

Datensicherheitsverordnung

Weisung

zur Überprüfung der Datensicherheit

Inhaltsverzeichnis

1. Zweck.....	3
2. Zuständigkeiten.....	3
3. Vorgehensmethodik	3
4. Zusammenfassung.....	5
Anhang A: Sicherheitsanforderungen für Organe.....	5
Anhang A: Sicherheitsanforderungen für Organe.....	6
Anhang B: Sicherheitsanforderungen für Informatikleistungserbringer.....	8
Anhang C: Mustervorlage Massnahmenkatalog.....	10
Anhang D: Begriffserläuterungen der Datenschutzstelle	11

Ausgabe vom 16. Januar 2007

(mit Änderung betr. A11 und B13 gestützt auf den RRB vom 13. April 2010)

Autoren: Daniel Wachter
René Loepfe

Kontaktstelle: Amt für Informatik und Organisation (AIO)
Aabachstrasse 1
6300 Zug
Telefon 041 728 51 00
Email info.aio@fd.zg.ch

1. Zweck

Die vorliegende Weisung basiert auf dem Datenschutzgesetz (DSG) vom 28. September 2000¹ sowie der Datensicherheitsverordnung vom 16. Januar 2007 (DSV)². Sie zeigt auf, wie eine Überprüfung der Datensicherheit durchgeführt werden muss, um die gesetzlichen Anforderungen zu erfüllen.

2. Zuständigkeiten

Zu Beginn bestimmen die Organe die zuständigen Personen für folgende Aufgaben:

Überprüfung der Datensicherheit;
Erstellung der Massnahmenkataloge;
Bewilligung der beantragten Massnahmen;
Instruktion der Mitarbeitenden.

Die Datenschutzstelle berät die Organe in grundsätzlichen Fragen der Datensicherheit. Für spezifische informatiktechnische Fragen können sich kantonale Organe an das AIO bzw. gemeindliche Organe an ihren jeweiligen Informatikleistungserbringer wenden.

Die Organe überprüfen die Datensicherheit in denjenigen Bereichen, die sie selber beeinflussen können: Zutrittsschutz zu Büros, Zugriffsschutz von Fachanwendungen, Aufbewahrung und Entsorgung von Datenträgern etc.

Die Sicherstellung eines angemessenen Sicherheitsniveaus im Bereich Netzwerke, Server, Arbeitsplatzeinrichtungen sowie organübergreifender Fachanwendungen erfolgt durch die jeweiligen Informatikleistungserbringer. Sofern es sich bei den Informatikleistungserbringern um externe Dritte handelt, sind diese entsprechend vertraglich zu verpflichten.

3. Vorgehensmethodik

Die Überprüfung der Datensicherheit und die Erstellung der Massnahmenkataloge erfolgt in folgenden Schritten:

a) Ermitteln der Schutzobjekte

Zuerst werden die zu beurteilenden Schutzobjekte ermittelt. Diese umfassen alle im Register der Datensammlungen aufgeführten Personendatensammlungen, ferner kurzfristige Personendatensammlungen sowie einzelne, vom Geltungsbereich des DSG erfasste Personendaten.

Dabei kann es sich um Personendaten handeln, die mit elektronischen Mitteln und/oder manuell bearbeitet werden. Die ermittelten Schutzobjekte werden in einer Liste festgehalten. Besonders schützenswerte Daten im Sinne von § 2 Bst. b DSG werden speziell bezeichnet.

¹ DSG; BGS 157.1

² DSV; BGS 157.12

b) Überprüfen der Datensicherheit (§ 3 DSV)

In einem zweiten Schritt erfolgt die Überprüfung der Datensicherheit durch die Organe und ihre Informatikleistungserbringer anhand der Sicherheitsanforderungen in Anhang A und B. Diese Überprüfung dient dazu, die vorhandenen Personendaten gegen folgende Gefahren zu schützen:

- a) zufällige Bekanntgabe, Vernichtung oder Verlust;
- b) technische Fehler;
- c) unbefugte Kenntnisnahme;
- d) unbefugte Bearbeitung;
- e) Fälschung, Entwendung oder widerrechtliche Verwendung.

Zu prüfen ist beispielsweise, ob sämtliche PC-Systeme und Fachanwendungen des Organs mit einem Authentifikationsprozess resp. mit sicheren Passwörtern geschützt sind und ein automatischer, periodischer Passwortwechsel erzwungen wird.

Die Sicherheitsanforderungen richten sich nicht an die Benutzerinnen und Benutzer von Informatikarbeitsplatzgeräten. Letztere erhalten im Rahmen ihrer Instruktion ein einfach umzusetzendes Merkblatt, welches auf der Homepage der kantonalen Datenschutzstelle zur Verfügung steht³.

c) Erstellen Massnahmenkatalog (§ 4 DSV)

Aufgrund des festgestellten Handlungsbedarfs sind die zu ergreifenden Massnahmen bereits vorgezeichnet, einzelne lassen sich direkt ableiten, wie beispielsweise Prozessverbesserungen, Kontrollen, Auswertungen und Schulungen. Die zu ergreifenden Sicherheitsmassnahmen sind in einem Massnahmenkatalog aufzulisten. Dabei ist dem gegenwärtigen Stand der Technik und den Grundsätzen der Verhältnismässigkeit und Wirtschaftlichkeit Rechnung zu tragen.

Für die Auswahl konkreter Massnahmen kann auf Arbeitsunterlagen und Massnahmenvorschläge des Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten (EDÖB)⁴ sowie des Informatikstrategieorgans Bund⁵ zurückgegriffen werden. Für ausgesprochen anspruchsvolle informatiktechnische Fragestellungen liefert das deutsche Bundesamt für Sicherheit in der Informationstechnik⁶ Massnahmenvorschläge.

Der vollständige Massnahmenkatalog gibt Auskunft über den Zweck, die Kosten sowie den Zeitbedarf für die Umsetzung der Massnahmen. Aus der Zweckumschreibung wird ersichtlich, welche Risiken die Bewilligungsinstanz bei einer Nichtrealisierung der entsprechenden Massnahme zu verantworten hätte. Im Anhang C steht eine Vorlage für die Erarbeitung eines Massnahmenkatalogs zur Verfügung.

d) Umsetzen der Massnahmen, überprüfen der Wirksamkeit (§ 5 DSV)

³ www.datenschutz-zug.ch

⁴ www.edoeb.admin.ch

⁵ www.isb.admin.ch

⁶ www.bsi.de

Die zuständigen Organe entscheiden, welche Massnahmen bis wann umgesetzt werden. Kostenwirksame Massnahmen werden im Rahmen der zur Verfügung stehenden Budgets umgesetzt, einfache Massnahmen ohne Kostenfolgen umgehend.

Die verantwortliche Person für die Instruktion der Mitarbeitenden stellt sicher, dass die Mitarbeitenden informiert und ausgebildet werden. Für die Instruktion der Mitarbeitenden steht auf der Homepage der Datenschutzstelle ein Merkblatt zur Verfügung¹. Die Organe überprüfen die Wirksamkeit der Massnahmen alle vier Jahre.

4. Zusammenfassung

Das Vorgehen zur Überprüfung der Datensicherheit lässt sich wie folgt zusammenfassen:

Arbeitspaket	Erledigt, wenn folgende Voraussetzungen erfüllt sind:
1.	Die zuständigen Personen für die Überprüfung der Datensicherheit, die Erstellung des Massnahmenkatalogs, die Bewilligung der beantragten Massnahmen sowie die Instruktion der Mitarbeitenden wurden bestimmt.
2.	Die zuständigen Personen wurden im Rahmen der erstmaligen Überprüfung der Datensicherheit von der kantonalen Datenschutzstelle und dem AIO zentral geschult. Sie verfügen über das notwendige Wissen und die Arbeitsunterlagen, um die weiteren Arbeiten in Angriff zu nehmen.
3.	Die Liste der Schutzobjekte wurde erstellt.
4.	Die Überprüfung der Datensicherheit wurde durchgeführt und, wo nötig, mit dem Informatikleistungserbringer oder den für die Sicherheit oder für die Bauten zuständigen Stellen koordiniert.
5.	Der Massnahmenkatalog wurde erarbeitet und der Bewilligungsinstanz zum Entscheid vorgelegt.
6.	Die umzusetzenden Massnahmen wurden von der Bewilligungsinstanz beschlossen. Nicht kostenwirksame Massnahmen wurden umgehend in Angriff genommen.
7.	Kostenwirksame Massnahmen wurden budgetiert, die Mittel bewilligt, die Arbeiten personell zugewiesen und zur Umsetzung freigegeben.
8.	Die Massnahmen wurden umgesetzt.

Anhang A: Sicherheitsanforderungen für Organe

Die Organe überprüfen die Sicherheit ihrer Personendaten anhand der nachstehenden Sicherheitsanforderungen. Die Sicherheitsanforderungen für Organe richten sich an die für die Überprüfung der Datensicherheit zuständigen Personen und nicht an die Benutzerinnen und Benutzer von Informatikarbeitsplatzgeräten. Für Letztere steht auf der Homepage der kantonalen Datenschutzstelle ein einfach umzusetzendes Merkblatt zur Verfügung.

Nr.	Sicherheitsanforderung
A1	Die Entsorgung von Datenträgern ist so geregelt, dass keine Rückschlüsse auf den Inhalt oder die gespeicherten Daten möglich sind. Reparaturen von Geräten sind von Fall zu Fall zu regeln (vertrauliche Daten sind vorher zu löschen).
A2	Sämtliche Zugriffe auf Fachanwendungen sind mit einem Authentifikationsprozess resp. mit sicheren Passwörtern geschützt. Die Fachanwendungen erzwingen einen automatischen, periodischen Passwortwechsel.
A3	Es dürfen keine Informationen an Unberechtigte weitergegeben werden. Vertrauliche Dokumente in gedruckter Form sowie elektronische Datenträger werden in den dafür vorgesehenen Schränken oder im Pult eingeschlossen. Nicht mehr benötigte geheime und vertrauliche Dokumententwürfe werden vernichtet.
A4	Bei Neuinstallationen und Releasewechseln von Hardware und Software werden mindestens alle geschäftskritischen und sicherheitstechnisch wichtigen Funktionen auf ihre Funktionstüchtigkeit überprüft.
A5	Es ist sichergestellt, dass nur Berechtigte Zugriff auf ein System oder bestimmte Fachanwendungen und deren Daten haben.
A6	Sicherheitsrelevante Prozesse (Onlinezugriffe, Mutationsprozesse jeglicher Art) werden von der für die jeweilige Datensammlung zuständigen Stelle organisiert, umgesetzt und dokumentiert.
A7	Änderungsaufträge an die Betriebsorganisation des Informatikbetreibers erfolgen schriftlich.
A8	Folgende Aktivitäten in den Fachanwendungen werden aufgezeichnet: gescheiterte Authentifikationsversuche, gescheiterte Objektzugriffe, Vergabe und Änderung von Privilegien und alle Aktionen, die erhöhte Privilegien benötigen.
A9	Bei der Installation von Fachanwendungen werden vordefinierte Accounts, Initialpasswörter, Privilegien oder Zugriffsrechte sofort kontrolliert und nötigenfalls angepasst oder gelöscht.
A10	Die Vertraulichkeit und Integrität von Benutzernamen, Passwörtern, Schlüsseln oder anderen kritischen Systemdaten aus Fachanwendungen ist bei der Übertragung über Netzwerke sichergestellt.

A11 ⁷	Systemzugriffssperren werden bei festen Arbeitsstationen nach 20 Minuten, bei Laptops nach 10 Minuten (ausser bei Präsentationen mit PowerPoint) und bei PDA nach 5 Minuten automatisch aktiviert. Die Informatikleistungserbringer können auf begründetes Gesuch hin und nach Einholung einer Stellungnahme der kantonalen Datenschutzstelle davon abweichende Einstellungen bewilligen. Der Entscheid des Informatikleistungserbringers ist der kantonalen Datenschutzstelle zuzustellen.
A12	Da mobile Informatikmittel (Notebooks, elektronische Agenden, Mobiltelefone, etc.) nicht nur im eigenen Büro verwendet werden, sondern auch ausserhalb des Arbeitsplatzes, sind sie mit geeigneten technischen Massnahmen zu schützen (z.B. Pre-Boot-Authentifikation, sichere Volumelabels, Diskverschlüsselung, etc.). Die Benutzerinnen und Benutzer sind in Fragen des Umgangs mit vertraulichen Daten in der Öffentlichkeit geschult. Für die Fernwartung sind speziell überwachte Accounts eingerichtet.
A13	Internet/E-Mail: Personendaten werden nur verschlüsselt übermittelt.
A14	Pro Fachanwendung ist festgelegt, welche Ausweichlösung zur Verfügung steht. Die Behandlung von Stör-, Not- und Katastrophenfällen und das konkrete Vorgehen sind vom Betreiber in Zusammenarbeit mit dem zuständigen Organ definiert und vereinbart worden.

⁷ Fassung gemäss RRB vom 13. April 2010.

Anhang B: Sicherheitsanforderungen für Informatikleistungserbringer

Die Informatikleistungserbringer der Organe überprüfen die Sicherheit im Bereich Netzwerke, Server, Arbeitsplatzeinrichtungen sowie organübergreifender Fachanwendungen anhand der nachfolgenden Sicherheitsanforderungen:

Nr.	Sicherheitsanforderung
B1	Es dürfen keine Informationen an Unberechtigte weitergegeben werden. Vertrauliche Dokumente in gedruckter Form sowie elektronische Datenträger werden in den dafür vorgesehenen Schränken oder im Pult eingeschlossen. Nicht mehr benötigte geheime und vertrauliche Dokumententwürfe werden vernichtet.
B2	Die Entsorgung von Datenträgern ist so geregelt, dass keine Rückschlüsse auf den Inhalt oder die gespeicherten Daten möglich sind. Reparaturen von Geräten sind von Fall zu Fall zu regeln (vertrauliche Daten sind vorher zu löschen).
B3	Es ist sichergestellt, dass nur Berechtigte Zugriff auf ein System oder bestimmte Anwendungen und deren Daten haben.
B4	Sämtliche Zugriffe auf PC-Systeme und Anwendungen sind mit einem Authentifikationsprozess resp. mit sicheren Passwörtern geschützt. Das Informatiksystem erzwingt einen automatischen, periodischen Passwortwechsel.
B5	Folgende Informatikmittel werden in Bezug auf Installation, Betrieb, Wartung und Benutzung fortlaufend dokumentiert: System-Hardware, Netzwerktopologie, Betriebssystem und systemnahe Software.
B6	Bei Neuinstallationen und Releasewechseln von Hardware und Software werden mindestens alle geschäftskritischen und sicherheitstechnisch wichtigen Funktionen auf ihre Funktionstüchtigkeit überprüft.
B7	Folgende Aktivitäten werden aufgezeichnet: System-Boot und -Shutdown, gescheiterte Authentifikationsversuche, gescheiterte Objektzugriffe, Vergabe und Änderung von Privilegien und alle Aktionen, die erhöhte Privilegien benötigen.
B8	Bei der Installation von Systemkomponenten werden vordefinierte Accounts, Initialpasswörter, Privilegien oder Zugriffsrechte sofort kontrolliert und nötigenfalls angepasst oder gelöscht.
B9	Das Netzwerk ist vor aktiven und passiven Angriffen geschützt.
B10	Auf allen Systemen werden nur die benötigten Protokolle zugelassen bzw. aktiviert.
B11	Zugriffsversuche durch Fremdsysteme mit unbekanntem oder unerlaubtem Netzwerkadressen werden aufgezeichnet.
B12	Die Vertraulichkeit und Integrität von Benutzernamen, Passwörtern, Schlüsseln oder anderen kritischen Systemdaten ist bei der Übertragung über Netzwerke geschützt.

B13 ⁸	Systemzugriffssperren werden, vorbehältlich einer Bewilligung gemäss Sicherheitsanforderung A11, bei festen Arbeitsstationen nach 20 Minuten, bei Laptops nach 10 Minuten (ausser bei Präsentationen mit PowerPoint) und bei PDA nach 5 Minuten automatisch aktiviert.
B14	Die gesamte Informatikinfrastruktur wird durch stets aktuell gehaltene Software vor schädlichen Programmen (Viren, Trojaner etc.) geschützt.
B15	Mobile Informatikmittel (Notebooks, elektronische Agenden, Mobiltelefone, etc.), da sie nicht nur im eigenen Büro verwendet werden, sondern auch ausserhalb des Arbeitsplatzes, sind mit geeigneten technischen Massnahmen geschützt (z.B. Pre-Boot-Authentifikation, sichere Volumelabels, Diskverschlüsselung, etc.). Die Benutzerinnen und Benutzer sind in Fragen des Umgangs mit vertraulichen Daten in der Öffentlichkeit geschult. Für die Fernwartung sind speziell überwachte Accounts eingerichtet.
B16	Internet/E-Mail: Personendaten werden nur verschlüsselt übermittelt.
B17	Systeme (Server, Clients etc.) sind mit den aktuellsten Fehlerbehebungsprogrammen versehen.
B18	Die Rekonstruktion und Wiederverwendbarkeit von Daten nach einem möglichen Datenverlust ist durch den Informatikbetreiber in einem Datensicherungskonzept beschrieben. Die Wiederherstellung von Daten wird pro Plattform periodisch geübt.
B19	Pro Anwendung ist festgelegt, welche Auswechlösung zur Verfügung steht. Die Behandlung von Stör-, Not- und Katastrophenfällen und das konkrete Vorgehen sind vom Betreiber in Zusammenarbeit mit dem zuständigen Organ definiert und vereinbart worden.

⁸ Fassung gemäss RRB vom 13. April 2010.

Anhang C: Mustervorlage Massnahmenkatalog

Nr.	Massnahme	Zweck gemäss § 2 DSV ¹					Verantwortlich:	Termin:	Kosten:	Entscheid Bewilligungsinstanz:
		a)	b)	c)	d)	e)				
	Konkrete Beschreibung der technischen und organisatorischen Massnahmen.						Zuständige Person oder Organisation.	Meilensteine, Endtermin	Ausgabewirksame Kosten Personalaufwand Sonstige Aufwendungen	Entscheid der Bewilligungsinstanz Ev. Auflagen

¹ Bitte ankreuzen, Mehrfachnennungen sind möglich

Anhang D: Begriffserläuterungen der Datenschutzstelle

Organ	Organe sind Behörden und Dienststellen, die für den Kanton oder die Gemeinden handeln, und natürliche oder juristische Personen oder Personengesellschaften des Handelsrechts, soweit ihnen öffentliche Aufgaben übertragen sind (§ 2 Bst. i DSG). Die Datensicherheitsverordnung gilt somit nicht nur für die kantonale Verwaltung und die Gerichte, sondern auch für die Gemeinden, für Anstalten (z.B. Pensionskasse, Gebäudeversicherung) sowie Personen, Unternehmen und Organisationen, die für den Kanton oder die Gemeinden öffentliche Aufgaben erfüllen (z.B. private Vereine mit Leistungsvereinbarung). Erfüllen letztere Aufgaben, die ihnen nicht von der öffentlichen Verwaltung übertragen worden sind, so unterliegen sie für diese Aufgaben selbstverständlich nicht der DSV.
Informatikleistungserbringer	Informatikleistungserbringer sind natürliche oder juristische Personen, welche für die Organe Informatikdienstleistungen erbringen, Informatiklösungen entwickeln, Informatikinfrastruktur bereitstellen, Anwendungen betreiben oder die Benutzerunterstützung (Support) sicherstellen
Datensammlung	Unter Datensammlung ist jeder Bestand von Personendaten zu verstehen, der so aufgebaut ist, dass die Daten nach den betroffenen Personen erschliessbar sind. Betroffene Personen sind natürliche oder juristische Person, über die Daten bearbeitet werden (§ 2 Bst. e und f DSG)
Datenträger	Unter den Begriff Datenträger fällt eine Vielzahl physischer Träger, auf denen Daten festgehalten werden können: Papier, Bilder, Durchschlagpapiere, Sticks, Disketten, Festplatten, Bänder, Compact-Disk, Farbbänder, etc.
Personendaten, gewöhnlich schützenswerte	<p>Das DSG umschreibt den Begriff der "Personendaten" wie folgt [§ 2 Bst. a DSG]: "Personendaten (im folgenden «Daten») sind alle Angaben, die sich auf eine bestimmte oder bestimmbare natürliche oder juristische Person oder auf eine Personengesellschaft des Handelsrechts beziehen." Alle Daten, die nicht besonders schützenswert bzw. Persönlichkeitsprofile sind, sind "gewöhnlich schützenswerte Personendaten" bzw. gemäss DSG "Daten". Da sich der Datenschutz nur auf Personendaten bezieht, spricht das DSG einfachheitshalber nur von Daten. Daten bedeutet somit immer Personendaten. Beispiele:</p> <ul style="list-style-type: none">• Name• Geschäftsadresse• Fahrzeugnummer• Vermögen <p>Vorsicht: Durch die Verbindung mit bestimmten Zusatzinformationen können diese Daten zu besonders schützenswerten Daten werden. Beispiele: Falls etwa der Name auf einer Liste von HIV-positiven Personen erscheint oder ein Fahrzeug zur Fahndung ausgeschrieben ist, etc.</p>

Personendaten, besonders schützenswerte

Das DSG umschreibt den Begriff der "besonders schützenswerten Personendaten" wie folgt [§ 2 Bst. b DSG]: "Besonders schützenswerte Daten sind alle Angaben über die religiösen, weltanschaulichen, politischen, berufspolitischen Ansichten oder Tätigkeiten, die Intimsphäre, die Gesundheit, die ethnische Zugehörigkeit, Massnahmen der sozialen Hilfe, administrative und strafrechtliche Verfolgungen und Sanktionen." Beispiele:

- Krankengeschichte
- Konfessionszugehörigkeit
- Partei- oder Gewerkschaftszugehörigkeit

Persönlichkeitsprofile

Das DSG behandelt Persönlichkeitsprofile rechtlich gleich wie besonders schützenswerte Personendaten. Das DSG umschreibt den Begriff des "Persönlichkeitsprofils" wie folgt [§ 2 Bst. b DSG]: "Daselbe gilt für eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der natürlichen Person (Persönlichkeitsprofil) erlaubt." Beispiele:

- Steuerakte einer Person
- Gerichtsakten einer Person

Abgrenzung Personen gegenüber Sachdaten

Sachdaten sind von Personendaten zu unterscheiden, da Sachdaten weder vom Datenschutzgesetz noch von der Datensicherheitsverordnung erfasst werden. Sachdaten sind Daten, die *in keiner Art und Weise* mit einer bestimmten oder bestimmbarer Person in Verbindung gebracht werden können. Beispiele für Sachdaten:

- Wassertemperatur des Zugersees
- Prozentualer Anteil der verschiedenen Konfessionen der schweizerischen Bevölkerung
- Fläche des Kantons Luzern

Vorsicht! Bei folgenden Beispielen handelt es sich hingegen um Personendaten, da die Daten ohne grossen Aufwand einer bestimmten Person zugeordnet werden können:

- Motorfahrzeugschild «ZG 4355»
- Radonbelastung eines bestimmten Grundstücks [es besteht ein Zusammenhang zur Vermögenssituation des Grundstückseigentümers]
- Telefonnummer

Bearbeiten von Personendaten

Das Bearbeiten von Personendaten ist jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten (§ 2 Bst. c DSG).
