Datenschutz – Leitlinie

**Inhaltsübersicht**

§ 1 Präambel

§ 2 Strategie

§ 3 Geltungsbereich

§ 4 Zielsetzung

§ 5 Organisation

§ 6 Maßnahmen

§ 7 kontinuierliche Verbesserung des Datenschutzniveaus

§ 8 Geltungsdauer

**§ 1 Präambel**

Im Mai 2016 ist die Europäische Datenschutz-Grundverordnung (DSGVO) in Kraft getreten. Nach einer Karenzzeit von zwei Jahren gilt die DSGVO ab dem 25.05.2018 als unmittelbar geltendes Recht in jedem Mitgliedsstaat. Zum gleichen Zeitpunkt werden am 25. Mai 2018 auch das neue Bundesdatenschutzgesetz und neue Landesdatenschutzgesetze in Kraft treten. Für alle Unternehmen ergeben sich daraus neue Chancen und Risiken.

Unsere Kunden, Beschäftigte und all unsere Geschäftspartner vertrauen uns ihre Daten an und erwarten zu Recht, dass wir ihre Privatsphäre achten. Die neue DSGVO fordert von uns ein proaktives Datenschutzmanagement. Die Respektierung des Datenschutzes ist künftig unabdingbare Voraussetzung für den Unternehmenserfolg. Es müssen angemessene Maßnahmen ergriffen werden, um Datenschutzkonformität zu erreichen und aufrecht zu erhalten.

Deshalb verabschiedet die Geschäftsleitung diese Leitlinie als Bestandteil ihrer Strategie. Mit dieser Leitlinie initiiert die Geschäftsleitung den Datenschutzprozess und übernimmt hierfür die Gesamtverantwortung.

**§ 2 Strategie**

Die Geschäftsleitung unterstützt die Wahrung der Datenschutz-Konformität durch eine proaktive Managementstrategie. Sie betreibt einen Datenschutz-Prozess als eine kontinuierliche Folge von Vorgängen zum Erreichen und Erhalten des erforderlichen Datenschutzniveaus.

Als erster Schritt erlässt die Geschäftsleitung eine Datenschutz-Richtlinie, gibt sie durch Unterzeichnung frei und macht sie allen Beschäftigten im Unternehmen bekannt.

Durch die Datenschutz-Leitlinie wird der Datenschutzprozess initiiert. Es werden Ziele vorgegeben, organisatorische Regelungen festgelegt und erste Maßnahmen bestimmt.

Die Leitlinie und das sich daraus entwickelnde Datenschutzkonzept wird regelmäßig auf Aktualität und Wirksamkeit überprüft. Die Überprüfung findet mindestens einmal jährlich statt. Bei gegebenem Anlass auch unterjährig.

Das Ergebnis der Überprüfung und die sich daraus ergebenden Maßnahmen werden dokumentiert und bilden somit die Grundlage für die Erfüllung der Rechenschaftspflicht nach Art. 5 Abs. 2 DSGVO.

**§ 3 Geltungsbereich**

Diese Leitlinie gilt für das gesamte Unternehmen. Die Leitlinie gilt auch für Prozesse, die in unserem Auftrag von Dienstleistern erbracht werden**.**

**§ 4 Zielsetzung**

Die Geschäftsleitung verfolgt das strategische Ziel, die Grundsätze der DSGVO für die Verarbeitung personenbezogener Daten bei allen Geschäftsprozessen konsequent einzuhalten. Diese Grundsätze sind gemäß Art. 5 DSGVO

* Vertraulichkeit, Integrität und Richtigkeit der Informationen,
* Rechtmäßigkeit und Transparenz, Verarbeitung nach Treu und Glauben,
* Datenminimierung und Zweckbindung sowie
* Begrenzung der Speicherdauer nach dem Grundsatz der Erforderlichkeit.

**§ 5 Organisation**

Die Verantwortung für die Sicherheitsorganisation liegt bei der Geschäftsleitung. Für einzelne Aufgabenbereiche definiert die Geschäftsleitung Funktionen und bestimmt die zuständigen Personen.

Zur Koordination der Aufgaben und Ergebnisse hat die Geschäftsleitung ein Datenschutz-Team berufen. Dieses setzt sich zusammen aus dem Datenschutzbeauftragten, der IT-Leitung und dem Leiter der Innenrevision (optional).

Das Team wird über alle Maßnahmen, die einen Bezug zum Datenschutz haben können, rechtzeitig informiert. Es prüft die Einhaltung der genannten Datenschutzgrundsätze, weist auf Risiken hin und erarbeitet Empfehlungen. Das Datenschutz-Team wird geleitet durch N. N., er/sie berichtet die Ergebnisse direkt an die Geschäftsleitung.

Alle Mitarbeiter und Führungskräfte des Unternehmens sind sich ihrer Verantwortung für den Datenschutz bewusst und haben das Datenschutz-Team zu unterstützen. Obwohl gesetzlich nicht vorgeschrieben, müssen alle Mitarbeiter eine Verpflichtungserklärung zur Kenntnis nehmen. Bei Zielkonflikten entscheidet die Geschäftsleitung nach vorheriger Beratung mit dem Datenschutz-Team und dem betroffenen Fachbereich.

**§ 6 Maßnahmen**

Der Datenschutzbeauftragte erstellt mit direkter Unterstützung des Datenschutz-Teams ein „Datenschutz-Rahmenkonzept“. Das Konzept konkretisiert die Vorgehensweise zur Erreichung und Aufrechterhaltung der Datenschutzkonformität.

Das Datenschutz-Rahmenkonzept beschreibt unter anderem die Vorgehensweise für die Erstellung des Verarbeitungsverzeichnisses, die Bewertung der Rechtsgrundlagen, die Risikoanalyse, die Transparenz-regularien, die Sensibilisierung der Beschäftigten, die technischen und organisatorischen Maßnahmen, das Löschkonzept sowie Verhaltensregeln in besonderen Situationen. Das Konzept dokumentiert auch die durch die Geschäftsleitung festgelegten Zuständigkeiten und Verantwortlichkeiten im Datenschutzprozess.

**§ 7 Kontinuierliche Verbesserung des Datenschutzniveaus**

Diese Leitlinie und das Datenschutz-Rahmenkonzept werden regelmäßig auf ihre Aktualität und Wirksamkeit geprüft. Sie werden auch regelmäßig daraufhin untersucht, ob sie den betroffenen Mitarbeitern bekannt sind, und ob sie umsetzbar und in den Betriebsablauf integrierbar sind.

Die Geschäftsleitung unterstützt die ständige Verbesserung des Datenschutzniveaus. Alle Mitarbeiter sind angehalten, mögliche Verbesserungen, Schwachstellen und Risiken an das Datenschutz-Team oder den Datenschutzbeauftragten zu berichten.

Die Überprüfung dieser Leitlinie und des Datenschutz-Rahmenkonzepts findet mindestens einmal jährlich statt.

**§ 8 Geltungsdauer**

Diese Leitlinie tritt mit Unterzeichnung durch die Geschäftsleitung in Kraft. Sie wird unverzüglich betriebsweit bekannt gegeben. Sie gilt, bis sie außer Kraft gesetzt oder durch eine jüngere Fassung ersetzt wird.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Datum Unterschrift Geschäftsleitung