Richtlinie bei Datenschutzverletzungen

INGOLD SOLUTIONS GMBH

Richtlinie bei Datenschutzverletzungen

(Referenz-Nr.: ISMS/IS/5.2/21)

Geltungsbereich:

1. Sicherheitsvorfälle (SI) beinhalten unsachgemäße Handhabung oder Offenlegung von Informationen und können bei personenbezogenen Daten zu Datenschutzverletzungen führen. Diese Richtlinie behandelt primär personenbezogene Datenschutzverletzungen, ist aber auch auf andere SI anwendbar (Eindämmung, Untersuchung, Verbesserung, Lessons Learned).

2. Datenschutzverletzungen können versehentlich auftreten, z. B. durch Fehlrteile oder Bedienfehler, wobei private Daten verloren gehen oder unrechtmäßig offengelegt werden. Die Richtlinie gilt auch für vertrauliche Geschäftsdaten.

3. Mitarbeiter müssen mit sensiblen Informationen verantwortungsvoll umgehen. INGOLD SOLUTIONS GMBH klassifiziert Informationen als OFFIZIELL oder OFFIZIELL SENSITIV mit entsprechenden Handhabungshinweisen. Verstöße können disziplinarisch geahndet werden.

4. Die meisten Verstöße sind menschliche Fehler, dennoch gilt diese Richtlinie auch für systembedingte Vorfälle.

5. Vorgehen bei Datenschutzverletzungen:

- Eindämmung des Vorfalls
- Informieren von Management und Datenschutzbeauftragten

Richtlinie bei Datenschutzverletzungen

- Untersuchung, Dokumentation und Risikoabschätzung
- Maßnahmen gegen verantwortliche Personen

Maßnahmen bei Datenschutzverletzung:

6. Wird eine falsche Datenweitergabe erkannt, sind umgehend der Vorgesetzte und der Datenschutzbeauftragte zu informieren. Andernfalls drohen disziplinarische Maßnahmen.

7. Vor etwaigen Gegenmaßnahmen ist Rücksprache mit dem Datenschutzbeauftragten zu halten.

8. Innerhalb von 24 Stunden erfolgt eine Erstuntersuchung durch den Datenschutzbeauftragten oder eine benannte Person.

9. Vorgehen nach dem CARE-Modell:

- Contain - Eindämmung
- Assess - Bewertung des Ausmaßes
- Respond - Maßnahmen ergreifen
- Evaluate - Maßnahmen überprüfen und nächste Schritte planen

10. Der Vorgesetzte informiert ggf. den Kommunikationsmanager, kontaktiert den irrtümlichen Empfänger (zur Löschung oder Rückgabe), informiert betroffene Personen per E-Mail mit:

- Kontaktdaten
- Zeitpunkt, Inhalt, Art der Daten
- Maßnahmen zur Rückgewinnung
- Informationen zu weiteren Entwicklungen

Richtlinie bei Datenschutzverletzungen

11. Innerhalb einer Woche erfolgt ein Abschlussbericht durch den Datenschutzbeauftragten an die Geschäftsleitung:

- Beschreibung des Vorfalls
- Betroffene Personen und Datenverarbeiter
- Risikoabschätzung
- Ursachenanalyse
- Maßnahmenplan
- Empfehlung zur Meldung an Aufsichtsbehörde (z. B. BfDI)

12. Die Personalabteilung wird regelmäßig über Entwicklungen informiert.

13. Erfolgt vom Empfänger innerhalb von 48 Stunden keine Rückmeldung, sind Nachfassaktionen per E-Mail und Telefon zu protokollieren und zu wiederholen, bis eine Lösung erzielt ist.