



Das INTARGIA Datenschutzmanagementsystem

Effektiver Datenschutz mit Augenmaß

Kontaktdaten:



IT-SICHERHEITS-
MANAGEMENT

Dr. Thomas Jurisch, Steffen Weber

Telefon: +49 (0)6103 350860

E-Mail: it-sicherheitsmanagement@intargia.com

Webseite: <http://www.intargia.com>

Das INTARGIA Datenschutzmanagementsystem (DSMS)

Nachhaltigkeit und Effektivität können sich in unseren Augen nur durch einen geplanten, systematischen und zyklischen Prozess einstellen. Aus diesem Grund haben wir unser DSMS auch am generischen Management-Kreislauf „Planen, Durchführen, Kontrollieren, Handeln“ angelehnt.



Aufbauend auf einem Initialaudit wird zusammen mit dem Kunden die Datenschutzstrategie definiert sowie anschließend technische und organisatorische Maßnahmen geplant und umgesetzt. Die Umsetzung wird kontrolliert und regelmäßig hinsichtlich Effektivität und Effizienz auditiert und durch bedarfsabhängige Datenschutzberatung ergänzt. Eingebettet in eine funktionierende Datenschutzorganisation und –Kultur wird durch professionelles Projektmanagement sichergestellt, dass alle Ziele unter Berücksichtigung von Zeit, Kosten und Qualität erreicht werden.

Wir möchten Ihnen nun die einzelnen Phasen im Detail vorstellen:

Audit, Übung, Wartung



Zu Beginn wird im Rahmen eines Initial-Audits der aktuelle Ist-Zustand aller relevanten Bereiche des betrieblichen Datenschutzes im Unternehmen analysiert und bewertet. Auf Basis dieser Erkenntnisse kann dann der weitere Projektverlauf systematisch geplant und die einzurichtenden technischen und organisatorischen Maßnahmen ausgewählt werden.

Untersucht werden alle datenschutzrechtlich relevanten Unternehmensbereiche wie die interne IT-Leistungserbringung, Personalwesen, Vertrieb, Einkauf und Finanzbuchhaltung. Neben diesen gewöhnlich zentral organisierten Funktionsbereichen müssen auch, falls vorhanden, weitere Standorte des Unternehmens in das Audit miteinbezogen werden. Für diese zusätzlichen Standorte ist jeweils ein eigenes Teil-Audit durchzuführen, für welches eine reduzierte Version des Auditkatalogs verwendet wird.

Das Initialaudit umfasst inhaltlich

- Das Unterzeichnen einer Vertraulichkeitsvereinbarung.
- Ein im Vorfeld durchzuführendes Self-Assessement (Inhalt sind hauptsächlich Fragen zu bereits stattgefundenen Datenschutz-Aktionen und erste Informationen über einzubeziehende Personen und Geschäftsprozesse).
- Eine Kick-off-Veranstaltung, in welcher INTARGIA dem Kunden das Datenschutzmanagementsystem vorstellt, für fachliche Fragen zur Verfügung steht und gemeinsam die Projektplanung durchgeführt wird.
- Eine Auswertung der bereits vorhandenen Dokumente.
- Vor-Ort-Interviews mit den einzubeziehenden Personen im Unternehmen. Dieser Punkt ist das Kernstück des Initial-Audits. Hierfür hat INTARGIA zusammen mit seinem Partner, der Gesellschaft für Datenschutz und Datensicherheit e. V., für alle wichtigen Funktionsbereiche eines Unternehmens spezifische Audit-Kataloge entwickelt, die gemeinsam bearbeitet werden. Die Kataloge enthalten alle relevanten Punkte, welche im Bereich betrieblicher Datenschutz wichtig sind und berücksichtigt die jeweils aktuelle Rechtslage. Einbezogen werden auch diverse nationale und internationale Standards für IT-Sicherheit, betriebli-

chen Kontinuitätsmanagement und Datenschutz (z. B. ISO/IEC 27000ff., BSI 100-1 bis 100-4 und BS 25999).

- Verifizierung der Angaben durch Stichprobenuntersuchungen vor Ort.
- Erkennen von Handlungsbedarf.
- Erstellung eines detaillierten Auditberichts in enger Abstimmung mit dem Kunden.
- Vorstellung der Vorgehensweise, Untersuchungsergebnisse und Handlungsempfehlungen in einer Abschlusspräsentation (hier erfolgt der Übergang zum nächsten Punkt des DSMS „Strategie definieren, Maßnahmen planen“).

Teil B: Prüfkatalog allgemeiner Teil

1) Zutrittskontrolle	
Beschreibung: Mit den einzelnen Zutrittskontrollen ist zu unterbinden, dass Unbefugte Zutritt zu Datenverarbeitungsanlagen erlangen können. Es stellt sich stets die Frage, welche technischen und organisatorischen Maßnahmen zur räumlichen Zutrittskontrolle eingesetzt werden.	
Fragen	Antworten
Existiert ein zentraler Werkschutz/Pfortner/Empfang?	
Existieren Türsicherungen an allen relevanten Zugangstüren zum Gebäude/Stockwerk/Abteilung? (Realisiert z. B. per Schliesssystem, Magnetkarten, Chipkarten, Ausweislesegeräte, Zugangscode/Numpads)?	
Wird die Vergabe dieser Zutrittsmedien systematisch vorgenommen, überwacht und ist dies revisionsicher dokumentiert (z. B. per Schlüsselbuch)?	

Abbildung 1: Beispiel für Fragen des Auditkatalogs

Erfahrungsgemäß ist die initiale Aufnahme des Status quo der aufwändigste Arbeitsschritt. Selbstverständlich werden im Laufe des Projektes weitere, zyklische Audits durchgeführt. Diese sind dann jedoch weniger aufwändig, da in diesen dann hauptsächlich die Prüfung des Umsetzungsgrades der empfohlenen Maßnahmen stattfindet und ggf. neue gesetzliche oder technische Entwicklungen vorgestellt werden. Hauptziel der Audits ist langfristig eine kontinuierliche Verbesserung des Niveaus des Datenschutzes im Unternehmen und eine Vergleichbarkeit mit vorherigen Perioden. Dazu mehr im Abschnitt „Umsetzung kontrollieren“.

Zugangskontrolle – Passwörter und Bildschirmspernung

Aktueller Status

- Passwörter werden einmal vom User vergeben, keine Änderungen vorgesehen.
- Eine Computerspernung ist nicht aktiv.

Untersuchungsergebnisse

- Ohne Passwort-Richtlinie kann nicht sichergestellt werden, dass die Passwörter der Mitarbeiter eine ausreichende Güte besitzen. Des Weiteren stellt die Einrichtung eines einzigen Passwortes auf unbestimmte Zeit eine Systemgefahr dar.
- Ohne Computerspernung kann z. B. bei nicht ordnungsgemäßem Herunterfahren des Systems Zugang auf die Netzlaufwerke und die IT-Systeme erlangt werden.


Handlungsempfehlungen	
<ul style="list-style-type: none"> • Passwort-Richtlinie erstellt werden. Integration in das Datenschutzhandbuch. • Zyklische systemseitige Passwortwechsel • Eine systemseitige Computerspernung sollte unumgänglich aktiviert werden. 	

Abbildung 2: Beispiel für die Ergebnispräsentation

Sowohl in Abschlusspräsentationen als auch den Auditberichten verwendet INTARGIA ein Reifegradmodell, welches auf Vorgaben aus Best-practice-Vorgehensweisen basiert. Durch fünf Reifegrade (z. B. „0“ bedeutet, dass keinerlei Datenschutzkonformität erreicht wird und wird mit einer roten Ampel ausgedrückt, „4“ stellt eine optimale Datenschutzkonformität dar und wird mit einer grünen Ampel ausgedrückt).

Strategie definieren, Maßnahmen planen



Basierend auf den Ergebnissen des/der Audits wird gemeinsam mit dem Kunden eine Datenschutzstrategie erstellt und sich daraus ableitende Maßnahmen definiert und geplant.



Des Weiteren werden von den Verantwortlichen im Unternehmen die Ziele festgelegt, welche durch das Datenschutzmanagementsystem erreicht werden sollen.

Ebenso sind in dieser Phase organisatorische Aspekte wie Gesamtverantwortlichkeit für den Datenschutz, Festlegung des primären Ansprechpartners, Berichtswege und angrenzende Funktionen (z. B. Risikomanagement oder Betriebsrat) zu behandeln. Elementar ist an dieser Stelle die Besprechung und Auswahl von geeigneten technischen und organisatorischen Maßnahmen.

Abschließend wird gemeinsam ein Zeitplan erarbeitet und die Durchlaufhäufigkeit der Zyklen festgelegt.

Strategien und Maßnahmen implementieren




Die Ergebnisse der Planungsphase werden nun umgesetzt. Basierend auf dem vorher erstellten Zeitplan werden alle Maßnahmen in Angriff genommen, welche bis zum nächsten Audit umgesetzt werden sollen. Gespeist werden diese Maßnahmenvorschläge durch die Vorgaben der relevanten Gesetze, die langjährige Erfahrung der Datenschutzexperten von INTARGIA sowie diversen Standards, in welchen „Best Practice“-Vorgehensmodelle beschrieben sind.

Beispiele für Maßnahmen sind z. B. die Etablierung der Datenschutzorganisation, die Erstellung und Veröffentlichung eines Datenschutzhandbuchs, die Sicherstellung der datenschutzkonformen Entsorgung von Datenträgern und Papiermüll, die Optimierung der IT-Sicherheitssysteme oder das Anlegen der vom Gesetzgeber geforderten Verzeichnisse.



INTARGIA

 INTARGIA	<Kunde> <Projekt> Verfahrensverzeichnis intern <Datum>	
--	---	--

Verfahrensverzeichnis

Bezeichnung: _____

Laufende Nummer: _____

Verfahren: neues Verfahren
 Anpassung Verfahren _____

- das Verfahren ist zur Einsichtnahme bestimmt
- das Verfahren ist nur teilweise zur Einsichtnahme bestimmt
 - 1 Name und Anschrift
 - 2 Zweckbestimmung
 - 3 Art der gespeicherten Daten
 - 4 Kreis der Betroffenen
 - 5 Art regelmäßig übermittelter Daten
 - 6 Zugriffsberechtigte Personen
 - 7 Technische und organisatorische Maßnahmen
 - 8 Technik des Verfahrens
 - 9 Fristen für die Löschung

Abbildung 3: Beispiel für ein Verfahrensverzeichnis

Während des gesamten Projektes steht INTARGIA mit seinen Datenschutzexperten und Kooperationspartnern jederzeit beratend zur Verfügung. Dies gilt für Anfragen der Geschäftsleitung ebenso wie für Anfragen von Mitarbeitern und externen Stakeholder wie Kunden oder Lieferanten.

Umsetzung kontrollieren



Als wichtiger Bestandteil des Datenschutzmanagements wird der Wirkungsgrad der einzelnen Maßnahmen in Kooperation mit dem Kunden ständig kontrolliert und ausgewertet.

Dazu dienen zyklische Folgeaudits, in welchen der Umsetzungsgrad der vorgeschlagenen Maßnahmen überprüft wird.

INTARGIA nutzt dazu ein Reifegradmodell, welches einerseits einen übersichtlichen Überblick über den aktuellen Status des Datenschutzes im Unternehmen zulässt und zum anderen einen direkten Vergleich mit früheren Stati ermöglicht. Daraus lassen sich dann jederzeit Aussagen über die Weiterentwicklung von Datenschutz im Unternehmen ableiten.

Regelmäßiges Reporting an die Verantwortlichen im Unternehmen gehört ebenso zur Umsetzungskontrolle wie die professionelle Dokumentation von Status und Fortschritt des Datenschutzmanagementsystems.

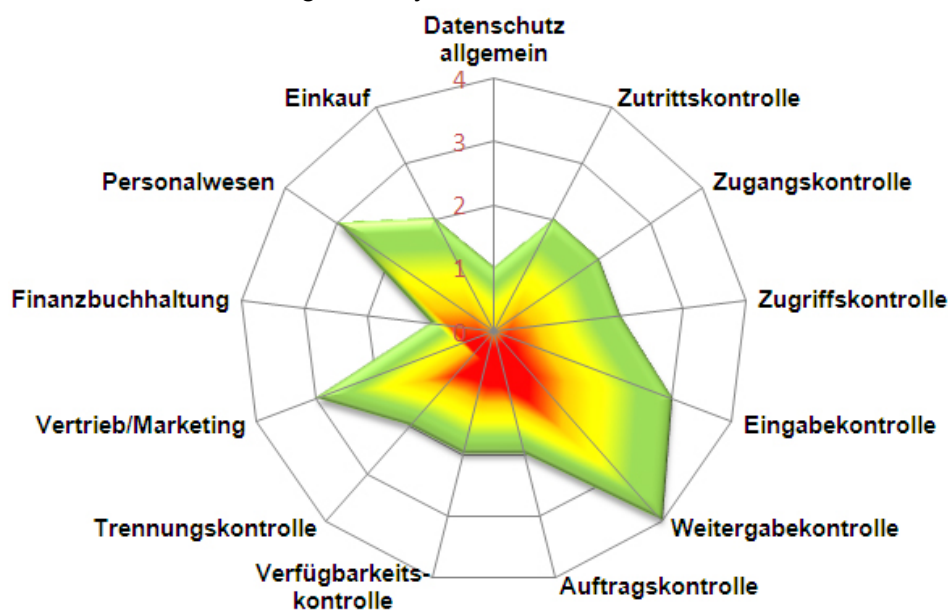
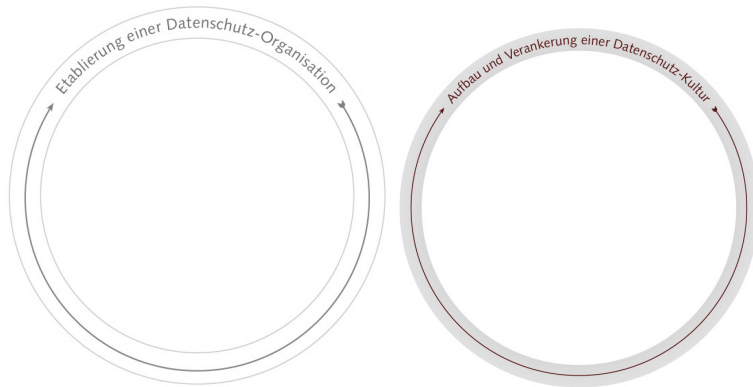


Abbildung 4: Beispiel für eine Reifegradmessung (Reifegrad 0-rot bis Reifegrad 4-grün)

Etablierung von Datenschutz-Organisation und Datenschutz-Kultur



„Der Mensch ist das größte Sicherheitsrisiko im Unternehmen.“ – Diese weitläufig akzeptierte Aussage zur Kritikalität von diversen Gefahrenquellen zeigt sehr deutlich, dass ohne eine vorhandene Sensibilität der Mitarbeiter und weiterer Stakeholder im Unternehmen kein zufriedenstellender Grad an Datenschutz erreicht werden kann. Deshalb liegt ein Hauptfokus unseres DSMS auch darauf, die Handelnden im Unternehmen für die Notwendigkeit von Datenschutz und Datensicherheit zu sensibilisieren. Dazu zählen z. B. Maßnahmen wie Datenschutzbildung, die Verpflichtung auf das Datengeheimnis gemäß Bundesdatenschutzgesetz oder regelmäßige Datenschutzhinweise, z. B. im Intranet oder per Newsletter.

Projektmanagement



Ein professionelles Projektmanagement sorgt in allen Phasen der Planungs-, Implementierungs-, Kontroll- und Auditprozesse dafür, dass die definierte Strategie und die Implementierung der ausgewählten Maßnahmen unter Einhaltung von Vorgaben hinsichtlich Zeit, Qualität und Kosten erfolgreich umgesetzt werden. Hierzu zählt selbstverständlich auch ständiges projektbegleitendes Reporting über den Projektfortschritt an die relevanten Personen im Unternehmen.



INTARGIA

<Datum>	IST					SOLL	Soll-Ist- Abgleich in d
	Verbrauch in h	Verbrauch in d	Verbrauch in %	Fachliche Fertig- stellung in %	Fachliche Fertig- stellung in %	Geplanter Aufwand in d	
Budget	280	35,0	143%				
Rest-Budget	-119	-14,9	-43%	aktuell	letzter Termin		
Meetings	11	1,4	55%	80%	60%	2,5	1,1
Workshops	20	2,5	42%	75%	70%	6	3,5
Projektmanagement	30	3,8	101%	90%	80%	3,7	0,0
Qualitätssicherung	100	12,5	250%	90%	80%	5	-7,5
Ungeplante Wartezeit	8	1,0	200%	90%	80%	0,5	-0,5
IT-Sicherheitsmanagement	22	2,8	50%	95%	80%	5,5	2,8
Organisation und Personal	55	6,9	181%	100%	90%	3,8	-3,1
Computervirenschutzkonzept	3	0,4	10%	85%	60%	3,6	3,2
Datensicherungskonzept	22	2,8	47%	60%	50%	5,8	3,1
Notfallvorsorgekonzept	29	3,6	107%	90%	70%	3,4	-0,2
Archivierung	25	3,1	112%	75%	50%	2,8	-0,3
Mitarbeitersensibilisierung	24	3,0	150%	80%	80%	2	-1,0
Internet- und E-Mail-Sicherheit	24	3,0	150%	85%	80%	2	-1,0
Netzwerk- und Serversicherheit	26	3,3	65%	60%	40%	5	1,8
Verbraucht	399	49,9				51,6	
Über-/Unterdeckung in Summe							1,7

Abbildung 5: Beispiel für proaktives Projektcontrolling

Fazit

Durch eine systematisch und methodisch saubere Planung und Durchführung von Datenschutzmanagement kann ein Unternehmen vielfältige Vorteile erzielen – Gesetzeskonformität, Minimierung der Geschäftsrisiken, Verbesserung der Geschäftsprozesse und der Organisation und Wettbewerbsvorteile stehen im Mittelpunkt der Überlegungen.

Die INTARGIA Managementberatung GmbH und ihre Kooperationspartner bieten hierfür ein eigens entwickeltes Datenschutzmanagement-System an, welches mit effizienter Methodik und eigenen Tools alle relevanten Aspekte von Datenschutz und Datensicherheit abdeckt und bei zahlreichen Unternehmen aller Branchen erfolgreich im Einsatz ist.

Wenn auch Sie Interesse an der Verbesserung Ihrer Unternehmensprozesse i. V. m. effektiver Gesetzeskonformität haben, sprechen Sie uns einfach an.