SWISS INFOSEC

RVK-KOMPAKT
REVISION VDSZ

VERORDNUNG ÜBER DATENSCHUTZZERTIFIZIERUNGEN (VDSZ)

Dimitri Korostylev
Rechtsanwalt, Head of Legal & Data Privacy Consulting
Mitglied der Geschäftsleitung

Dimitri Korostylev

DIMITRI KOROSTYLEV

- Rechtsanwalt
- Head of Legal & Data Privacy Consulting
- Mitglied der Geschäftsleitung
- Fellow of Information Privacy (FIP)
- Artificial Intelligence Governance Professional (AIGP)
- CIPM, CIPT, CIPP/E

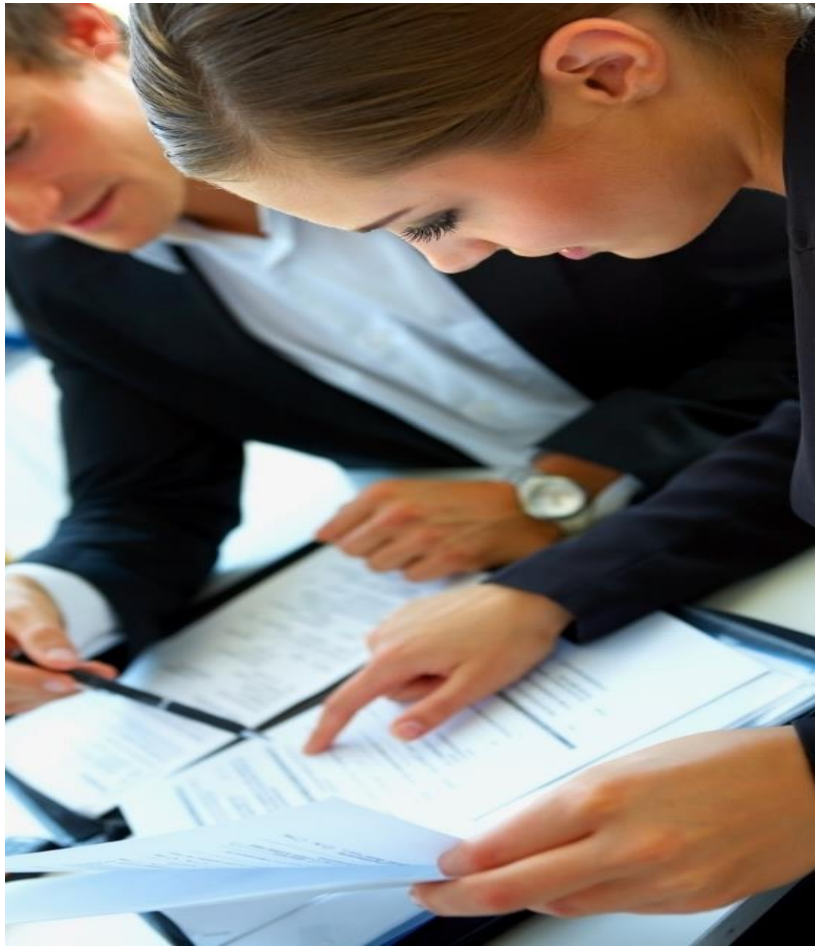
SPEZIALGEBIETE

- Legal & Compliance
- Datenschutz, KI, IT-Recht, Verträge
- Rechtsfragen zur Digitalisierung
- Externer Datenschutzbeauftragter
- Datenschutzberater

BESTEHENDES ZERTIFIZIERTES DSMS NACH VDSZ:2014?

- Die Überarbeitung der VDSZ erfolgt im Rahmen der **Totalrevision des Datenschutzgesetzes (DSG),** um technologische Entwicklungen und das weiterentwickelte europäische Recht zu berücksichtigen.
- Bestehende Zertifikate nach **VDSZ:2014** sind bis zum **31.08.2025** gültig.
- Neue Norm **VDSZ:2023**: Enthält auch die Anforderungen der **ISO/IEC 27001:2022.**

→**Wichtig: Frühzeitige Planung der Anpassung und Durchführung der Transitions-Audits. Spätestens bis Juli 2025 müssen Transitions-Audits erfolgreich durchgeführt werden**



DATENSCHUTZZERTIFIZIERUNG NACH VDSZ

Wieso ein DSMS?

- Verbesserung der Datensicherheit
- Qualitätsnachweis
- Verpflichtung der Mitarbeitenden und Partner zum Datenschutz
- ggfs. ein Verkaufsargument
- Bewertung der Systeme, Verfahren und Organisation des Datenschutzes durch anerkannte unabhängige Zertifizierungsstellen
- Mit Zertifizierung **keine Datenschutz-Folgenabschätzung (DSFA)** gemäss Artikel 22 DSG erforderlich, wenn die Zertifizierung die Bearbeitung, die im Rahmen der DSFA zu prüfen wäre, einschliesst.
- **Sonderfall gesetzlicher Zwang zur Zertifizierung:**
  Die Datenannahmestellen der Krankenversicherer benötigen ein DSMS-Zertifikat nach VDSZ

HAUPTÄNDERUNGEN DER VDSZ

- **Terminologie und Präzision**
  - Neue Begriffe eingeführt, z. B. "Managementsysteme" statt "Systeme", um Konformität mit ISO-Normen sicherzustellen.
  - EDÖB ersetzt den Begriff der oder des Beauftragten.

- **Erweiterung der Zertifizierungsgegenstände**
  - Neben Managementsystemen und Produkten sind nun auch **Dienstleistungen** und **Prozesse** zertifizierbar (z. B. Cloud-Dienste, Datenverarbeitungsprozesse).
  - Aufnahme von Datenschutzbearbeitungen als potenzielles Zertifizierungsobjekt.

HAUPTÄNDERUNGEN DER VDSZ

- **Anforderungen an Zertifizierungsprogramme**
  - Begriffe wie "Kontrollprogramm" durch "Zertifizierungsprogramm" ersetzt, um Konsistenz mit ISO-Normen sicherzustellen.
  - Einführung von Faktoren zur Festlegung von Prüfkriterien.
  - Berücksichtigung der Art der bearbeiteten Daten.
  - Betrachtung technischer Infrastruktur und organisatorischer Massnahmen.

- **Anpassungen für Konformität mit ISO-Normen**
  - Integration der ISO/IEC 27001
  - Einführung von Mindestanforderungen für das Personal von Zertifizierungsstellen.

HAUPTÄNDERUNGEN DER VDSZ

- **Änderungen in der Gültigkeit und Verfahren**
  - Dauer der Zertifizierung: Vereinheitlichung auf 3 Jahre für alle Zertifizierungsgegenstände.
  - Ausnahme von der Datenschutz-Folgenabschätzung: Verantwortliche können bei zertifizierten Systemen, Produkten oder Dienstleistungen auf die Erstellung verzichten.

- **Harmonisierung mit europäischem Recht**
  - Aufnahme datenschutzrechtlicher Prinzipien wie Verhältnismässigkeit und Zweckbindung.
  - Förderung der Anerkennung schweizerischer Zertifizierungen durch europäische Datenschutzbehörden.

ZERTIFIZIERUNGSVERFAHREN

Art. 13 DSG: Die Hersteller von Datenbearbeitungssystemen oder programmen sowie die Verantwortlichen und Auftragsbearbeiter können ihre Systeme, Produkte und Dienstleistungen einer Bewertung durch anerkannte unabhängige Zertifizierungsstellen unterziehen.

Art. 4 VDSZ: Zertifizierbar sind:

1. **Managementsysteme** (Gesamtheit des Systems, einzelne Teile der Organisation oder einzelne, abgrenzbare Verfahren)**,**
2. **Produkte, Dienstleistungen und Prozesse**
   a. Produkte, die hauptsächlich der Bearbeitung von Personendaten dienen oder bei deren Benutzung Personendaten erzeugt werden;
   b. Dienstleistungen oder Prozesse, die hauptsächlich der Bearbeitung von Personendaten dienen oder die Personendaten erzeugen.

ZERTIFIZIERUNGSVERFAHREN

Erteilung und Gültigkeit der Datenschutzzertifizierung

Art. 8 VDSZ: Die Zertifizierung wird erteilt, wenn das Zertifizierungsverfahren zum Ergebnis führt, dass die datenschutzrechtlichen Anforderungen erfüllt werden. Die Zertifizierung kann mit Auflagen verbunden werden.

Die Zertifizierung ist drei Jahren gültig. Die Zertifizierungsstelle muss jährlich prüfen, ob die Voraussetzungen weiterhin erfüllt sind.

Sistierung und Entzug der Zertifizierung

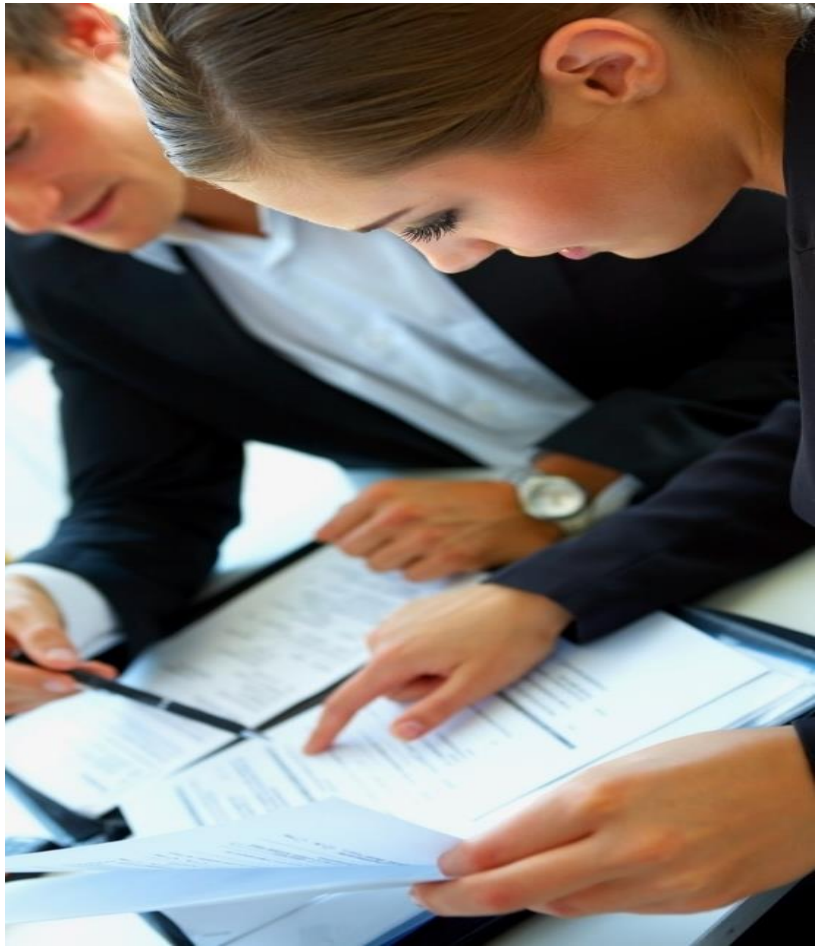
Art. 11 VDSZ: Die Zertifizierungsstelle kann eine Zertifizierung sistieren oder entziehen, namentlich wenn sie im Rahmen der Überprüfung schwere Mängel feststellt. Ein schwerer Mangel liegt insbesondere vor, wenn:

- wesentliche Voraussetzungen der Datenschutzzertifizierung nicht mehr erfüllt sind
- eine Zertifizierung irreführend oder missbräuchlich verwendet wird

ZERTIFIZIERUNGSVERFAHREN VON MANAGEMENTSYSTEMEN

Art. 6 VDSZ: Gegenstand der Prüfung von Managementsystemen durch die Zertifizierungsstellen umfasst namentlich:

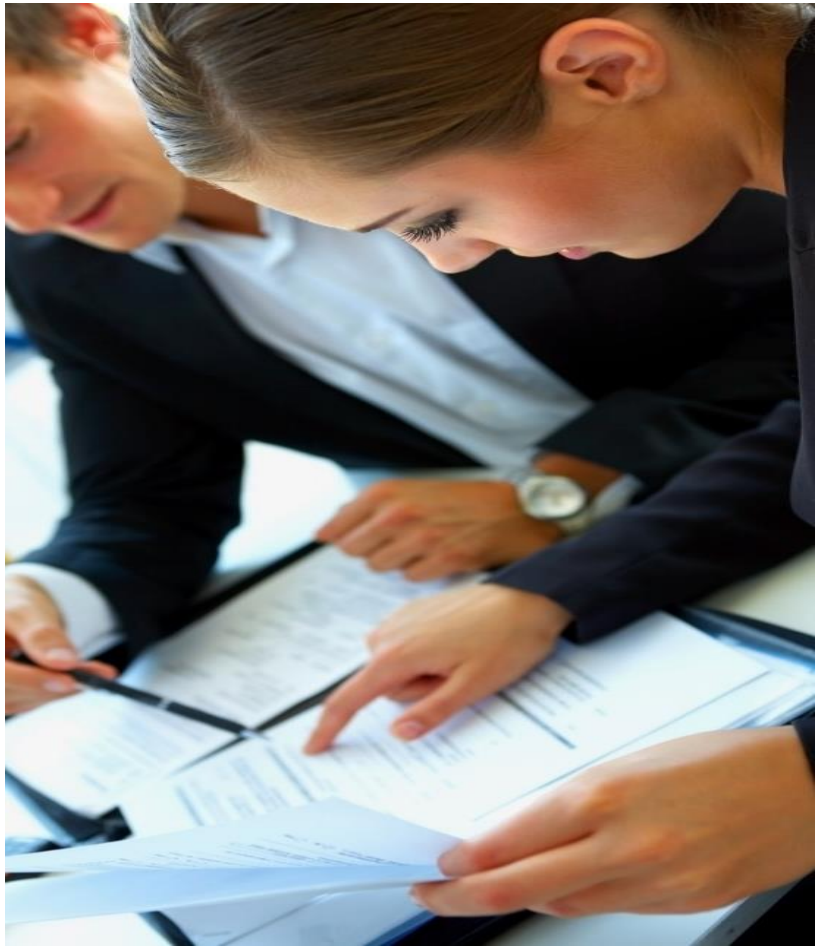
a. die Datenschutzpolitik
b. die Dokumentation von Zielen, Risiken und Massnahmen zur Gewährleistung des Datenschutzes und der Datensicherheit
c. die organisatorischen und technischen Vorkehrungen zur Umsetzung der festgelegten Ziele und Massnahmen, insbesondere die Vorkehrungen zur Behebung von Mängeln



ZERTIFIZIERUNGSVERFAHREN VON MANAGEMENTSYSTEMEN

Richtlinien über die Mindestanforderungen an ein Managementsystem:

- Die in der **Norm ISO/IEC 27001** aufgeführten Mindestanforderungen



ALLGEMEINE ANFORDERUNGEN NACH ISO/IEC 27001

- **Managementgremium**
  - Bspw. GL verstärkt um CISO, DSB
  - Steuert, entscheidet, koordiniert
  - Übernahme Restrisiken
- **Regelmässige Überprüfung der Risikosituation**
  - Risiken identifizieren, bewerten
  - Massnahmen evaluieren
  - Nachvollziehbare Risikobehandlung bzw. Risikoumgang
- **Dokumentenlenkungssystem**
- **Lenkung der Nachweise**

ALLGEMEINE ANFORDERUNGEN NACH ISO/IEC 27001

- **Klassifizierung**
- **Inventarisierung**
- Gelebtes **Owner-Konzept**
- **Incident Management**
- Darstellung **Sicherheitsbedarfs und Realität**
- Nachvollziehbare und begründete **Abweichungen** von ISO 27002

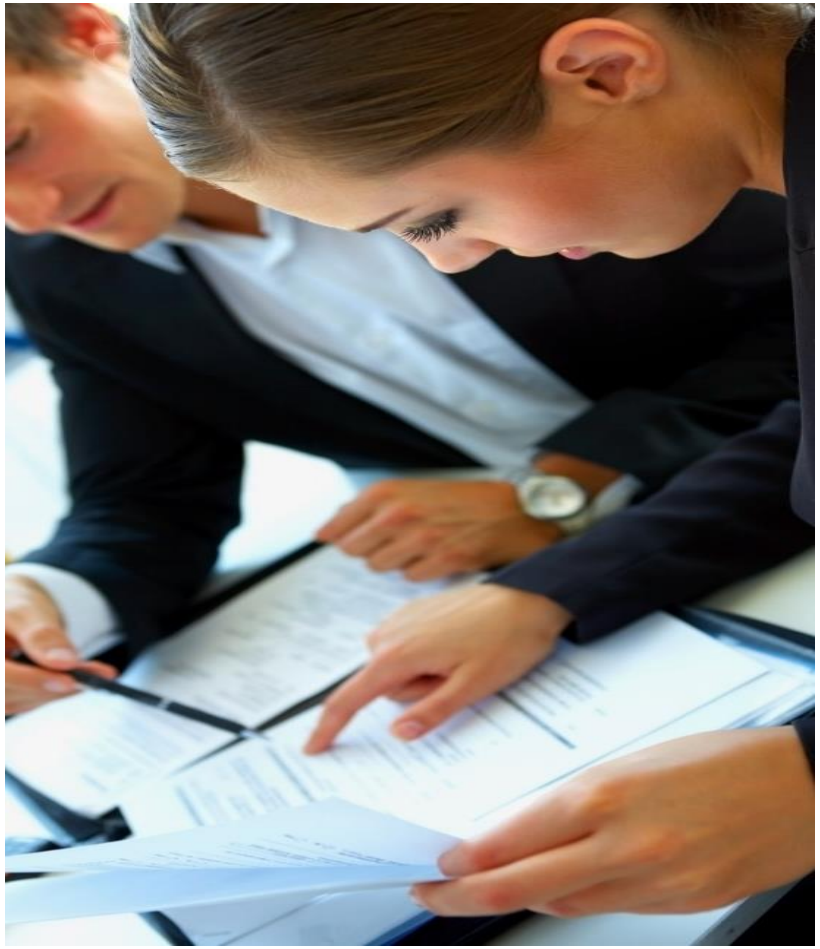
ALLGEMEINE ANFORDERUNGEN NACH ISO/IEC 27001

- **Grundregeln** in Form eines Vorgabedokuments "Sicherheitspolitik"
- **Bekannte und gelebte Regeln und Massnahmen**
- **Information und Ausbildung** der beteiligten Personen
- Implementierung der Sicherheit in **Verfahren und Prozesse**
- **Sicherheit im Betrieb**:
  - Software-Freigabe
  - Installationen
  - Change Management
  - Projektführung
- **Überprüfungshandlungen** (Audits etc.)
- Nachvollziehbare **kontinuierliche Verbesserung**

ZERTIFIZIERUNGSVERFAHREN VON MANAGEMENTSYSTEMEN

Richtlinien über die Mindestanforderungen an ein Managementsystem:

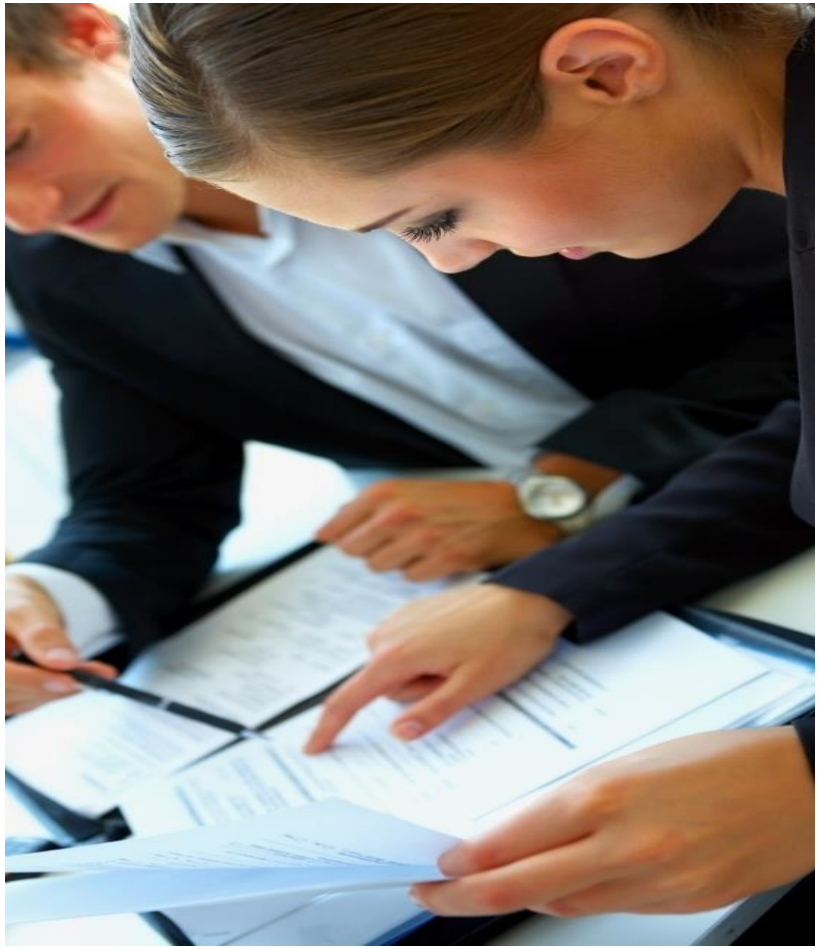
- Zusätzlich die folgenden datenschutzrechtlichen Aspekte berücksichtigen:
  - **Rechtmässigkeit** (Art. 6 Abs. 1 DSG):
    - Rechtfertigungsgründe (Art. 31 DSG),
    - Gesetzliche Grundlage (Art. 34 und 36 DSG),
    - Datenbearbeitung durch Auftragsbearbeiter (Art. 9 DSG i.V.m. Art. 7 DSV);



ZERTIFIZIERUNGSVERFAHREN VON MANAGEMENTSYSTEMEN

Richtlinien über die Mindestanforderungen an ein Managementsystem:

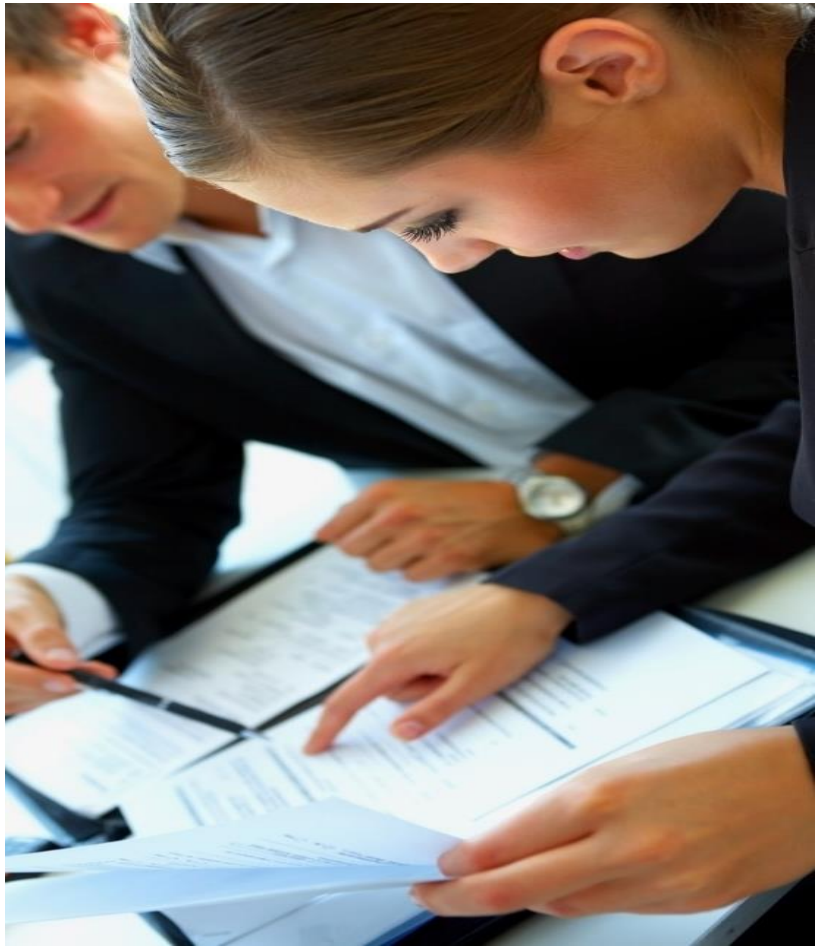
- Zusätzlich die folgenden datenschutzrechtlichen Aspekte berücksichtigen:
  - **Transparenz**:
    - Treu und Glauben (Art. 6 Abs. 2 DSG),
    - Erkennbarkeit (Art. 6 Abs. 3 DSG),
    - Informationspflicht (Art. 19 – 21 DSG i.V.m. Art. 13 DSV),
    - Verzeichnis der Bearbeitungstätigkeiten (Art. 12 DSG i.V.m. Art. 24 DSV),
    - Datenschutz-Folgenabschätzung (Art. 22 DSG i.V.m. Art. 14 DSV),
    - Meldung von Verletzungen der Datensicherheit (Art. 24 DSG i.V.m. Art. 15 DSV);



ZERTIFIZIERUNGSVERFAHREN VON MANAGEMENTSYSTEMEN

Richtlinien über die Mindestanforderungen an ein Managementsystem:

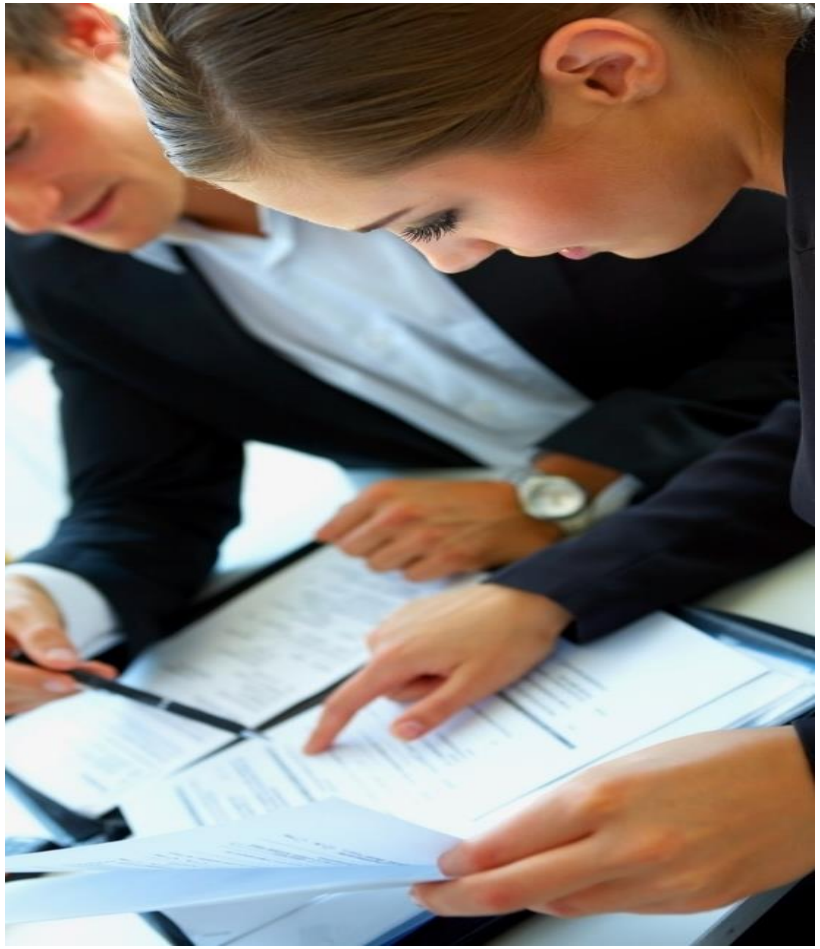
- Zusätzlich die folgenden datenschutzrechtlichen Aspekte berücksichtigen:
  - **Verhältnismässigkeit**:
    - Verhältnismässige Bearbeitung (Art. 6 Abs. 2 DSG),
    - Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen (Art. 7 DSG);
  - **Zweckbindung** (Art. 6 Abs. 3 DSG);
  - **Datenrichtigkeit** (Art. 6 Abs. 5 DSG);
  - **Bekanntgabe von Personendaten ins Ausland** (Art. 16 DSG i.V.m. Art. 8 – 12 DSV);
  - **Datensicherheit** (Art. 8 DSG i.V.m. Art. 1 – 6 DSV);



ZERTIFIZIERUNGSVERFAHREN VON MANAGEMENTSYSTEMEN

Richtlinien über die Mindestanforderungen an ein Managementsystem:

- Zusätzlich die folgenden datenschutzrechtlichen Aspekte berücksichtigen:
  - **Rechte und Verfahren**:
    - Auskunftsrecht über eine Person betreffende Daten (Art. 25 DSG i.V.m. Art. 26, 27 DSG, Art. 16 – 19 DSV),
    - Recht auf Datenherausgabe oder -übertragung (Art. 28 DSG i.V.m. Art. 29 DSG, Art. 20 – 22 DSV),
    - Rechtsansprüche und Verfahren (Art. 32 und 41f. DSG).



ZERTIFIZIERUNGSVERFAHREN VON PRODUKTEN, DIENSTLEISTUNGEN UND PROZESSEN

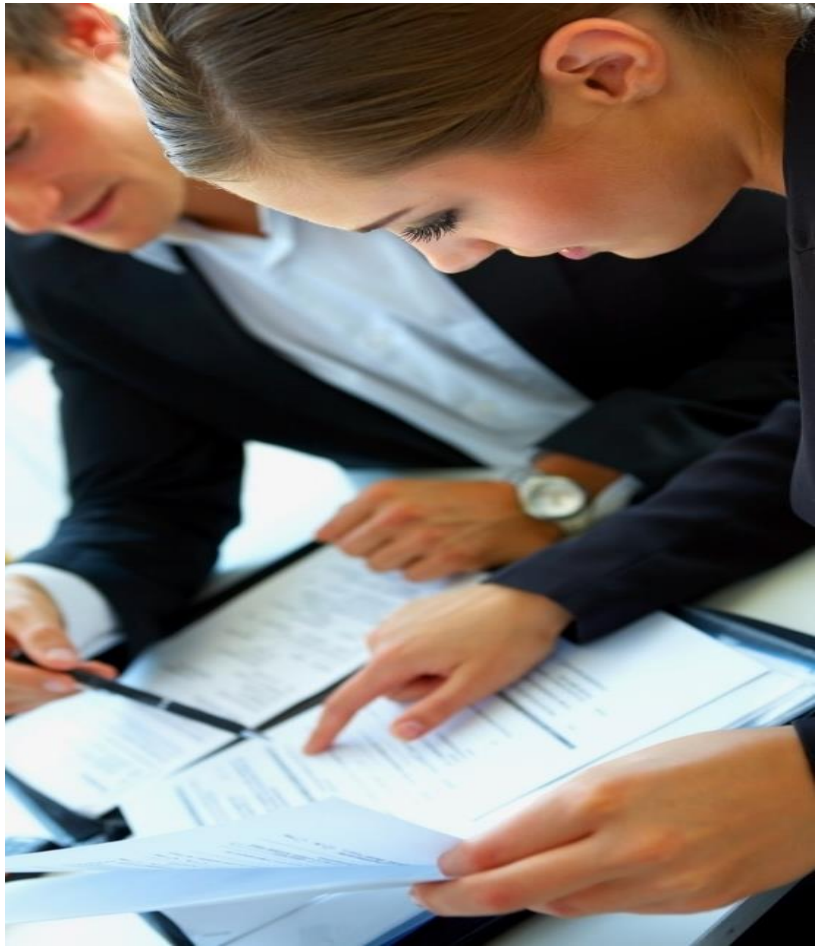
Gegenstand der Prüfung ist insbesondere die Gewährleistung:

a. der **Vertraulichkeit, Integrität, Verfügbarkeit** und **Nachvollziehbarkeit** der bearbeiteten Personendaten;

b. der **Vermeidung der Bearbeitung von Personendaten**, die im Hinblick auf den Verwendungszweck des Produkts, der Dienstleistung oder des Prozesses **nicht erforderlich** sind;

c. der **Transparenz** der Bearbeitung von Personendaten;

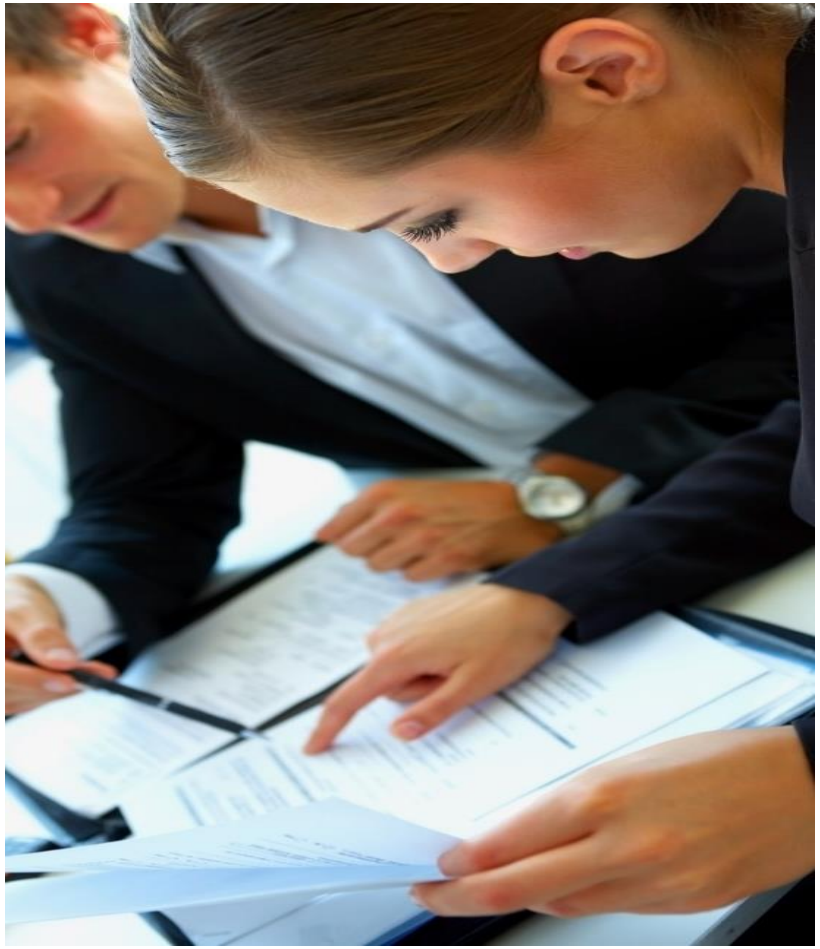
d. von **technischen Massnahmen** zur Unterstützung der Anwenderin oder des Anwenders bei der Einhaltung weiterer Datenschutzgrundsätze und datenschutzrechtlicher Pflichten, insbesondere der Rechte der betroffenen Personen.



ZERTIFIZIERUNGSVERFAHREN VON PRODUKTEN, DIENSTLEISTUNGEN UND PROZESSEN

Richtlinien über die die weiteren datenschutzrechtlichen Kriterien für die Prüfung zu den Anforderungen an die Zertifizierung von Produkten, Dienstleistungen und Prozessen

→ Identische Massnahmen wie in den Richtlinien über die Mindestanforderungen an ein Managementsystem beschrieben.



DATENSCHUTZ-ZERTIFIZIERUNG NACH VDSZ UND DEREN VORTEIL

- Zertifizierung von Datenbearbeitungssystemen oder –programmen durch eine unabhängige Zertifizierungsstelle
- Datenschutz-Zertifizierungen nach Art. 13 VDSZ berücksichtigt ISO-Normen (ISO 27001 + ISO 27002)
- Erfüllung der Mindestanforderungen von ISO 27001, ergänzt mit den Massnahmen aus ISO 27002
- „Datenschutz-Gütesiegel“
- Zertifizierte Verantwortliche sind gemäss Artikel 22 Abs. 5 Alt. 1 DSG von einer Datenschutz-Folgenabschätzung befreit.

HABEN SIE NOCH FRAGEN?