Funktion, Quelle, Speicherdauer und Abmelde-/Entfernungsmöglichkeiten.

Der Einsatz von Google Analytics oder vergleichbaren Analyse-/Trackingtools ist zu dokumentieren.

11.8.4 Rollen und Verantwortung

Rolle	Verantwortung
Prozesseigentümer bzw. Asset-Eigentümer	<ul style="list-style-type: none"> ▪ Ist für die datenschutzkonforme Gestaltung zuständig. ▪ Dokumentiert alle datenschutzrechtlichen Anforderungen im Zusammenhang mit Webseiten und Social-Media-Auftritten in das Verzeichnis von Verarbeitungstätigkeiten (u.a. Datenschutzinformationen, TOM, etc.). ▪ Prüft, regelmäßig, ob Änderungen an Webseiten/Social-Media-Auftritten vorliegen (z. B. neue Funktionen, neue Cookies, neue Plug-Ins, neue Einbindungen), die einer datenschutzrechtlichen Prüfung und Dokumentation bedürfen. ▪ Prüft regelmäßig, ob angemessene technische und organisatorische Maßnahmen (nach dem aktuellen Stand der Technik) zur Absicherung der Verarbeitungstätigkeiten sowie zur Erfüllung der datenschutzrechtlichen Anforderungen im Zusammenhang mit dem Betrieb einer Webseite bzw. eines Social-Media-Auftritts getroffen wurden. ▪ Bezieht bei der Gestaltung von neuen Webseiten/Social-Media-Auftritten sowie bei nicht bloß redaktionellen Änderungen an bestehenden Webseiten/Social-Media-Auftritten den zuständige Data Privacy Officer ein.
Informationssicherheit	<ul style="list-style-type: none"> ▪ Unterstützt bei der Festlegung, Implementierung und Dokumentation der risiko- adäquaten technischen und organisatorischen Maßnahmen.


Rolle	Verantwortung
Data Privacy Officer	<ul style="list-style-type: none">▪ Berät bei datenschutzrechtlichen Fragen rund um die Gestaltung und den Betrieb von Webseiten bzw. Social-Media-Auftritten.
Datenschutzbeauftragter	<ul style="list-style-type: none">▪ Berät bei datenschutzrechtlichen Fragen rund um die Gestaltung und den Betrieb von Webseiten bzw. Social-Media-Auftritten.

C DOKUMENTENMANAGEMENT

Herausgeber und Autor

Herausgeber	Position	Abteilung	Unterschrift
Michael Salzmann	Chief Compliance Officer	RhAG CPL	
Autor			
Thomas Kautsch	Corporate Data Privacy Officer	RhAG CPL	

Freigabe

Freigabe durch	Position	Organisation	Unterschrift
Armin Papperger	Vorstandsvorsitzender und Ressortvorstand	Rheinmetall AG	

Änderungsdienst

Version	Datum	Herausgeber	Änderungen
Verschiedene Vorversionen seit 2017 bis zuletzt 1.1/2019	zuletzt 31.05.2019	G. v. Waldowski	Dienstleister UIMC im Auftrag von Rheinmetall AG / Legal Siehe dort „Versionsverwaltung“.
2.0	01.11.2021	M. Salzmann	Neufassung.

Verteiler

Bereiche	Adressaten	Standorte	Erreichbarkeit
Rheinmetall Konzern	Divisionsleitungen Geschäftsführungen und vergleichbare Organe Führungskräfte Mitarbeiter bzw. Beschäftigte	EU/EWR	Intranet gate ² Zentrales Regelungsverzeichnis <ul style="list-style-type: none"> Handbücher & Richtlinien Data Privacy

HINWEIS: Die nicht deutschsprachigen Versionen sind auch ohne Unterschrift gültig!