**Leitlinie zu Datenschutz- und Informationssicherheit**

### Änderungshistorie

|  |  |  |  |
| --- | --- | --- | --- |
| **Version** | **Datum** | **Autor** | **Änderungen** |
| **0.1** | 09.05.0218 | S. Paulus | Initiale Erstellung |
|  |  |  |  |

### Inhaltsverzeichnis

Änderungshistorie 2

Inhaltsverzeichnis 2

§1 Zweck und Ziele 3

§2 Verbindliche Aktivitäten 3

§3 Sicherstellung der nachhaltigen Wirksamkeit des Management-Systems 4

§4 Rollen und Verantwortlichkeiten 4

§5 Verstöße 5

§6 Weitergehende Regelungen 5

§7 Inkrafttreten 5

# §1 Zweck und Ziele

(1) Zweck dieser Leitlinie ist es, Vorgaben an eine gesetzeskonforme und angemessene Steuerung von Datenschutz- und Informationssicherheitsrisiken für die Firma XXX zu formulieren, Rollen und Verantwortlichkeiten festzulegen und weitere, mitgeltende Dokumente zu spezifizieren.

(2) Die Ziele der in diesem Dokument formulierten Vorgaben sind:

* + die gesetzeskonforme Verarbeitung von personenbezogenen Daten sicherzustellen,
  + die Vertraulichkeit, Integrität und Verfügbarkeit von schützenswerten, durch Verfahren verarbeiteten Informationen sicherzustellen,
  + die Verfügbarkeit des eigenen Geschäftsbetriebs sicherzustellen und

negative Auswirkungen auf Dritte zu verhindern.

(3) Hierzu führt die Firma XX ein integriertes Datenschutz- und Informationssicherheitsmanagementsystem (DISMS) ein.

(4) Diese Leitlinie ist für alle Beschäftigte verbindlich. Sich aus dieser Leitlinie ergebende Anforderungen an Dienstleister oder andere Dritte sind geeignet vertraglich zu regeln.

(5) Diese Leitlinie regelt den datenschutzkonformen und sicheren Umgang mit Informationen in jedweder Erscheinungsform (digital, in Papierform, gesprochenes Wort etc.).

# §2 Verbindliche Aktivitäten

(1) Die Firma XX erstellt und pflegt ein Verzeichnis der Verfahren, welche personenbezogene Daten verarbeiten. Dabei werden Löschfristen für alle personenbezogenen Daten definiert; die gesetzlichen Aufbewahrungsfristen sind zu beachten.

(2) Die Firma XX führt eine regelmäßige Risikoanalyse durch, welche die Schutzziele des Datenschutzes und die Risiken für die Informationssicherheit berücksichtigt. Für Verfahren, die sehr hohe Risiken für betroffene Personen aufweisen, ist eine Datenschutz-Folgenabschätzung durchzuführen.

(3) Es werden angemessene technische und organisatorische Schutzmaßnahmen eingesetzt, um die Risiken adäquat zu senken.

(4) Bei der Verarbeitung von personenbezogenen Daten sind die Informationspflichten zu beachten.

(5) Die Firma XX setzt geeignete und angemessene Erkennungsmaßnahmen ein, um eine Verletzung von Schutzzielen (z.B. durch einen unerlaubten Zugriff auf personenbeziehbare Daten, oder einen Cyber-Angriff) feststellen zu können. Bei Verletzung von Schutzzielen („Vorfällen“) werden die Auswirkungen eingedämmt und es wird unverzüglich wieder ein sicherer Zustand hergestellt.

(6) Es wird ein Berichtsweg für die Meldung von Datenschutz- und Sicherheitsvorfällen (ggf. auch an externe Interessensgruppen, z.B. Datenschutzbehörden oder Betroffene) eingerichtet.

(7) Es wird eine Kontaktstelle für die Erfüllung der Betroffenenrechte (Transparenz, Herausgabe der Daten, Löschung) eingerichtet.

(8) Die Beschäftigten, Professoren und Studierenden werden regelmäßig auf ein Datenschutz-konformes und sicheres Verhalten sensibilisiert und geschult.

# §3 Sicherstellung der nachhaltigen Wirksamkeit des Management-Systems

(1) Die Einhaltung der Vorgaben und die Wirksamkeit der Maßnahmen wird regelmäßig geprüft. Der Grad der Erreichung der Datenschutz- und Sicherheitsziele wird regelmäßig ermittelt. Diese Leitlinie wird regelmäßig auf Aktualität geprüft und ggf. angepasst.

(2) Die Geschäftsführung ist mindestens jährlich über den aktuellen Status in Bezug auf Datenschutz und Informationssicherheit zu informieren, und hat in der Folge über ggf. erforderliche Anpassungen zu entscheiden.

# §4 Rollen und Verantwortlichkeiten

(1) Die Geschäftsführung ist für die erfolgreiche Umsetzung des DISMS verantwortlich, stellt die hierfür erforderlichen personellen, organisatorischen und materiellen Ressourcen bereit und beschließt weitergehende Regelungen zu den Themen Informationssicherheit und Datenschutz.

(2) Die Abteilungsleiter sind dafür verantwortlich, sich über die DISMS-bezogenen Risiken in ihrem Bereich Kenntnis zu verschaffen, deren Steuerung einzuleiten und zu kontrollieren, Datenschutz- und Informationssicherheitsvorfälle zu behandeln sowie Anpassungen umzusetzen.

(3) Die Firma XX bestellt einen Datenschutz- (und Informationssicherheits-) beauftragten. Er wirkt auf die Einhaltung des Datenschutzes hin. Insbesondere überwacht er die Anwendung der Datenverarbeitungsprogramme und informiert, sensibilisiert und berät alle Mitarbeiter zur gesetzeskonformen Verarbeitung von Daten. Er erfasst kontinuierlich den Status der Informationssicherheits-Risiken, bewertet diese und berichtet sie an die Geschäftsleitung. Er unterstützt er die Geschäftsleitung bei der Auswahl angemessener Sicherheitsmaßnahmen zur Steuerung der Risiken. Der Informationssicherheitsbeauftragte ist der erste Ansprechpartner bei Sicherheitsvorfällen, unterstützt bei der Behandlung und verfolgt die Abarbeitung. Er ist Kontaktstelle für die zuständige Aufsichtsbehörde. Der Datenschutzbeauftragte ist weisungsfrei und berichtet direkt an die Geschäftsführung. Ihm werden alle erforderlichen Einrichtungen, Geräte und Mittel zur Verfügung gestellt, die er für die Ausübung seiner Tätigkeit benötigt. Der Datenschutzbeauftragte ist zu regelmäßigen Weiterbildungen verpflichtet.

(6) Die IT-Verantwortlichen stellen die Umsetzung der Anforderungen in Bezug auf Datenschutz und Informationssicherheit mit geeigneten technischen Maßnahmen zur Risikominderung sicher. Wird ein externer IT-Leistungserbringer eingesetzt, so sind die Anforderungen zu übermitteln und deren Einhaltung bzw. Umsetzung sicherzustellen.

(7) Alle Mitarbeiter haben sich jederzeit so zu verhalten, dass Datenschutz und Informationssicherheit in ihrem Aufgaben- und Verantwortungsbereich sichergestellt ist. Datenschutz- bzw. sicherheitsrelevante Vorkommnisse sind unverzüglich an den Datenschutzbeauftragten zu melden.

# §5 Verstöße

(1) Verstöße gegen die Vorgaben in dieser Leitlinie können zu disziplinar- oder arbeitsrechtlichen Konsequenzen führen.

# §6 Weitergehende Regelungen

(1) Die Geschäftsleitung veröffentlicht mitgeltende Dokumente zu Präzisierung dieser Regelungen in geeigneter Form.

# §7 Inkrafttreten

(1) Diese Leitlinie tritt am XXX in Kraft.

Ort, Unterschrift