Datenschutz “leichter gemacht”: DSGVO-Umsetzung mit Schnittstellen zu ISO 27001

Dr. Bettina Thurnher, Information Security Manager,
Gebrüder Weiss

Agenda

- **DSGVO in der Praxis**
- **Umsetzungsprojekt: Rollen und Verantwortlichkeiten**
- **Datenschutz Prozesse im Unternehmen**
- **Mehrwerte aus dem Datenschutz-Projekt**

Fragen

1. Wie war Datenschutz bisher geregelt – was ändert sich drastisch?

2. Was bewirkt die österreichische Gesetzesnovelle vom 25.04.2018?

3. Gilt die DSGVO für alle Unternehmensformen und -größen?

4. Welche Daten sind durch die DSGVO geschützt bzw. welche nicht?
   (Kundendaten, Mitarbeiter-/Personaldaten, ...?)

5. Welche Abteilungen/Teile des Unternehmens sind davon betroffen?

6. Wie hat sich Gebrüder Weiss darauf vorbereitet?
   z.B. Mitarbeiter ausgebildet (Wo und wie – welche Kurse)?

7. Was hat sich bei der Software-Entwicklung diesbezüglich getan?

Data Protection Management System: DPMS-Konzept

Hintergrund:
Insbesondere die Erhöhung des **Strafrahmens** von derzeit max. EUR 25.000,-- auf **bis zu EUR 20 Millionen oder bis zu 4 % des weltweiten Jahresumsatzes bei Datenschutzverstößen ab Mai 2018** löst akuten Handlungsbedarf aus.

- Strafen bis EUR 20 Mio. oder 4 % vom weltweiten Jahresumsatz
- *EUR 1,36 Mrd. Nettoumsatz => EUR 54 Mio. Strafe*

Einhaltung der DSGVO:
Nur möglich über ein im Unternehmen durchgängig implementiertes Datenschutzmanagementsystem (DPMS) -> Prozess.

Die neue Datenschutz-Grundverordnung (DSGVO)

Hintergrund:

Mit der DSGVO gibt es ab 2018 eine neue, EU-weit einheitliche Rechtsgrundlage, die rechtliche Verschärfungen und hohe Strafen vorsieht. Die DSGVO verpflichtet Unternehmen ein Datenschutz-Management einzuführen, das den Schutz der personenbezogenen Daten in Unternehmen sicherstellen soll.

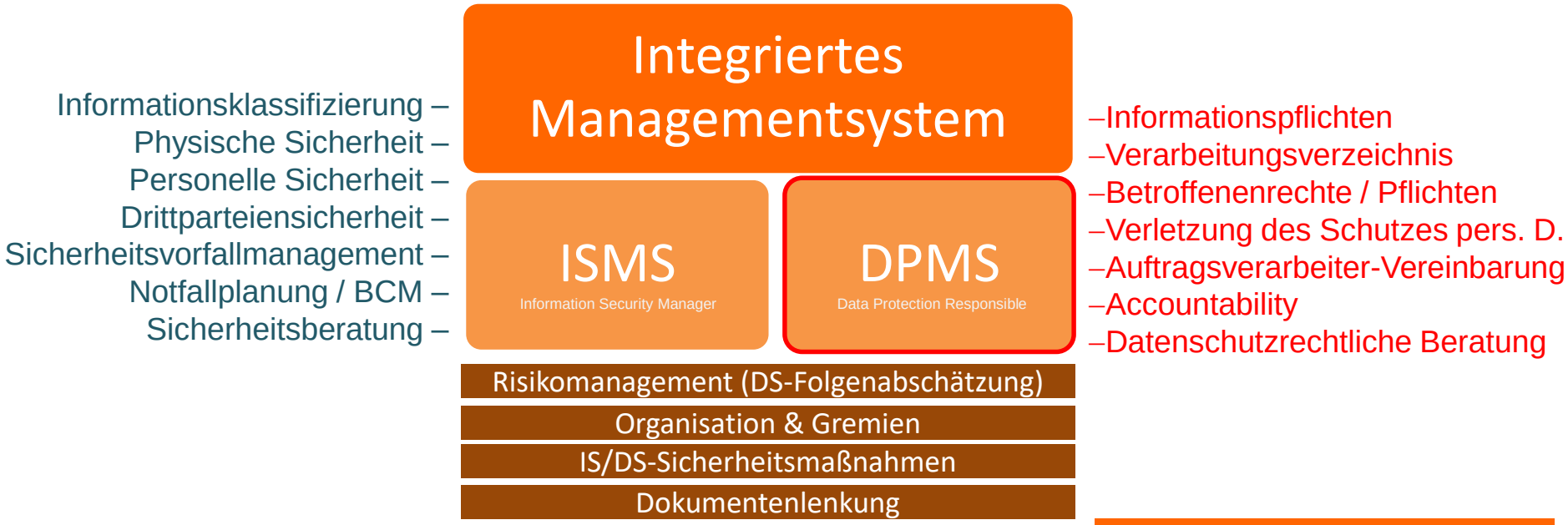
Durch unsere ISO 27001 Zertifizierung erfüllen wir bereits die Anforderungen an Datensicherheit gemäß Artikel 32 der DSGVO!

Mit der neuen **Rechenschaftspflicht („Accountability“)** müssen Gebrüder Weiss jederzeit und dokumentiert nachweisen, **wie, wo, wann und warum** personenbezogene Daten verarbeitet werden.

Data Protection Management System: DPMS-Konzept

Integration im Unternehmen:

Datenschutzkontrollen und -maßnahmen (controls) garantieren die richtige und effiziente Umsetzung der rechtlichen Vorgaben.



Was bedeutet die Umsetzung eines Data Protection Management Systems?

Was?

Personenbezogene Daten müssen identifiziert werden!

Personenbezogene Daten sind alle Daten, die sich auf bestimmte **Menschen** beziehen oder durch einfache Rückschlüsse auf diese Menschen beziehen lassen, sprich alle Informationen zu ihrer Identität.
Beispiele: Name, Personalnummer, Kundennummer

Wie?

- Es wird mittels Excel-Listen und Workshops erhoben wo überall personenbezogene Daten verarbeitet werden
- Vorgänge und verarbeitete Daten sowie Datenflüsse werden dokumentiert
- Ein Datenschutzhandbuch sowie Prozessbeschreibungen werden erstellt und ISMS-Richtlinien integriert
- Sicherheitsmaßnahmen werden etabliert

Wer?

- Data Protection Responsible (DPR)
- Data Protection Manager (DPM)
- Data Protection Agent (DPA)

Welche?

Sämtliche Verarbeitungen von personenbezogenen Daten‘ (Lesen, Speichern, Erheben, Ausdrucken, Übermitteln etc.)
Betroffenenrechte

Wo?

- Datenanwendungen, IT-Systeme
- Daten auf Fileshares
- Daten in Ablagen, Schränken, Aktenordnern etc.

Wozu?

- Wir müssen wissen, wo personenbezogene Daten verarbeitet werden
- Der Zweck und die Rechtsgrundlage müssen für die Datenverarbeitung vorliegen
- Der Aufforderung von Betroffenen zur Auskunft, Löschung, Richtigstellung oder Datenübertragung muss umgehend und vollständig nachgekommen werden
- Es müssen Verträge mit Auftragsverarbeitern/Dienstleistern vorliegen
- Die Dokumentation zu verarbeiteten personenbezogenen Daten muss der Behörde übermittelt werden

Datenschutzprozesse

- Beauskunftung
- Vertragsmanagement mit Partnern und Lieferanten
- Mitarbeiterprozesse: Eintritt, Aus- und Weiterbildung, Austritt
- Effiziente Umsetzung der gesetzlichen Anforderungen
- Schulung der Mitarbeiter

Mehrwerte aus dem Datenschutz-Projekt?

- Erfüllung von Kundenanforderungen: Halten von Kunden und Neukundengewinnung
- Verbesserungen der Datenqualität – Beispiel: Personalakte, Lieferabwicklung
- Festigung der Marktposition von GW

Data Protection Management System – Was bringt´s? Die Vorteile

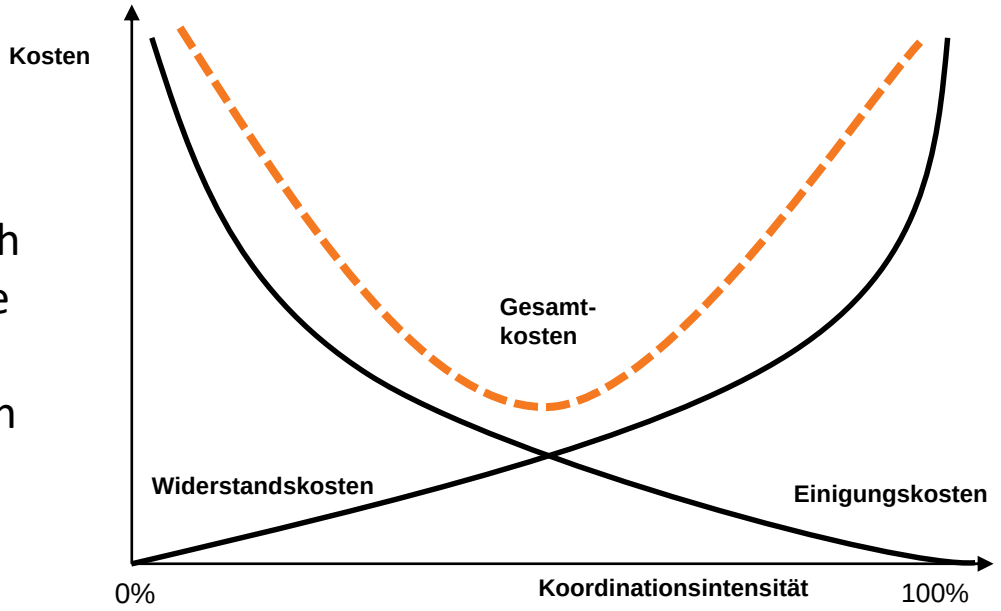
- Identifikation von effektivem Optimierungspotenzial bei bestehenden Geschäftsprozessen
  - Kosteneinsparungspotenzial durch Erhöhung der Daten[illegible]ität und...
  - Zukünftige effiziente Kundenabwicklung durch [illegible] Datenverwaltung bei GW
- Verbesserung der Datenqualität
  - Reduktion von Redun[illegible]enablage (elektronisch[illegible]
- Basis für Custon[illegible]
- Rechtssicherheit zu gesetzlichen Anforderungen
- Basis für datenschutzrechtl. Zertifizierungen (mögliche Erweiterung zur ISO 27001)
- Vermeidung von drohenden Risiken, Haftungen und Sanktionen

Data Protection Management ist ein Organisationsentwicklungsprojekt

Widerstand und Einigung – Zusammenhänge

Im Veränderungsmanagement wirken sich Widerstand und Einigung auf die Kosten aus

- Widerstandskosten entstehen durch fehlende Zustimmung der beteiligten Personen
- Einigungskosten ergeben sich durch Koordination von Aktivitäten, diese erhöhen sich mit dem relativen Anteil der entscheidungsbeteiligten Personen
- Ziel: Minimierung von Widerstandskosten und somit Optimierung der Koordinationsintensität



Quelle: Osterloh/Frost (1998), S. 181

Vielen Dank für Ihre Aufmerksamkeit

Dr. Bettina Thurnher

Information Security Manager

Gebrüder Weiss