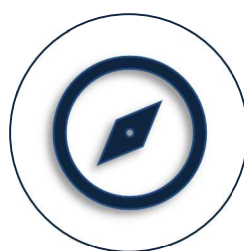


# Datenschutz-Leitlinie

## Datenschutz-Grundverordnung

---

Thieme Compliance GmbH  
Version 1.1 vom 31.03.2021



## Dokumentenverlauf

| Version | Datum      | Autor             | Kommentare   |
|---------|------------|-------------------|--|
| 0.1     | 17.06.2020 | Blossey & Partner | Erstfassung zur Anpassung an das Unternehmen         |
| 1.0     | 08.09.2020 | Blossey & Partner | Freigegeben durch GF                                 |
| 1.0.1   | 13.01.2021 | Radecke           | Rechtschreibkorrekturen                              |
| 1.1     | 31.03.2021 | Radecke           | Beschlussdatum zur Veröffentlichung, Signaturbereich |
|         |            |                   |  |
|         |            |                   |  |
|         |            |                   |  |

## Präambel

Mit dieser Datenschutz-Leitlinie gibt sich unser Unternehmen den verbindlichen Rahmen für einen rechtskonformen und nachhaltigen ganzheitlichen Schutz personenbezogener Daten und damit der Privatsphäre aller an unseren Geschäftsprozessen Beteiligten.

Ziel dieser Datenschutz-Leitlinie ist es, im gesamten Unternehmen ein einheitliches hohes Datenschutzniveau zu schaffen, das die Erwartungen aller beteiligten Personen erfüllt und den gesetzlichen Anforderungen der EU Datenschutz-Grundverordnung (DSGVO), dem Bundesdatenschutzgesetz (BDSG) und den weiteren relevanten Regelungen, z.B. Telekommunikationsgesetz, Strafgesetzbuch gerecht wird.

## Geltungsbereich und Geltungsdauer

Die Datenschutz-Leitlinie regelt den Umgang mit personenbezogenen Daten natürlicher Personen, insbesondere Daten von Kunden, Interessenten, Beschäftigten und sonstigen Betroffenen im gesamten Unternehmen. Sie ist für alle Beschäftigten im Sinne der DSGVO, darunter auch Externe und Berater, bindend.

Diese Datenschutz-Leitlinie tritt mit Beschluss der Geschäftsführung vom 17.03.2021 in Kraft. Sie gilt, bis sie außer Kraft gesetzt oder durch eine neuere Fassung ersetzt wird.

## Rechtliche Rahmenbedingungen

Die rechtliche Basis für diese Datenschutz-Leitlinie bilden vor allem zwei Gesetze: EU Datenschutz-Grundverordnung (DSGVO)

Bundesdatenschutzgesetz in der Neufassung vom 12.05.2017 (BDSG)

Ergänzend kommen weitere gesetzliche Regelungen in Bezug auf die Verarbeitung von und den Umgang mit personenbezogenen Daten zur Anwendung, unter anderem das Telekommunikationsgesetz (§§ 88 bis 107 TKG), das Telemediengesetz (§ 11 bis § 15a TMG), die derzeit noch in Erarbeitung befindliche ePrivacy-Verordnung sowie branchenspezifische und länderbezogene Spezialregelungen.

## Ziele des Datenschutzes und dieser Datenschutz-Leitlinie

Bei der Verarbeitung personenbezogener Daten sind gemäß Gesetz für jede Datenkategorie vier Schutzziele zu berücksichtigen:

- ✓ **Vertraulichkeit**
- ✓ **Integrität (inkl. Authentizität)**
- ✓ **Verfügbarkeit**
- ✓ **Accountability (Rechenschaftspflicht)**

Alle verantwortlichen Stellen („Verantwortliche“) sind verpflichtet, mit angemessenen Maßnahmen dafür zu sorgen, dass personenbezogene Daten gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, gegen Verlust oder Zerstörung sowie gegen Verfälschung, Manipulation oder unbeabsichtigte Veränderung geschützt sind. Dies gilt unabhängig davon, ob die Datenverarbeitung elektronisch oder in Papierform erfolgt.

## **Selbstverpflichtung und Datenschutz-Leitbild**

Die Geschäftsführung und die Beschäftigten sind sich ihrer Verantwortung im Umgang mit personenbezogenen Daten und den hierfür eingesetzten Informations- und Kommunikationssystemen bewusst. Wir beachten die einschlägigen Gesetze, vertraglichen Regelungen und internen Richtlinien. Wir verstehen, dass Datenschutz personenbezogene Daten ebenso wie Geschäftsgeheimnisse schützt und so zum Schutz der Privatsphäre aller Beteiligten und der wirtschaftlichen Existenz des Unternehmens beiträgt.

Das Unternehmen hat sich einem hohen Qualitätsstandard verpflichtet. Alle Datenschutzaktivitäten werden seit Jahren nach einem detaillierten Basiskonzept geplant, umgesetzt und geprüft. Nach bestem Wissen und Gewissen wird eine Vielzahl technischer und organisatorischer Maßnahmen sorgfältig erarbeitet und umgesetzt, dem Stand der Technik angepasst, auf ihre Wirksamkeit getestet, ihre Nachhaltigkeit regelmäßig kontrolliert.

Die Einhaltung der Datenschutzvorschriften durch jeden einzelnen Beschäftigten wird durch kontinuierliche Sensibilisierung, Verschwiegenheitsverpflichtungen, datenschutzkonforme Arbeitsplatzgestaltung, Arbeits- und Verfahrensanweisungen und transparente Unternehmenskommunikation gefördert.

Für Datenschutz-Vorfälle sind Verfahrensweisen etabliert, um drohende negative materielle wie immaterielle Folgen für Betroffene und den Verantwortlichen zu reduzieren und die gesetzlichen Fristen wahren zu können.

Eine fortlaufende Dokumentation der Datenschutzaktivität wird vom Datenschutzbeauftragten geführt.

## Grundprinzipien der Datenschutzorganisation

Folgende Kernaspekte erfordern die gesetzlichen Grundprinzipien der DSGVO und weiteren Vorschriften vom Verantwortlichen hinsichtlich der Verarbeitung personenbezogener Daten.

- Festlegung der Verantwortlichkeiten
- Führen eines Verzeichnisses der Verarbeitungstätigkeiten
- Einhaltung der DSGVO-Grundprinzipien für die Verarbeitung personenbezogener Daten
- Ausdrückliche Berücksichtigung besonderer Kategorien personenbezogener Daten
- Erfüllung der Informationspflichten und Anbieterkennzeichnung zur optimalen Transparenz
- Wahrung der weiteren Rechte Betroffener (Auskunft, Berichtigung, Löschung, Portabilität etc.)
- Datenschutzkonforme Produktgestaltung und datenschutzfreundliche Grundeinstellungen
- Gesetzeskonforme Gestaltung der ausgelagerten bzw. gemeinsamen Datenverarbeitung (Outsourcing)
- Sicherstellung eines angemessenen Datenschutzniveaus für den Fall der Übermittlung in Drittstaaten
- Wahrung der Privatsphäre unserer Beschäftigten in ihrer Arbeitsumgebung
- Durchführung von Risikobewertungen, ggf. mit dokumentierter Datenschutz-Folgenabschätzung
- Regelung zum Umgang mit Datenschutzvorfällen und Betroffenenanfragen (Einhaltung der Fristen)
- Mechanismen zur Erfüllung der Accountability (Dokumentation, standardisierte Verfahren, Audits etc.)

## Überprüfung und Überarbeitung dieser Datenschutz-Leitlinie

Die Geschäftsleitung und der Datenschutzbeauftragte überprüfen die Datenschutz-Leitlinie regelmäßig, mindestens jährlich, auf deren Vereinbarkeit mit den geltenden Gesetzen und passen diese bei Bedarf an.

Die Geschäftsleitung informiert alle relevanten Personen, für die diese Datenschutz-Leitlinie verbindlich ist, über die inhaltlichen Änderungen.

Erlangen, den 1.4.2021

Reinhold Tokar  
Geschäftsführer

Erlangen, den 06.05.2021

Thomas Eilfort  
Geschäftsführer