Leitlinie zum Datenschutz

OA1001

Group24 AG (group24)

INHALTSVERZEICHNIS

STAMMDATEN

Referenz-Nummer:	OA1001
Dokumententitel:	Leitlinie zum Datenschutz
Fachlich Verantwortlicher:	Datenschutzbeauftragter der group24 AG
Zuständiger Bereich:	Datenschutzmanagement
Geltungsbereich:	group24 AG
Gültig von:	01.11.2022
Gültig bis:	31.12.2024
Verantwortlicher Prüfer:	Christian Hornhues
Wiedervorlage Datum:	01.10.2024
Dokumentenkategorie	intern

ÄNDERUNGSVERZEICHNIS

Version	Datum	Autor	Inhalte der Änderung

REVIEWNACHWEIS UND FREIGABE

Version	Datum	Teilnehmer	Inhalte des Reviews
V1.0	31.10.2022	Christian Hornhues	Ersterstellung
V1.1	15.11.2023	Christian Hornhues	Review 2023

1 EINLEITUNG

Die vorliegende Organisationsanweisung beschreibt die organisatorischen Rahmenbedingungen des Datenschutzes und der Datensicherheit.

1.1 Grundlagen

Gemäß Artikel 3 Ziffer 1 der EU-Datenschutz-Grundverordnung (EU-DSGVO) sind personenbezogene Daten alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Der Datenschutz bezweckt somit den Schutz des Einzelnen vor Beeinträchtigungen in seinem Persönlichkeitsrecht durch den angemessenen Umgang mit seinen personenbezogenen Daten.

Der Umgang mit personenbezogenen Daten in Umsetzung völkerrechtlicher Verpflichtungen ist ab dem 25. Mai 2018 in der EU-DSGV0 geregelt, die in den europäischen Staaten und damit auch für die Group24 ohne weitere Umsetzung gilt. Damit obliegt es ihm, die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der EU-DSGVO zu gewährleisten.

Der Schutz sensitiver betrieblicher Daten, Informationen und Systeme ist ebenfalls eine zwingende Anforderung, obwohl dieser Bereich gesetzlich weniger explizit als der Datenschutz geregelt ist. Diese Anforderung ergibt sich vielfach aus vertraglichen und rechtlichen Verpflichtungen, darüber hinaus aber auch aus dem Eigeninteresse, die Ziele der Group24 nicht durch ein zu niedriges Sicherheitsniveau zu gefährden.

1.2 Ziel des Datenschutzes

Es ist Ziel von Datenschutz und Datensicherheit, die Anforderungen an ebenjene stets angemessen zu berücksichtigen. Diese Anforderungen basieren auf den Vorgaben des europäischen und deutschen Datenschutzrechts, sind aber nicht auf diese beschränkt.

1.3 Beitrag aller Mitarbeiter

Datenschutz und Datensicherheit lassen sich nicht durch die Einhaltung einmal festgelegter Regeln dauerhaft sicherstellen. Mit neuen Techniken und neuen Abläufen muss die Frage nach der Angemessenheit und Wirksamkeit der Sicherheit immer wieder neu gestellt und beantwortet werden. Jeder Mitarbeiter der Group24 kann und soll hierzu seinen Beitrag leisten und auf Schutzmaßnahmen, die er für notwendig hält, ebenso hinweisen wie auf jene, die er für unangemessen oder nicht mehr erforderlich hält.

2 MANAGEMENT DES DATENSCHUTZES

Das Erreichen der angestrebten Datenschutzziele und die Durchsetzung kann nur durch ein geplantes und organisiertes Vorgehen aller Beteiligten gewährleistet werden. Voraussetzung für einen funktionierenden Sicherheitsprozess ist ein geeigneter organisatorischer Rahmen, in dem die jeweiligen Rollen und Verantwortlichkeiten festgelegt werden.

2.1 Geschäftsführung

Die Verantwortung für den Datenschutz in der Group24 liegt bei der höchsten Kontrollinstanz. Die Geschäftsführung ist verantwortlich für die Umsetzung des Datenschutzes.

Die höchste Kontrollinstanz gibt die Datenschutzpolitik der Group24 vor, fördert die Datenschutzkultur und unterstützt die Umsetzung der Datenschutzpolitik in allen Unternehmensbereichen der Group24. Sie delegiert soweit erforderlich die notwendigen Zuständigkeiten und Kompetenzen zur Koordination und Kontrolle des Datenschutzes.

2.2 Führungskräfte

Zur Wahrung des Datenschutzes ist die aktive Mitwirkung der verantwortlichen Führungskräfte unerlässlich. Die Führungskräfte müssen darauf achten, dass die in ihrem Verantwortungsbereich eingeführten Datenschutzmaßnahmen eingehalten werden. Sie haben bezüglich der Einhaltung der Datenschutzpolitik Vorbildfunktion und sorgen für die Sensibilisierung und Schulung ihrer Mitarbeiter. Sie motivieren die Mitarbeiter dazu, Datenschutzmaßnahmen einzuhalten und sorgen für die entsprechenden Informationen und Weiterbildungsmaßnahmen.

Bei, den Datenschutz betreffenden Schwachstellen oder Vorfällen, ist unverzüglich der Datenschutzkoordinator oder der Beauftragte für den Datenschutz zu informieren.

Der Beauftragte für den Datenschutz hat im Rahmen seines Wirkungskreises ein uneingeschränktes aktives Informationsrecht: Dazu sind ihm auf Anfrage unverzüglich die erforderlichen Informationen zu erteilen, alle notwendigen Unterlagen zur Verfügung zu stellen und Einblick in die relevanten Betriebs- und Geschäftsabläufe zu gewähren. Eine wirkungsvolle Datenschutzarbeit setzt eine umfassende Versorgung mit Information voraus: Jede Führungskraft muss sicherstellen, dass der Beauftragte für den Datenschutz über datenschutzrelevante Ereignisse, Planungen und Entwicklungstendenzen der jeweils zuständigen Einheit sowie Anweisungen, Richtlinien und Verfahren unterrichtet ist. Die Schnittstellen zwischen den jeweiligen Einheiten und dem Beauftragten für Datenschutz können in Rahmenvereinbarungen spezifiziert werden.

2.3 Mitarbeiter

Jeder Mitarbeiter der Group24 ist persönlich verantwortlich für die Einhaltung des Datenschutzes. Jeder Mitarbeiter muss die Datenschutzpolitik der Group24 und das abgeleitete Regelwerk kennen, verstehen und in seiner Funktion und Zuständigkeit umsetzen. Insbesondere sollen sie Datenschutzvorfälle, Fehler, Schwachstellen oder Bedrohungen so früh wie möglich dem Datenschutzkoordinator oder dem Datenschutzbeauftragen melden, um die Evaluation und Quantifizierung der Vorfälle zu ermöglichen.

2.4 Beauftragter für Datenschutz

Die Anforderung einen Beauftragten für den Datenschutz (DSB) zu benennen, ergibt sich aus der jeweiligen Gesetzeslage oder aus rein betrieblichen Erfordernissen. Die Benennung zum Datenschutzbeauftragten erfolgt schriftlich.

2.4.1 Berufsgrundsätze

Aufgrund der Stellung des DSB im Hause werden besondere Anforderungen an das Verhalten des DSB gestellt, insbesondere Verschwiegenheit, Gewissenhaftigkeit, Unabhängigkeit, Objektivität und Integrität.

2.4.2 Stellung im Unternehmen

Der DSB ist der höchsten Kontrollinstanz direkt unterstellt. Er hat im Rahmen seiner Aufgabenerfüllung ein umfassendes Prüfungs- und Einsichtsrecht. In die Änderungsprozesse des Unternehmens ist er frühzeitig einzubeziehen. Regelmäßig berichtet der DSB der höchsten Kontrollinstanz über den Stand des Datenschutzes.

Bei der Erfüllung seiner Aufgaben ist der DSB auf dem Gebiet des Datenschutzes weisungsfrei. Er darf nicht mit Aufgaben betraut werden, die mit der Datenschutztätigkeit nicht im Einklang stehen.

2.4.3 Grundlagen der Tätigkeit

Der Schutzbedarf von Daten ergibt sich zum einen aus gesetzlichen oder vertraglichen Anforderungen und zum anderen aus betrieblichen Anforderungen an einen sicheren Geschäftsbetrieb (z.B. bei Betriebsgeheimnissen).

Im Hinblick auf die Verarbeitung personenbezogener Daten nimmt der DSB hoheitliche Aufgaben wahr. Die Definition personenbezogener Daten ist in verschiedenen Rechtsräumen unterschiedlich. Ebenso kann der Personenbezug von Daten abhängig vom jeweiligen Kontext (z.B. Adressdaten in einer Kundendatei) oder von der technischen Umsetzung (z.B. IP-Nummern) sein. Die Beurteilung, ob ein Personenbezug bei Daten vorliegt, obliegt dem DSB. Der Schutzbedarf von Daten kann – neben gesetzlichen oder vertraglichen Anforderungen –

durch Anforderungen des Dateneigentümers bzw. der Fachabteilung festgelegt werden (z.B. bei Protokollen der Sitzungen der höchsten Kontrollinstanz).

Der Zuständigkeitsbereich des DSB umfasst IT-gebundene und nicht-IT-gebundene Daten.

2.4.4 Aufgaben und Ziele

Der DSB wirkt auf die Einhaltung datenschutzrelevanter Gesetze und anderer Vorschriften über den Datenschutz hin. Er ist Teil des internen Kontroll- und Qualitätssicherungssystems der Group24.

Ziel des Datenschutzes in der Group24 ist die Umsetzung eines ordnungsgemäßen und angemessenen Datenschutzniveaus.

Die Aufgaben des DSB sind die Empfehlung und Überprüfung eines angemessenen Datenschutzniveaus innerhalb der Group24, im Rahmen der rechtlichen, technischen und organisatorischen Möglichkeiten auf der einen und den unternehmensweiten Vorgaben auf der anderen Seite.

Ziele sind:

- die datenschutzrechtliche Würdigung von Verfahren, Verträgen und Projekten,
- die Überprüfung der ordnungsgemäßen Anwendung von IT-Systemen,
- die Überprüfung des ordnungsgemäßen Umgangs mit Daten,
- die Durchführung von Datenschutzschulungen,
- die Festlegung der technischen Zugriffsbeschränkungen in Abstimmung mit den zuständigen Organisationsbereichen,
- die Einhaltung der Meldungsvorschriften der zuständigen Aufsichtsbehörden in Abstimmung mit der zuständigen Geschäftsführung,
- die Erstellung eines Jahresberichts.

Die Prüfungen des DSB umfassen alle Betriebs- und Geschäftsabläufe, sofern sie datenschutzrelevant sind. Sie werden in einem Jahresplan dokumentiert.

3 VERZEICHNIS VON VERARBEITUNGSTÄTIGKEITEN

Um personenbezogenen Daten nach Maßgaben der Datenschutz-Grundverordnung schützen zu können, hat die Group24 zunächst ermittelt, in welchen Fällen personenbezogene Daten – z.B. von Kunden, Lieferanten oder Beschäftigten – erhoben und verarbeitet werden.

Nach Art. 30 DSGVO ist der Verantwortliche verpflichtet, ein Verzeichnis von Verarbeitungstätigkeiten zu führen. In diesem Verzeichnis sind die wesentlichen Informationen zu Datenverarbeitungstätigkeiten zusammenzufassen, insbesondere also Angaben zum Zweck der Verarbeitung und eine Beschreibung der Kategorien der personenbezogenen Daten, der betroffenen Personen und der Empfänger.

Innerhalb der Group24 wird die Dokumentation von Verarbeitungstätigkeiten durch den Datenschutzbeauftragten durchgeführt.

Die Verwaltung der Verarbeitungstätigkeiten erfolgt durch den Datenschutzkoordinator in der Ablage des Datenschutzmanagements.

3.1 Datenschutz-Folgenabschätzung

Daneben ist die Group24 in bestimmten Fällen verpflichtet, eine Datenschutz-Folgenabschätzung nach Art. 35 DSGVO durchzuführen. Diese ist durchzuführen, wenn eine Form der Verarbeitung wahrscheinlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat, insbesondere bei neuen Technologien oder aufgrund ihres Wesens, ihres Umfangs, ihres Kontexts oder ihrer Zwecke.

Innerhalb der Group24 wird die Durchführung der Datenschutz-Folgeabschätzung durch den Datenschutzbeauftragten durchgeführt.

Die Verwaltung der Datenschutz-Folgeabschätzungen erfolgt durch den Datenschutzbeauftragten.

4 VERTRAGSMANAGEMENT

Im Rahmen des Vertragsmanagements hat die Group24 alle von ihr eingesetzten Dienstleister, die Auftragsverarbeiter sind, und alle Kunden in einer Liste zusammengefasst.

Der Datenschutzbeauftragte überprüft die Verträge zur Auftragsverarbeitung.

Die Verwaltung der Verträge zur Auftragsverarbeitung erfolgt durch den Datenschutzkoordinator. Die Aktualität der AVVs wird jährlich geprüft.

5 DATENSCHUTZPOLITIK

Das Ziel der Datenschutzpolitik ist es, die Vertraulichkeit, Integrität und Verfügbarkeit von Daten und den eingesetzten Systemen und einen sicheren und ordnungsgemäßen Umgang mit personenbezogenen Daten zu gewährleisten. Die Datenschutzpolitik ist eine Richtungsvorgabe für die Umsetzung des Datenschutzes bei der Group24Informationssicherheit. Sie ist die Grundlage für alle nachgeordneten Konzepte, Vorgaben und Empfehlungen.

5.1 Prinzipien

Der Umgang mit personenbezogenen Daten ist in der EU-DSGVO als Verbot mit Erlaubnisvorbehalt geregelt. Damit ist das Verarbeiten von personenbezogenen Daten grundsätzlich verboten. Ausnahmen bestehen nur, wenn ein Gesetz dies erlaubt oder der Betroffene einwilligt. Personenbezogene Daten müssen:

a. auf rechtmäßige Weise, nach Treu und Glauben und in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden („**Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz**“);

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

c. dem Zweck angemessen und erheblich sowie auf das für die Zwecke der Verarbeitung notwendige Maß beschränkt sein („**Datenminimierung**“);

d. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; es sind alle angemessenen Maßnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden („**Richtigkeit**“); 4.5.2016 L 119/35 Amtsblatt der Europäischen Union DE (1) Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates vom 9. September 2015 über ein Informationsverfahren auf dem Gebiet der technischen Vorschriften und der Vorschriften für die Dienste der Informationsgesellschaft (ABl. L 241 vom 17.9.2015, S. 1).

e. in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden,

erforderlich ist; personenbezogene Daten dürfen länger gespeichert werden, soweit die personenbezogenen Daten vorbehaltlich der Durchführung geeigneter technischer und organisatorischer Maßnahmen, die von dieser Verordnung zum Schutz der Rechte und Freiheiten der betroffenen Person gefordert werden, ausschließlich für im öffentlichen Interesse liegende Archivzwecke oder für wissenschaftliche und historische Forschungszwecke oder für statistische Zwecke gemäß Artikel 89 Absatz 1 verarbeitet werden („**Speicherbegrenzung**“);

f. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschließlich Schutz vor unbefugter oder unrechtmäßiger Verarbeitung und vor unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung durch geeignete technische und organisatorische Maßnahmen („**Integrität und Vertraulichkeit**“)

5.2 Grundlagen der Datenschutzpolitik

Die Datenschutzpolitik basiert auf folgenden Vorgaben:

Alle Maßnahmen zur Wahrung des Datenschutzes müssen dem Risiko und den zu schützenden Werten angemessen sein. Um die Angemessenheit zu gewährleisten, sind regelmäßig die Risiken und Schwachstellen zu identifizieren sowie geeignete Datenschutzmaßnahmen auszuwählen und zu realisieren.

1. Die Einsicht in personenbezogene Daten und deren Bearbeitung oder Weitergabe ist nur dann zu gewähren, wenn sie zu Erfüllung der dienstlichen Tätigkeit erforderlich ist. Der ordnungsgemäße Datenzugriff und –transfer wird durch die jeweilige Berechtigungsverwaltung systemtechnisch sichergestellt.
2. Da der Umgang mit personenbezogenen Daten grundsätzlich verboten ist, wird eine unzulässige Nutzung von personenbezogenen Daten– soweit sinnvoll – systemtechnisch unterbunden.
3. Für die wesentlichen Datenbestände der Group24 sowie die dazugehörenden Verfahren werden die zuständigen bzw. verantwortlichen Mitarbeiter benannt. Die Datenflüsse dieser Daten sind zu dokumentieren.
4. Regelungen zum Datenschutz werden schriftlich festgehalten und allen Mitarbeitern zur Kenntnis gebracht.
5. Datenschutzvorfälle und -schäden werden quantifiziert und dem Datenschutzkoordinator gemeldet. Allen wesentlichen Datenschutzvorfällen muss nachgegangen werden; zugrundeliegende Mängel werden ermittelt.
6. Die Einhaltung der Datenschutzpolitik wird überprüft.

6 VERBINDLICHKEIT DER REGELUNGEN

6.1 Verbindlichkeit der Regelungen

Die im Anhang aufgeführten, veröffentlichten und in Kraft gesetzten Dokumente gelten als Anlage zu dieser OA und sind für alle Mitarbeiter verbindlich.

Sie sind insoweit Bestandteil dieser Organisationsanweisung.

6.2 Ausnahmeregelung

Sollte eine gültige Regelung für einzelne Systeme oder Prozesse, aus welchen Gründen auch immer, nicht umsetzbar sein, so kann der Datenschutzkoordinator für dieses System bzw. diesen Prozess eine Ausnahme von den Regeln genehmigen. Die Entscheidung des Datenschutzkoordinatoren erfolgt risikobasiert.

Diese Ausnahmen sind zentral vom Datenschutzkoordinator zu dokumentieren.