Cyber-Sicherheitstag Niedersachsen 2018

22. Oktober 2018

Fachforum 5

Datenschutz und Informationssicherheit

ISMS und DSMS können in Teilen gemeinsam entwickelt werden

Heike Köhler, Geschäftsführerin WITstor GmbH

Informationssicherheit und Datenschutz

Hannover IT

Informationen = digitale Daten + gesprochenes Wort + geschriebenes Wort

KATEGORIE	SCHUTZ
INFORMATIONSSICHERHEIT	aller Informationen mit Schutzbedarf.
DATENSCHUTZ	natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Verkehr solcher Daten.
	der Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
	Der freie Verkehr personenbezogener Daten in der Union darf aus Gründen des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten weder eingeschränkt noch verboten werden.

DSMS – ISMS

Hannover IT

Datenschutz-Managementsystem (DSMS)

Schutz von personenbezogenen Daten

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben
- Transparenz
- Zweckbindung
- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaftspflicht
- persönliche Teilhabe und Zugang

Gefährdung
Verletzung von Persönlichkeitsrechten

Informationssicherheits-Managementsystem (ISMS)

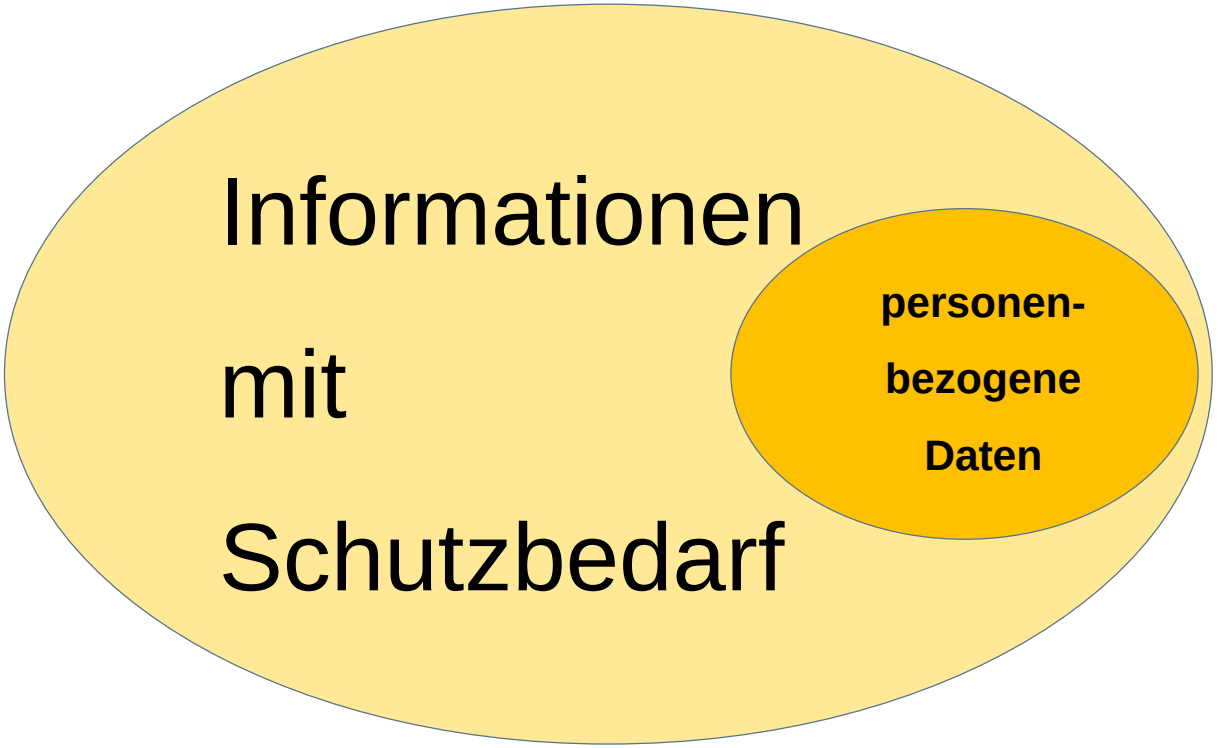
Schutz von Informationen der Organisation

- Vertraulichkeit
- Integrität
- Verfügbarkeit
- Authentizität

Gefährdung
Zerstörung, Verlust oder Verfälschung von Informationen

Informationssicherheit und Datenschutz

Hannover IT



Personenbezogene Daten sind eine TEILMENGE der in der Informationssicherheit zu schützenden Informationen. Die rechtlichen Anforderungen des Datenschutzes sind dabei zwingend zu beachten.

In Teilen gleiche Schutzziele

Hannover IT

Schutzziel	Informationssicherheit (ISMS)	Datenschutz (DSMS)
Vertraulichkeit Informationen dürfen nicht in unbefugte Hände, Ohren, Augen gelangen	✔	✔
Integrität Informationen müssen korrekt und verlässlich sein	✔	✔
Verfügbarkeit Informationen müssen entsprechend der Anforderungen verfügbar sein	✔	✔
Authentizität Echtheit, Zuverlässigkeit und Glaubwürdigkeit einer Information	✔	✔
Belastbarkeit (Resilenz) Widerstandsfähigkeit der Systeme	✔	✔

Das ISMS kann mit dem DSMS kombiniert werden bzw. auf Basis der ISO 27001 an den Datenschutz angepasst werden. ISO/IEC 27001, Annex A (Control objectivs and controls), kann so angepasst werden, dass die rechtlichen Anforderungen der DSGVO abgebildet werden können.

Managementsysteme

Hannover IT

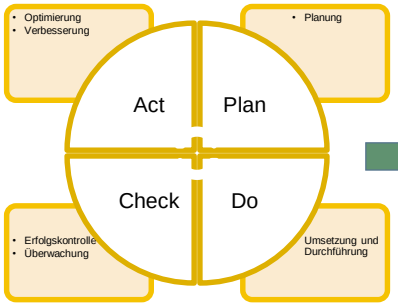
QMS
(Prozesskarte)

Assets
(HW, SW, Daten, DL…)

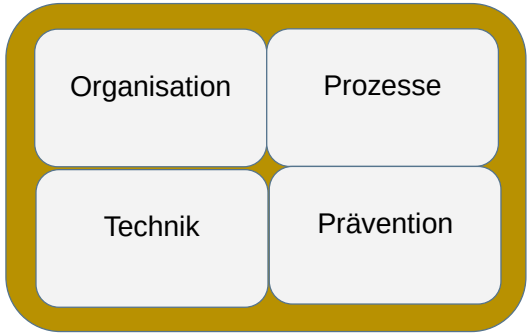
Management von organisations-eigenen Werten anhand des **Asset-Registers**

Management
von datenschutzrelevanten
Assets anhand der **Verarbeitungsübersicht**

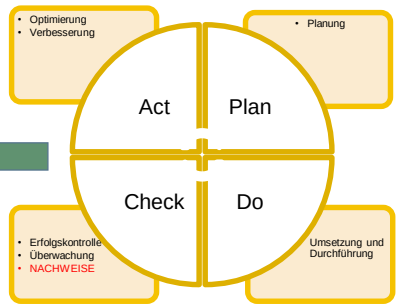
PDCA ISMS



Datenklassifikation
- öffentlich
- intern
- vertraulich
- geheim



PDCA DSMS



Datenklassifikation
- personenbezogene Daten
- personenbezogene Daten mit gesteigerter Schutzbedürftigkeit

Beide Managementsysteme verfolgen einen risikobasierten Ansatz und sind im Vorgehen identisch.

Risikomanagement

Hannover IT

RM ISMS

Organisation

Kriterien für **Eintrittswahrscheinlichkeit** und **Schwere eines Risikos** für **eine juristische Person**

Informationssicherheits-Beauftragter (CISO)

- Rechtliche Konsequenzen
- Finanzielle Schäden
- Prozessunterbrechung
- Stillstand
- Imageschäden
- Vertrauensverlust
- Verlust von Schlüsselpersonal

Datenverarbeitung

mögliche Schäden
physisch, materiell
und immateriell

Schwere des Schadens
geringfügig, überschaubar, substantiell
groß/existenzgefährdend

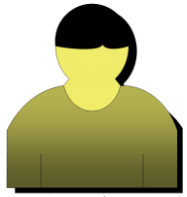
Eintrittswahrscheinlichkeit des Ereignisses
gering, normal, hoch, sehr hoch

Risikoabstufung
geringes Risiko, Risiko, hohes Risiko

RM DSMS

Betroffene

Kriterien für **Eintrittswahrscheinlichkeit** und **Schwere eines Risikos** für die **Rechte und Freiheiten** einer **natürlichen Person**



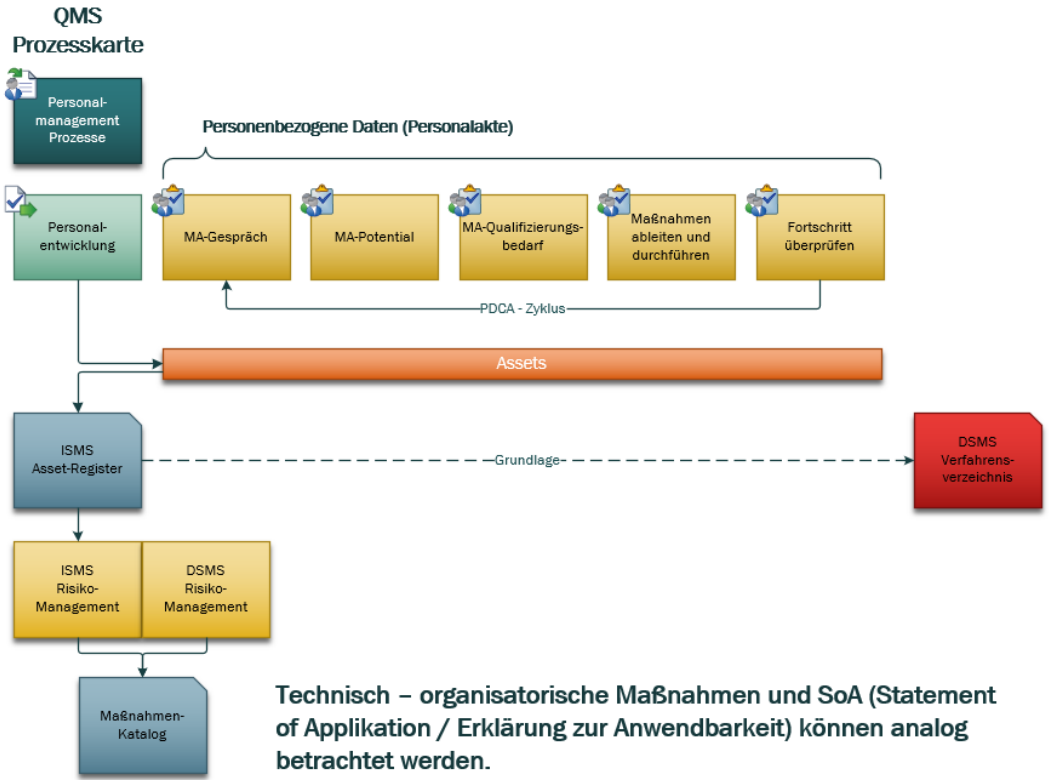
Datenschutz-Beauftragter

- Diskriminierung
- Rufschädigung
- Finanzieller Verlust
- Identitätsdiebstahl, -betrug
- wirtschaftliche und gesellschaftliche Nachteile
- Profilerstellung
- Ausschluss oder Einschränkung der Ausübung von Rechten und Freiheiten etc.

Im ISMS und DSMS können der gleiche Risiko-Prozess und dasselbe Risikobewertungsverfahren angewendet werden. Das RM DSMS ist im RM ISMS für organisatorisch-technische Maßnahmen abbildbar.

Beispiel: Daten Personalentwicklung

Hannover IT



Technisch – organisatorische Maßnahmen und SoA (Statement of Applikation / Erklärung zur Anwendbarkeit) können analog betrachtet werden.

ISO 27001, Assex A

5. Richtlinien
6. Organisation
7. Personalsicherheit
8. Verwaltung der Werte
9. Zugangssteuerung
10. Kryptographie
11. Physische und umgebungsbezogene Sicherheit
12. Betriebssicherheit

Technisch -organisatorische Maßnahmen (Auszug)

Hannover IT

Annex A	ISMS	DSMS
5. Richtlinien	5. 1 Informationssicherheitsrichtlinie 5.2 Überprüfung der Richtlinie	5.1 Datenschutzrichtlinie 5.2 Überprüfung der Richtlinie
6. Organisation	6.1 Interne Organisation 6.2 Richtlinie Mobilgeräte und Telearbeit	6.1 Interne Organisation 6.2 Richtlinien zur Auftragsverarbeitung
8. Verwaltung der Werte	Asset-Register	Verarbeitungsübersicht
9. Zugangssteuerung	9.1 Anforderungen 9.2 Benutzerzugangsverwaltung 9.3 Benutzerverantwortlichkeiten 9.4 Zugangssteuerung für Systeme und Anwendungen	9.1 Anforderung an Zugriffsberechtigte pers.b. Daten 9.2 Benutzerzugangsverwaltung 9.3 Benutzerverantwortlichkeiten 9.4 Zugangssteuerung für Systeme und Anwendungen
10. Kryptographie	10.1 Kryptografische Maßnahmen zum Schutz der Vertraulichkeit, Integrität und Authentizität	10.1 Kryptografische Maßnahmen pers.b. Daten zum Schutz von V, I, A
11. Physische und umgebungsbezogene Sicherheit	physische und umgebungsbezogene Sicherheit 11.1 Sicherheitsbereiche 11.2 Geräte und Betriebsmittel	physischer und Umgebungsdatenschutz 11.1 Datenschutzrelevante Bereiche 11.2 Datenschutz von Betriebsmitteln
12. Betriebssicherheit	12.1 Betriebsabläufe und Verantwortlichkeiten 12.2 Schutz vor Schadsoftware 12.3 Datensicherung 12.4 Protokollierung und Überwachung etc.	12.1 Betriebsabläufe und Verantwortlichkeiten, Systemabnahme 12.2 Schutz vor Schadsoftware 12.3 Datensicherung 12.4 Protokollierung und Überwachung etc.

Entwicklung ISMS und DSMS

Hannover IT

Bereich	Übereinstimmung	ISMS	DSMS
Schutzziele	Vertraulichkeit, Integrität, Verfügbarkeit, Authentizität, Resilenz der Systeme (Belastbarkeit)	✔	✔
Datenklassifikation	Zuordnung personenbezogener Daten zur ISMS-Datenklassifizierung	✔	✔
Anwendung PDCA - Zyklus	Planen – Umsetzen – Kontrollieren - Verbessern	✔	✔
Risikobasiertes Vorgehen	Datendiebstahl, Datenverlust, Datenveröffentlichung, Datenverfälschung	✔ Institutions-werte	✔ Betroffene
Maßnahmenbereiche	Organisation, Prozesse, Technik, Prävention	✔	✔
In Teilen gleiche Maßnahmen	z.B. Prozess Schulungen/Unterweisungen, sicherere IT-Systeme, Zugriffsschutz, Datensicherung, Anwendungssicherheit, Informationspflege usw.	✔	✔

Datenschutz-und Informationssicherheits-Konzepte können in weiten Teilen gemeinsam entwickelt werden. Technisch-organisatorische Maßnahmen, Erklärung zur Anwendbarkeit können analog betrachtet werden.