

Sorgfaltspflichten der Führungskräfte in der Verwaltung im Umgang mit datenschutzrelevanten Informationen

**Lukas Fässler
Rechtsanwalt & Informatikexperte**



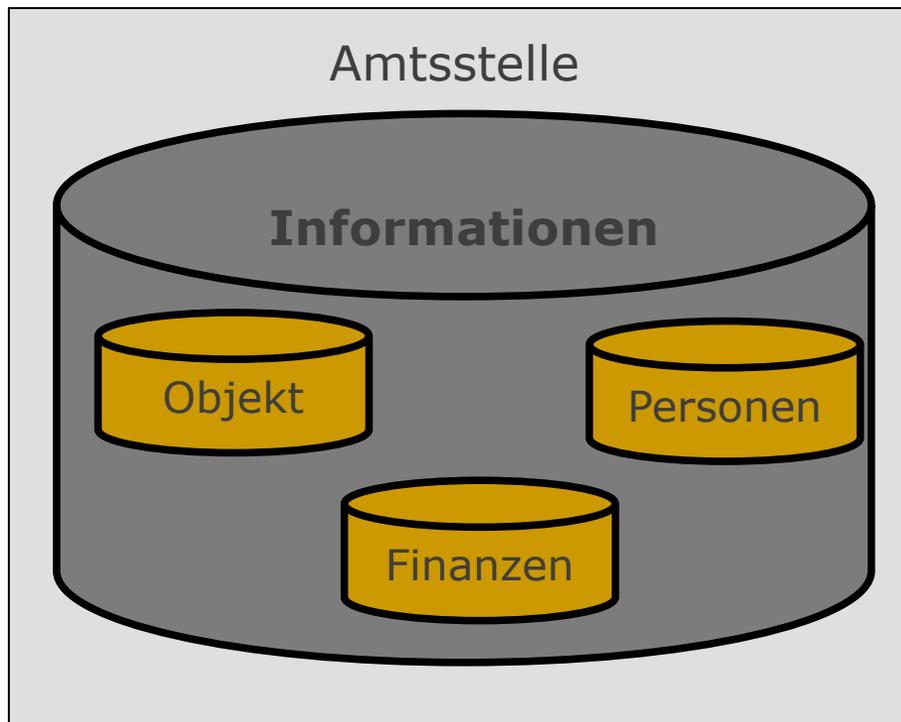
Inhaltsverzeichnis

- 1. Informationsmanagement in der Verwaltung**
 2. Verantwortliches Organ
 3. Sorgfaltspflichten – Einflussfaktoren der Verantwortung
 4. Abgrenzung zum Service-Provider KSD
 5. Massnahmen
 6. Schlussfolgerungen
-

Informations-Management in der Verwaltung



Geschäftsrelevante Informationen



**Verordnung
über das Staatsarchiv und die Archivierung
der Verwaltungsakten
(Archivverordnung)**

vom 8. Februar 1994

§ 2

Als Verwaltungsakten gelten alle Schrift-, Bild- und Tonträger sowie elektronischen und anderen Informationsträger, die aus der Behörden- und Verwaltungstätigkeit hervorgegangen sind oder mit ihr im Zusammenhang stehen.

Informations-Management in der Verwaltung



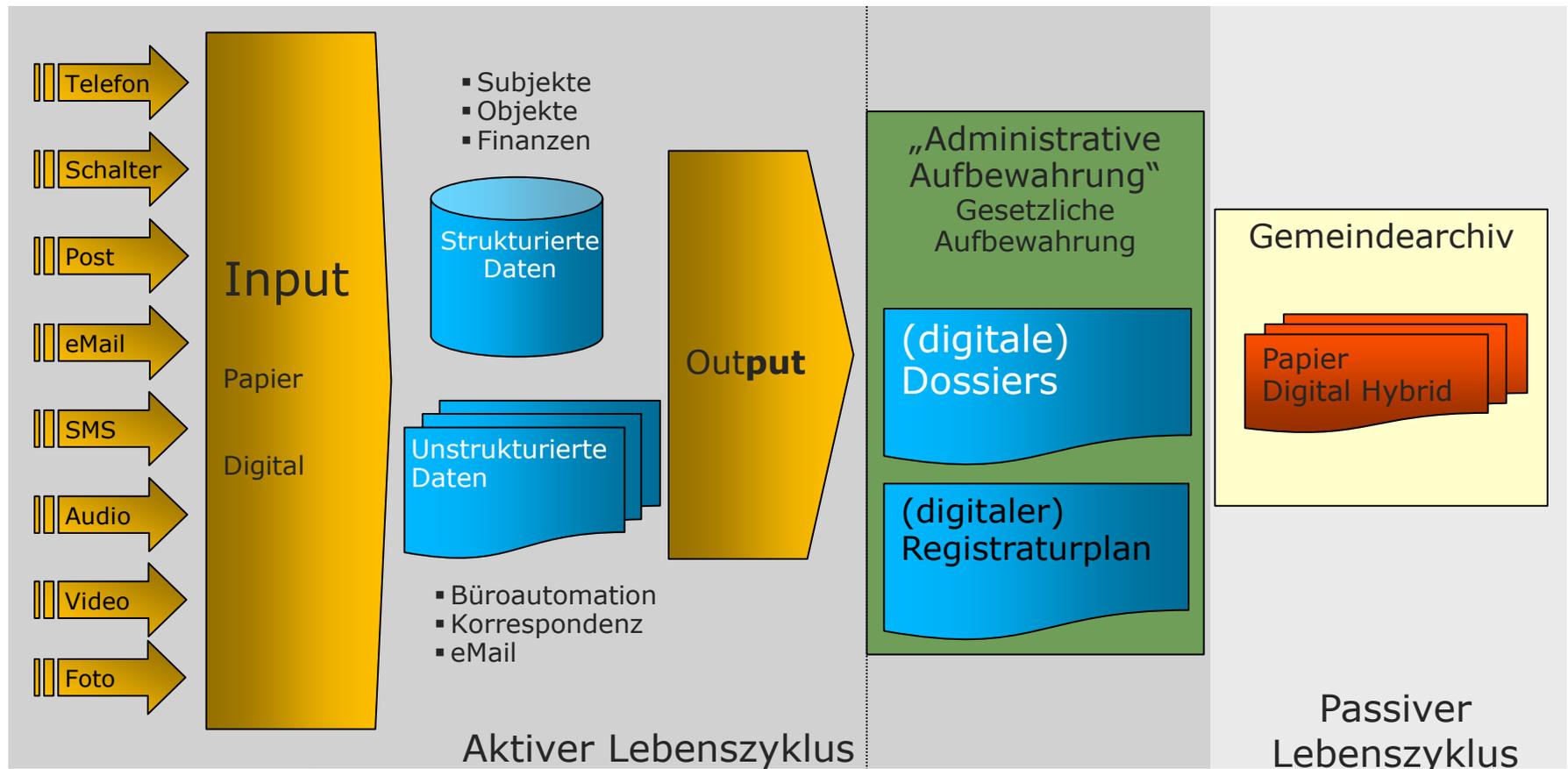
Herausforderung Hybrides Informationsmanagement



Informations-Management in der Verwaltung



Lebenszyklus geschäftsrelevanter Informationen



**Reglement
über den Schutz und die Sicherung von Daten
bei der «KSD Kanton und Stadt Schaffhausen
Datenverarbeitung»
(Datenschutzreglement)**

vom 22. April 1980

Der Regierungsrat des Kantons Schaffhausen

3.

¹ Daten dürfen nur erfasst und gespeichert werden, soweit dies für die Erfüllung der Aufgaben der Verwaltung nötig ist.



Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz)

vom 7. März 1994

Art. 4

¹ Personendaten dürfen bearbeitet werden, wenn eine gesetzliche Grundlage dafür besteht.



Gesetz über den Rechtsschutz in Verwaltungssachen (Verwaltungsrechtspflegegesetz)¹⁾

vom 20. September 1971

Art. 6

Die Beteiligten haben Anspruch auf Einsicht in die Akten, soweit nicht wichtige öffentliche oder schutzwürdige private Interessen entgegenstehen.



Inhaltsverzeichnis

1. Informationsmanagement in der Verwaltung
 - 2. Verantwortliches Organ**
 3. Sorgfaltspflichten – Einflussfaktoren der Verantwortung
 4. Abgrenzung zum Service-Provider KSD
 5. Massnahmen
 6. Schlussfolgerungen
-



Verantwortliches Organ

172.100

Gesetz über die Organisation der Regierungs- und Verwaltungstätigkeit (Organisationsgesetz)

vom 18. Februar 1985

Art. 4

¹ Der Regierungsrat sorgt für eine rechtmässige, leistungsfähige und sparsame Verwaltung und bestimmt deren zweckmässige Organisation.

² Er sorgt für die Koordination auf allen Ebenen der Verwaltung sowie zwischen dieser und andern Trägern von Verwaltungsaufgaben.

³ Er beaufsichtigt regelmässig und systematisch die Verwaltung.

Verantwortliches Organ

172.100

Gesetz über die Organisation der Regierungs- und Verwaltungstätigkeit (Organisationsgesetz)

vom 18. Februar 1985

Art. 34

Der Departementsvorsteher ist dafür verantwortlich, dass das Departement und die ihm unterstellten Dienststellen und unselbständigen Anstalten nach den Grundsätzen einer rechtmässigen, leistungsfähigen und sparsamen Verwaltung organisiert und geleitet werden.

Art. 35

Der Departementsvorsteher nimmt seine Leitungsaufgabe wahr, indem er insbesondere

- e) die Departementsorganisation periodisch auf ihre Zweckmässigkeit überprüft und Massnahmen zu ihrer Anpassung an veränderte Erfordernisse in die Wege leitet;
-

Verantwortliches Organ

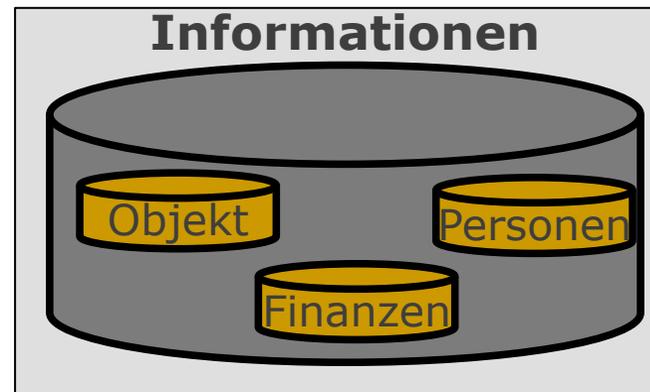
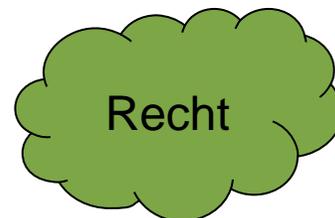
174.102

**Reglement
über den Schutz und die Sicherung von Daten
bei der «KSD Kanton und Stadt Schaffhausen
Datenverarbeitung»
(Datenschutzreglement)**

- Verantwortliches Organ
- Inhaber der Datensammlung
- Datenherr

4.

¹ Die **Amtsstelle**, die bei der KSD Daten speichern lässt, ist allein berechtigt, über diese zu verfügen.



Verantwortliches Organ

174.102

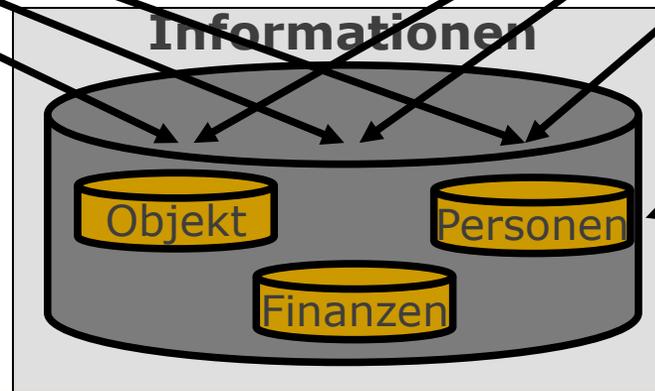
**Reglement
über den Schutz und die Sicherung von Daten
bei der «KSD Kanton und Stadt Schaffhausen
Datenverarbeitung»
(Datenschutzreglement)**

- Verantwortliches Organ
- Inhaber der Datensammlung
- Datenherr

Pflichten

Amtsgeheimnis

Datenschutz





Inhaltsverzeichnis

1. Informationsmanagement in der Verwaltung
 2. Verantwortliches Organ
 - 3. Sorgfaltspflichten – Einflussfaktoren der Verantwortung**
 4. Abgrenzung zum Service-Provider KSD
 5. Massnahmen
 6. Schlussfolgerungen
-

Sorgfaltspflichten

172.301

Verordnung
über das Staatsarchiv und die Archivierung
der Verwaltungsakten
(Archivverordnung)

vom 8. Februar 1994

Amtsstelle

- Verantwortliches Organ
- Inhaber der Datensammlung
- Datenherr

§ 3

¹ Die Dienststellen und Anstalten der kantonalen Verwaltung sammeln die im Rahmen ihrer Tätigkeit entstehenden Verwaltungsakten in einer Registratur.

³ Die Registraturen der Dienststellen und Anstalten haben sich auf die Akten zu beschränken, welche unmittelbar aus ihrer Tätigkeit anfallen oder für die Erfüllung ihrer Aufgaben erforderlich sind. Für Personendaten bleiben die Bestimmungen des Datenschutzrechts vorbehalten.

Registraturpflicht

§ 6

¹ Die Akten werden in den Registraturen der Verwaltungsstellen und Anstalten so lange aufbewahrt, als sie für die laufende Verwaltungstätigkeit benötigt werden, in der Regel jedoch mindestens zehn Jahre .

Aufbewahrungspflicht



Sorgfaltspflichten

174.100

Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz)

vom 7. März 1994

Amtsstelle

- Verantwortliches Organ
- Inhaber der Datensammlung
- Datenherr

Art. 6

¹ Für den Datenschutz ist jenes Organ verantwortlich, das die Personendaten bearbeitet oder bearbeiten lässt.

Schutzpflicht 1

Art. 14

Personendaten sind durch angemessene technische und organisatorische Massnahmen vor Verlust, Entwendung und unbefugtem Bearbeiten zu schützen.

Schutzpflicht 2



Sorgfaltspflichten

174.100

Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz)

vom 7. März 1994

Amtsstelle

- Verantwortliches Organ
- Inhaber der Datensammlung
- Datenherr

Art. 16a¹⁰⁾

¹ Ein automatisiertes Verfahren zur Verarbeitung von personenbezogenen Daten, das mit besonderen Risiken für die Rechte und Freiheit der betroffenen Personen verbunden sein kann, insbesondere auf Grund der Art und Zweckbestimmung, darf erst eingesetzt oder wesentlich geändert werden, wenn sichergestellt ist, dass diese Risiken nicht bestehen oder durch technische oder organisatorische Massnahmen verhindert werden.

Schutzpflicht 3



Sorgfaltspflichten

174.100

**Gesetz
über den Schutz von Personendaten
(Kantonales Datenschutzgesetz)**

vom 7. März 1994

Amtsstelle

- Verantwortliches Organ
- Inhaber der Datensammlung
- Datenherr

Art. 13

¹ Beauftragt das verantwortliche Organ ein anderes öffentliches Organ oder Dritte mit dem Bearbeiten von Personendaten, ist der Datenschutz durch Vereinbarung, Auflagen oder auf andere Weise sicherzustellen.

Drittvereinbarungspflicht

Aufgaben kann man delegieren, VERANTWORTUNG NIE



Sorgfaltspflichten

**Reglement
über den Schutz und die Sicherung von Daten
bei der «KSD Kanton und Stadt Schaffhausen
Datenverarbeitung»
(Datenschutzreglement)**

174.102

Amtsstelle

- Verantwortliches Organ
- Inhaber der Datensammlung
- Datenherr

4.

¹ Die Amtsstelle, die bei der KSD Daten speichern lässt, ist allein berechtigt, über diese zu verfügen.

² Die Zugriffsberechtigung wird für jede Datei, bei integrierten Dateien für jeden Teilbereich, festgelegt.

Zugriffsrechte
festlegen

Sorgfaltspflichten



174.102

Amtsstelle

- Verantwortliches Organ
- Inhaber der Datensammlung
- Datenherr

**Reglement
über den Schutz und die Sicherung von Daten
bei der «KSD Kanton und Stadt Schaffhausen
Datenverarbeitung»
(Datenschutzreglement)**

8.

¹ Innerhalb der kantonalen und der städtischen Verwaltung können Daten mit Zustimmung der verfügungsberechtigten Amtsstelle weitergegeben werden, wenn sie vom Empfänger zur Erfüllung seiner öffentlichen Aufgaben benötigt werden. Das gleiche gilt auch für andere Gemeinden, Kantone und den Bund.

² Die Weitergabe von Daten an Dritte bedarf der Bewilligung der zuständigen Direktion ¹⁾ des Regierungsrates bzw. des zuständigen Referates des Stadtrates.

Prüfungspflicht vor
Weitergabe innerhalb
der Verwaltung

Bewilligungspflicht
vor Weitergabe
an Dritte



Inhaltsverzeichnis

1. Informationsmanagement in der Verwaltung
 2. Verantwortliches Organ
 3. Sorgfaltspflichten – Einflussfaktoren der Verantwortung
 - 4. Abgrenzung zum Service-Provider KSD**
 5. Massnahmen
 6. Schlussfolgerungen
-



Abgrenzung zur KSD

172.601

Vereinbarung über die E-Government- und Informatikstrategie sowie den gemeinsamen Informatikbetrieb

vom 9. November 2010 / 16. November 2010

Art. 6

¹ Unter dem Namen KSD betreiben der Kanton Schaffhausen und die Stadt Schaffhausen einen gemeinsamen Informatik-Betrieb.

² Zweck des Betriebes ist es, die für die Kantons- und die Stadtverwaltung erforderlichen Informatik-Dienstleistungen kostengünstig und sicher zu erbringen.

Verwaltungsinterne Service-Dienstleisterin

Abgrenzung zur KSD

174.102

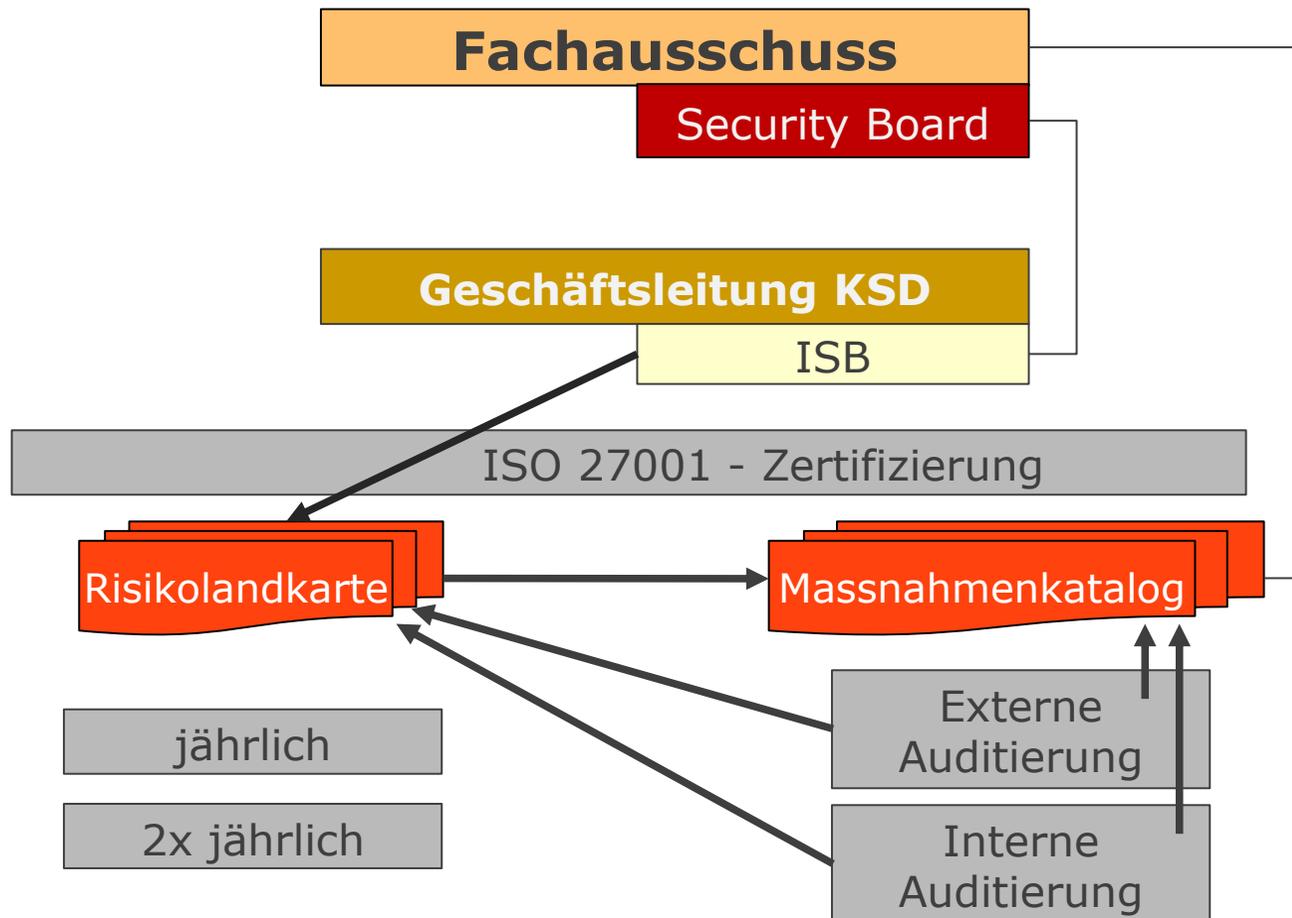
**Reglement
über den Schutz und die Sicherung von Daten
bei der «KSD Kanton und Stadt Schaffhausen
Datenverarbeitung»
(Datenschutzreglement)**

³ Die KSD ist in technischer Hinsicht für den Bestand und die Verwendung der ihr anvertrauten Daten verantwortlich.

Technische Betriebs-
verantwortung

- Verantwortliches Organ
 - Inhaber der Datensammlung
 - Datenherr

Abgrenzung zur KSD



Abgrenzung zur KSD

Verordnung über den Schutz von Personendaten (Kantonale Datenschutzverordnung)

vom 28. Februar 1995

§ 3

¹ Das verantwortliche Organ hat eine angemessene Datensicherung zu gewährleisten und Personendaten insbesondere vor folgenden Gefahren zu schützen:

- a) unbefugte oder zufällige Vernichtung;
- b) zufälliger Verlust;
- c) technische Fehler;
- d) Fälschung, Diebstahl oder widerrechtliche Verwendung;
- e) unbefugtes Ändern, Kopieren, Zugreifen oder andere unbefugte Bearbeitungen.

² Die technischen und organisatorischen Massnahmen müssen verhältnismässig sein und periodisch überprüft werden.

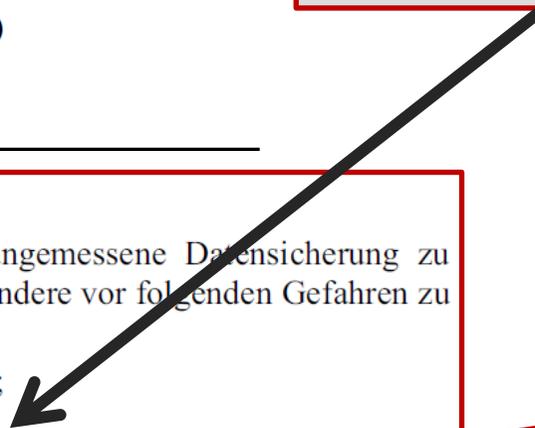
174.101

Amtsstelle

- Verantwortliches Organ
- Inhaber der Datensammlung
- Datenherr

KSD

Technische Betriebssicherheit
Datensicherung



Abgrenzung zur KSD

- 136 Anträge für Abweichungen von den ISMS¹ – Sicherheitsanforderungen der KSD sind zuviel
- Beschaffung von Fachapplikationen müssen rechtzeitig auf Sicherheits- und Datenschutz-Vorgaben ausgerichtet werden (Pflichtenheft)
- Einbezug des ISB der KSD ist zeitnah zu planen
- Aufschalten von Informationen im Internet:
 - Clearing- und Freigabeprozess bei der Amtsstelle

¹ ISMS: Information Security Management System



Inhaltsverzeichnis

1. Informationsmanagement in der Verwaltung
 2. Verantwortliches Organ
 3. Sorgfaltspflichten – Einflussfaktoren der Verantwortung
 4. Abgrenzung zum Service-Provider KSD
 - 5. Massnahmen**
 6. Schlussfolgerungen
-

Massnahmen - Verantwortung



- Umsetzung aller Sorgfaltspflichten gemäss Ziffer 3 oben
- Periodische Überprüfung der Zugriffsberechtigungen
- Periodische Überprüfung der Risikobewertungen
- Beantragen von zusätzlichen Schutzmassnahmen bei hochsensiblen Daten (Datenklau verhindern)
- Periodische Sensibilisierung der Mitarbeitenden (Datenschutz / Datensicherheit)

▪ Verantwortliches Organ
▪ Inhaber der Datensammlung
▪ Datenherr

Massnahmen - Verantwortung

170.300



Gesetz über die Haftung des Staates und der Gemeinden sowie ihrer Behördemitglieder und Arbeitnehmer (Haftungsgesetz)

vom 23. September 1985

Art. 3

¹ Der Staat haftet für den Schaden, den ein Arbeitnehmer in Ausübung amtlicher Verrichtung einem Dritten widerrechtlich zufügt; dem Geschädigten steht gegen den Arbeitnehmer kein Anspruch zu.

Art. 5a ¹⁰⁾

Wer in seiner Persönlichkeit widerrechtlich verletzt wird, hat Anspruch auf Feststellung der Verletzung, auf Schadenersatz und, sofern die Schwere der Verletzung es rechtfertigt und diese nicht anders wieder gutgemacht worden ist, auch auf Genugtuung.

Massnahmen - Verantwortung

170.300



Gesetz über die Haftung des Staates und der Gemeinden sowie ihrer Behördemitglieder und Arbeitnehmer (Haftungsgesetz)

vom 23. September 1985

Art. 8

¹ Der Arbeitnehmer haftet dem Staat für den Schaden, den er ihm durch vorsätzliche oder grobfahrlässige Verletzung seiner Dienstpflichten zufügt.

Art. 9

¹ Hat der Staat einem Geschädigten aufgrund dieses oder eines anderen Gesetzes Ersatz leisten müssen, so nimmt er ganz oder teilweise Rückgriff auf den Arbeitnehmer, der den Schaden vorsätzlich oder grobfahrlässig verschuldet hat.

Massnahmen - Verantwortung

174.100



Gesetz über den Schutz von Personendaten (Kantonales Datenschutzgesetz)

vom 7. März 1994

Art. 28

Wer als beauftragte Person für das Bearbeiten von Personendaten gemäss Art. 13 ohne anderslautende ausdrückliche Ermächtigung des auftraggebenden Organs Personendaten für sich oder andere verwendet oder anderen bekanntgibt, wird mit Busse⁸⁾ bestraft.



Massnahmen - Verantwortung

Schweizerisches Strafgesetzbuch

311.0

vom 21. Dezember 1937 (Stand am 1. Oktober 2012)

Art. 320

1. Wer ein Geheimnis offenbart, das ihm in seiner Eigenschaft als Mitglied einer Behörde oder als Beamter anvertraut worden ist, oder das er in seiner amtlichen oder dienstlichen Stellung wahrgenommen hat, wird mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.

Die Verletzung des Amtsgeheimnisses ist auch nach Beendigung des amtlichen oder dienstlichen Verhältnisses strafbar.

Art. 179^{novies 138}

Wer unbefugt besonders schützenswerte Personendaten oder Persönlichkeitsprofile, die nicht frei zugänglich sind, aus einer Datensammlung beschafft, wird auf Antrag mit Freiheitsstrafe bis zu drei Jahren oder Geldstrafe bestraft.



Inhaltsverzeichnis

1. Informationsmanagement in der Verwaltung
 2. Verantwortliches Organ
 3. Sorgfaltspflichten – Einflussfaktoren der Verantwortung
 4. Abgrenzung zum Service-Provider KSD
 5. Massnahmen
 - 6. Schlussfolgerungen**
-

Schlussfolgerungen

- Amtsstelle als Datenherr und verantwortliches Organ ist für Einhaltung **ALLER** Sorgfaltspflichten im Umgang mit Verwaltungsdaten verantwortlich
 - Primäre Verantwortung trifft den Amtsstellenleiter
 - Sekundäre Verantwortung trifft alle Angestellten, die Verwaltungsdaten bearbeiten
 - Alle organisatorischen und technischen Massnahmen zum Schutz der Verwaltungsdaten ergreifen
 - KSD ist Service-Dienstleisterin und (nur, aber immerhin) für die **technische Betriebs- und Datensicherheit** verantwortlich
-

Schlussfolgerungen

- Die KSD sorgt durch interne und externe Auditierung und Betrieb eines IS-Management-Systems für den notwendigen technischen **Grundschutz**, nimmt dadurch aber die Verantwortung der Vorgesetzten und Mitarbeiter bezüglich Datenschutz und Datensicherheit nicht ab
 - **Kommandieren, Kontrollieren und Korrigieren** der Vorgesetzten bezüglich Informations-Management (Schutz und Sicherheit) gehört zu den elementaren Sorgfaltspflichten eines Amtsvorstehers
 - Vorsätzliche oder grobfahrlässige Nichteinhaltung der Sorgfaltspflichten führt zu **zivilrechtlicher** (Regress des Staates) und **strafrechtlicher** (Offizialdelikt) **Verantwortung**
-



Danke für Ihre Aufmerksamkeit
