

# Datenschutzrichtlinie

**[Organisation]  
[Straße  
L-PLZ-Ort]**

**[LOGO ggf.]**

**Gültigkeit der Richtlinie für  
[Unternehmen / Bereich / Gesellschaft]  
[Unternehmen / Bereich / Gesellschaft]**

**Ort  
[L-PLZ-Ort]  
[L-PLZ-Ort]**

## Inhaltsverzeichnis

1. Ziel der Datenschutzrichtlinie.....	3
2. Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz....	3
3. Verarbeitung von personenbezogenen Daten.....	3
(a) Technische und organisatorische Maßnahmen (TOMs).....	3
(b) Verfahrenorientierte Schutzmaßnahmen.....	3
(c) Datenschutz-Folgenabschätzungen (DSFA).....	4
4. Rechte der betroffenen Personen.....	4
5. Meldepflicht bei Datenschutzverstößen.....	4
6. Weiterführende Dokumente.....	5
7. Letzte Änderung:.....	5

## 1. Ziel der Datenschutzrichtlinie

Diese Datenschutz-Richtlinie dient zur Beschreibung der Maßnahmen, die zur Umsetzung der Datenschutzgrundverordnung (nachfolgend DS-GVO) im Unternehmen getroffen worden sind. Diese Richtlinie findet im gesamten Unternehmen Anwendung und verpflichtet alle Mitarbeiter sowie Auftragsverarbeiter (externe Dienstleister), die direkt oder indirekt an der Verarbeitung von personenbezogenen Daten beteiligt sind, die Vorgaben der DS-GVO beim Umgang mit personenbezogenen Daten einzuhalten. Abweichungen davon sind nur nach einer Freigabe durch die Geschäftsführung rechtmäßig. Die Freigabe ist entsprechend zu dokumentieren.

## 2. Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz

Eine Verarbeitung personenbezogener Daten ist nur dann zulässig, wenn dafür ein Erlaubnis - Tatbestand, d.h. eine Rechtsgrundlage nach Art. 6 oder 9 DS-GVO vorliegt. Dies kann beispielsweise eine nachweisbare Einwilligung der betroffenen Person, ein Vertrag oder ein Gesetz sein, das die Datenverarbeitung gestattet. Soweit möglich, werden personenbezogene Daten stets direkt bei der betroffenen Person erhoben, damit diese Kenntnis darüber hat, welche personenbezogene Daten von ihr erhoben, gespeichert oder in anderer Weise verarbeitet werden. Gemäß Art. 13 DS-GVO wird die betroffene Person über die Datenverarbeitung entsprechend informiert. Werden personenbezogene Daten ohne Kenntnis der betroffenen Person erhoben, gespeichert oder in anderer Weise verarbeitet, dann erfüllt das Unternehmen seine Informationspflichten gemäß Art. 14 DS-GVO gegenüber der betroffenen Person. Dem Auskunftsrecht gemäß Art. 15 DS-GVO wird entsprechend nachgekommen. Die Grundsätze der Integrität, Vertraulichkeit, Verfügbarkeit, Zweckbindung, Datenminimierung, Richtigkeit und Speicherbegrenzung werden zum Schutz personenbezogener Daten berücksichtigt.

## 3. Verarbeitung von personenbezogenen Daten

Die DS-GVO stellt die Grundlage für die Verarbeitung von personenbezogenen Daten im Unternehmen dar. Zur Gewährleistung von Transparenz und in Erfüllung der Rechenschaftspflicht werden alle relevanten Datenverarbeitungstätigkeiten gemäß den Vorgaben nach Art. 30 DS-GVO in einem Verzeichnis (sog. Verzeichnis der Verarbeitungstätigkeiten) erfasst.

### (a) Technische und organisatorische Maßnahmen (TOMs)

Um den Anforderungen an Datenschutz und Datensicherheit, insbesondere den Vorgaben von Art. 5, 25 und 32 DS-GVO nachzukommen, wurden technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten getroffen. Bei der Bestimmung und Umsetzung der geeigneten Maßnahmen wurden der Art der verarbeiteten personenbezogenen Daten und dem daraus folgenden Schutzbedarf Rechnung getragen.

## **(b)Verfahrensorientierte Schutzmaßnahmen**

Zur Gewährleistung der Sicherheit der Datenverarbeitung sind verfahrensorientierte Schutzmaßnahmen unter Beachtung der zu verarbeitenden personenbezogenen Daten, dem Ort der Datenverarbeitung sowie den an der Datenverarbeitung beteiligten Personen geplant, implementiert und werden regelmäßig überwacht. Diese Schutzmaßnahmen orientieren sich am aktuellen Stand der Technik sowie dem Schutzbedarf der jeweiligen Datenverarbeitung. Eine Verarbeitung (z.B. Erhebung, Nutzung, Speicherung) von personenbezogenen Daten erfolgt nur, soweit dies zwingend für den Zweck der Datenverarbeitung erforderlich ist.

Bei jeder Verarbeitung von personenbezogenen Daten wird überprüft, inwieweit die Grundsätze der Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Speicherbegrenzung, Integrität und Vertraulichkeit im Hinblick auf bestehende oder zukünftige Risiken bei der Datenverarbeitung, dem aktuellen Stand der Technik sowie anfallenden Implementierungskosten beachtet sind.

## **(c)Datenschutz-Folgenabschätzungen (DSFA)**

Der Pflicht zur Durchführung einer DSFA wird nachgekommen, wenn ein Datenverarbeitungsvorgang voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person zur Folge hat. Zur Minimierung identifizierter Risiken werden Abhilfemaßnahmen geplant und umgesetzt. Diese können Garantien, Sicherheitsvorkehrungen und Verfahren umfassen, durch die der Schutz personenbezogener Daten sichergestellt werden kann. Zusätzlich verpflichtet sich das Unternehmen zur Konsultation der zuständigen Aufsichtsbehörde, wenn trotz der Anwendung der auf Grundlage der DSFA festgelegten Abhilfemaßnahmen, ein besonders hohes Risiko für die personenbezogenen Daten und die betroffene Person fortbesteht.

## **4.Rechte der betroffenen Personen**

Jede Person, deren personenbezogene Daten verarbeitet werden ist berechtigt die Löschung, Einschränkung und Berichtigung seiner personenbezogenen Daten zu verlangen. Die damit einhergehenden Anfragen der betroffenen Personen werden von dem für das jeweilige Daten - Verarbeitungsverfahren Verantwortlichen sowie der für den Datenschutz im Unternehmen verantwortliche Stelle geprüft, umgesetzt und entsprechend dokumentiert. Dies schließt gegebenenfalls auch die Einbeziehung von Auftragsverarbeitern und Empfänger der betroffenen personenbezogenen Daten mit ein. Die betroffene Person wird entsprechend benachrichtigt. Den von der Datenverarbeitung betroffenen Personen werden auf Anforderung die sie betreffenden personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format überlassen. Im Rahmen der technischen Möglichkeiten und auf Anforderung werden diese Daten auch direkt an einen anderen Verantwortlichen übermittelt.

## **5.Meldepflicht bei Datenschutzverstößen**

Zur Dokumentation und zum Umgang mit Datenschutzverstößen wurde ein Verfahren eingerichtet. Alle Mitarbeiter, Auftragsverarbeiter und Dienstleister, die an der Verarbeitung personenbezogener Daten beteiligt sind, müssen die Geschäftsführung über

*Diese Entwurfsvorlage ist immer individuell anzupassen*

jede Verletzung des Schutzes personenbezogener Daten informieren. Die Geschäftsführung entscheidet unter Einbeziehung des Datenschutzbeauftragten über weitere zu treffende Maßnahmen, insbesondere über die Benachrichtigungspflicht des Betroffenen und die Meldepflicht an die Datenschutz-Aufsichtsbehörde.

## 6. Weiterführende Dokumentationen

*[Hinweis: Individuelle Gestaltung der weiteren Dokumentation (z. B. zusammen oder getrennte Dokumentation von Verzeichnissen mit technisch – organisatorischen Maßnahmen sowie Ausnahmegenehmigungen, Meldepflichten und Datenschutzverletzungen]*

- Verzeichnis der Verarbeitungstätigkeiten**
- Rollierende Dokumentation (Prüfung, Schulung, DS-Folgenabschätzung, Ausnahmen)**
  - ☞ Zur Vereinfachung der Umsetzung ggf. separate Dokumentation zu:*
    - Liste der Auftragsverarbeiter und Verträge*
    - TOM – Technische und organisatorische Maßnahmen*
    - ...*

## 7. Letzte Änderung:

*[Hinweis: Aufbewahrung von 2 Jahren zum rückwirkenden Nachweis]*

Ort, Datum:

---

Geschäftsführung / Verantwortlicher

---

Dokument erstellt/veröffentlicht [Datum] / [ORT]

---