Vorlage für ein
Datenschutzkonzept
nach den Vorgaben des Schweizer Bundesgesetzes über den Datenschutz (Datenschutzgesetz – DSG)

**Erläuterungen zu dieser Vorlage**

Die Vorlage ist nicht abschliessend und umfasst unter Umständen nicht alle erforderlichen Elemente. Zudem können in der Vorlage Elemente enthalten sein, die auf einzelne Unternehmen nicht zutreffen. Es ist daher stets eine entsprechende Anpassung und Ergänzung der Vorlage durch den jeweiligen Verantwortlichen erforderlich. Hinweise dazu finden Sie ggfs. in den Kommentaren.

**Nutzungshinweise für unser kostenloses Template**

Diese Vorlage wird von den Spezialisten von activeMind.ch erstellt und regelmässig aktualisiert. Das Template kann nicht auf alle denkbaren Spezialfälle eingehen. Eine datenschutzrechtliche oder sonstige anwaltliche Beratung kann und soll es nicht ersetzen.

Jegliche Haftung ist ausgeschlossen!

Alle Rechte an der Vorlage bleiben vorbehalten. Der Einsatz des von uns zur Verfügung gestellten Textes ist Ihnen zu eigenen (auch kommerziellen) Zwecken erlaubt und frei möglich.

Wir bieten für diesen kostenfreien Dienst weder Support noch Beratung an und bitten höflich, von entsprechenden Anfragen abzusehen.

Wenn Sie die Vorlage oder Teile davon veröffentlichen, sind der Hinweis und der Link auf htttps://www.activemind.ch auf jeden Fall im Text zu belassen.

Datenschutzkonzept

# Ziel des Datenschutzkonzeptes

Das Datenschutzkonzept hat zum Ziel, in einer zusammenfassenden Dokumentation alle datenschutzrechtlichen Aspekte im Unternehmen darzustellen. Es kann auch als Grundlage für datenschutzrechtliche Prüfungen z. B. durch Auftraggeber im Rahmen der Auftragsbearbeitung genutzt werden. Dadurch soll der Nachweis der Einhaltung des Schweizer Datenschutzgesetzes (DSG) geschaffen werden.

# Präambel

*Kurzbeschreibung des Unternehmens und Motivation zur Einhaltung des Datenschutzes.*

# Datenschutzpolitik und Verantwortlichkeiten im Unternehmen

* *Festlegung der obersten Datenschutzziele Ihres Unternehmens und Einordnung neben ggf. bereits bestehenden Unternehmenszielen. Datenschutzziele orientieren sich an den Datenschutz-Grundsätzen und sind individuell auf ein Unternehmen anzupassen.*
* *Festlegung der Rollen und Verantwortlichkeiten (z. B. Vertreter des Unternehmens, Datenschutzberater, 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 für Systeme und Dienste im Zusammenhang mit der Bearbeitung der Personendaten.*
* *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.*

*Beispiele für solche Massnahmen:*

* *Pseudonymisierung*
* *Verschlüsselung*
* *Vertraulichkeit*
	+ *Zutrittskontrolle*
	+ *Zugangskontrolle*
	+ *Zugriffskontrolle*
	+ *Trennungskontrolle*
* *Integrität*
	+ *Weitergabekontrolle*
	+ *Eingabekontrolle*
* *Verfügbarkeit und Belastbarkeit*
	+ *Gewährleistung der Verfügbarkeit und Belastbarkeit*
	+ *Wiederherstellung der Verfügbarkeit*
* *Verfahren zur regelmässigen Überprüfung, Bewertung und Evaluierung*
	+ *Datenschutzmanagement*
	+ *Incident-Response-Management*
	+ *Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen*
	+ *Auftragskontrolle*

*Die jeweiligen Kapitel sollten durch Hinweis auf bestehende Richtlinien nachgewiesen werden.*

*Beispiele für solche Richtlinien sind unter anderem:*

* *Richtlinie für Betroffenenrechte*
* *Lösch- und Aufbewahrungskonzept*
* *Berechtigungskonzept*
* *Informationsklassifizierung (und deren Handhabung)*
* *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*
* *Lieferantenbeziehungen Hinweis auf regelmässige Überprüfung und Bewertung der Datenverarbeitung, insbesondere der Wirksamkeit der umgesetzten technischen und organisatorischen Massnahmen.*

Dieses Datenschutzkonzept wurde mit Hilfe von [www.activemind.ch](https://www.activemind.ch/) erstellt – den Experten für Datenschutz und Informationssicherheit.