

# Kostenlose Vorlage: Datenschutzkonzept nach DSGVO

Bei diesem Dokument handelt es sich um eine kostenlose Vorlage bzw. Checkliste der activeMind AG zu den Themenbereichen Datenschutz und Datensicherheit. Die aktuellste Version finden Sie stets auf [im Downloadbereich unserer Website](https://www.activemind.de/datenschutz/dokumente/).

Sie können dieses Dokument an die Bedürfnisse in Ihrem Unternehmen anpassen, speichern und ausdrucken. Bitte haben Sie Verständnis dafür, dass die activeMind AG keinerlei Haftung für etwaige Fehler übernimmt.

Bei Fragen oder Problemen helfen wir Ihnen gerne weiter!

Ihr Team der activeMind AG

Telefon: +49 (0)89 / 91 92 94 – 900  
E-Mail: [anfrage@activemind.de](mailto:anfrage@activemind.de)  
Web: <https://www.activemind.de>

# Datenschutzkonzept

## Ziel des Datenschutzkonzeptes

Das Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation die datenschutzrechtlichen Aspekte darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen z. B. durch Auftraggeber im Rahmen der [Auftragsverarbeitung](https://www.activemind.de/datenschutz/auftragsverarbeitung/) genutzt werden. Dadurch soll die Einhaltung der europäischen [Datenschutz-Grundverordnung (DSGVO)](https://www.activemind.de/datenschutz/dsgvo/) nicht nur gewährleistet, sondern auch der Nachweis der Einhaltung geschaffen werden.

## Präambel

Kurzbeschreibung des Unternehmens und Motivation zur Einhaltung des Datenschutzes.

## Datenschutzpolitik und Verantwortlichkeiten im Unternehmen

* Für ein Unternehmen sind die obersten Datenschutzziele ggf. neben bereits bestehenden Unternehmenszielen festzulegen und zu dokumentieren. Datenschutzziele orientieren sich an den Datenschutz-Grundsätzen und sind individuell auf ein Unternehmen anzupassen.
* Festlegung der Rollen und Verantwortlichkeiten (z. B. Vertreter des Unternehmens, betriebliche Datenschutzbeauftragte, Koordinatoren oder Datenschutzteam und operativ Verantwortliche).
* Verpflichtung zur kontinuierlichen Verbesserung eines Datenschutzmanagementsystems.
* Schulung, Sensibilisierung und Verpflichtung der Mitarbeiter

## Rechtliche Rahmenbedingungen im Unternehmen

* Branchenspezifische gesetzliche Regelungen oder Verhaltensregeln für den Umgang mit personenbezogenen Daten.
* Anforderungen interner und externer Parteien.
* Anwendbare Gesetze mit ggf. lokalen Sonderregelungen.

## Dokumentation

* Schutzbedarf der Daten: Schutzbedarfsfeststellung bezüglich Vertraulichkeit, Integrität und Verfügbarkeit (hilfreich sind die Kategorien des [BSI-Standard 100-2](https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/BSI-Standard_1002.pdf?__blob=publicationFile) z.B. „normal“, „hoch“ und „sehr hoch“)
* Durchgeführte interne und externe Überprüfungen

## Bestehende technische und organisatorische Maßnahmen (TOM)

Geeignete technische und organisatorische Maßnahmen, die unter Berücksichtigung u. a. des Zwecks der Verarbeitung, des Stands der Technik und der Implementierungskosten zu treffen und nachzuweisen sind.

Die Beschreibung der umgesetzten Umsetzung TOM kann sich beispielsweise an dem Aufbau der ISO/IEC 27002 unter Berücksichtigung der ISO/IEC 29151 (Leitfaden für den Schutz personenbezogener Daten) orientieren. Die jeweiligen Kapitel sollten durch Hinweis auf bestehende Richtlinien nachgewiesen werden.

Beispiele für solche Richtlinien sind unter anderem:

* Richtlinie für Betroffenenrechte
* Zugangssteuerung
* Informationsklassifizierung (und deren Handhabung)
* physische und umgebungsbezogene Sicherheit
* an den Endanwender gerichtete Themen wie:
  + zulässiger Gebrauch von Werten
  + Richtlinie für eine aufgrund der Arbeitsumgebung und Bildschirmsperren
  + Informationsübertragung
  + Mobilgeräte und Telearbeit
  + Einschränkung von Software Installation und -verwendung
* Datensicherung
* Informationsübertragung
* Schutz vor Schadsoftware
* Handhabung technischer Schwachstellen
* kryptografische Maßnahmen
* Kommunikationssicherheit
* Privatsphäre und Schutz von personenbezogenen Informationen
* Lieferanten Beziehungen Hinweis auf regelmäßige Überprüfung und Bewertung der Datenverarbeitung, insbesondere der Wirksamkeit der umgesetzten technischen und organisatorischen Maßnahmen.