RICHTLINIEN

betreffend die Mindestanforderungen an das Datenschutzmanagementsystem (Zertifizierung von Organisationen und Verfahren im Sinne von Art. 4 VDSZ)

vom XX November 2007

Der Eidgenössische Datenschutz- und Öffentlichkeitsbeauftragte,

gestützt auf Art. 11 Abs. 2 des Bundesgesetzes vom 19. Juni 1992 über den Datenschutz (DSG)[1],

gestützt auf Art. 4 Abs. 3 der Verordnung vom 28. September 2007 über die Datenschutzzertifizierungen (VDSZ)[2],

erlässt folgende Richtlinien:

Art. 1 Zweck

[1] Die Richtlinien legen die Mindestanforderungen an das Datenschutzmanagementsystem (DSMS) fest, um eine Zertifizierung von Organisationen und Verfahren im Sinne von Art. 4 VDSZ zu erhalten. Sie berücksichtigen dabei internationale Normen und Standards für die Errichtung, den Betrieb, die Überwachung und die Verbesserung von Managementsystemen, insbesondere die Norm ISO/IEC 27001:2005[3].

[2] Diese Richtlinien decken die gesamte vorgenannte Norm ISO 27001 ab, die sie im Sinne von Art. 2 auslegen und gemäss Art. 3 nachfolgend ergänzen oder abändern.

Art. 2 Auslegung

[1] Im Sinne der vorliegenden Richtlinien, ist *Informationssicherheit (IS)* in **Datenschutz (DS)** umzudeuten, insbesondere betreffend die Managementsysteme (**DSMS** anstelle von ISMS).

[2] Der Begriff der **(Nicht-)Konformität** betreffend die Datenschutzvoraussetzungen ergänzt systematisch denjenigen der *Risiken* betreffend die Ziele der Informationssicherheit.

---

[1] SR **235.1**
[2] SR **……..**
[3] DIN ISO/IEC 27001:2007-02 "Informationssicherheits-Managementsysteme – Anforderungen" Deutsche Übersetzung unter Lizenz erhältlich in Papierform oder als PDF-Datei bei www.din.de ;.

Art. 3 Umsetzung

0. Einleitung

1. Anwendungsbereich

   Mit Art. 4 Abs. 1 VDSZ kompatibel.

2. Normative Verweisungen

   Bundesgesetz über den Datenschutz
   (DSG vom 19. Juni 1992; SR 235.1)

   Verordnung zum Bundesgesetz über den Datenschutz
   (VDSG vom 14. Juni 1993; SR 235.11)

   Verordnung über die Datenschutzzertifizierungen
   (VDSZ vom 28. September 2007; SR ….)

   Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten (Übereinkommen STE 108 / ER vom 28. Januar 1981)

   Zusatzprotokoll zum Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung von personenbezogenen Daten (STE 108) bezüglich Aufsichtsbehörden und grenzüberschreitende Datenübermittlung (Protokoll STE 181 vom 8. November 2001)

3. Begriffe und Definitionen

   3.17 Datenschutz: (Art. 1 DSG)
   „Schutz der Persönlichkeit und der Grundrechte von Personen, über die Personendaten bearbeitet werden."

   3.18 Konformitätsmanagement:
   Koordinierte Tätigkeiten einer Organisation um die gesetzlichen und reglementarischen Voraussetzungen, insbesondere alle betreffend Datenschutz und denen sie unterstellt ist, einzuhalten.

   3.19 Nichtkonformitätsanalyse (-einschätzung):
   Systematische Benutzung von Informationen um die Ursachen der Nichtkonformität zu identifizieren und sie zu bewerten (leichter oder erheblicher Art).

   3.20 Behandlung der Nichtkonformität :
   Auswahl- und Umsetzungsverfahren von Massnahmen um eine Nichtkonformität zu beseitigen. Andernfalls kann eine Nichtkonformität auch dadurch verhindert werden, indem auf die betreffende Bearbeitung verzichtet wird.

4. Managementsystem

   4.2.1 b) 2) Grundlegende Klausel.

   4.2.1 d) 1) Besondere Aufmerksamkeit ist den organisationseigenen Werten der Art **Datensammlungen** (Art. 3 Bst. g DSG) zu gewähren und „Eigentümer" als **Dateninhaber** (Art. 3 Bst. i DSG) zu verstehen.

   4.2.1 e) 4) Alle Nichtkonformitäten müssen behandelt werden.

   4.2.1 f) 2) Nicht anwendbar auf die Nichtkonformitäten.

   4.2.1 f) 4) Nicht anwendbar auf die Nichtkonformitäten.

   4.2.1 g) Vgl. **Leitfaden für die Umsetzung des DSMS** (Anhang)

   4.2.1 h) Nicht anwendbar auf die Nichtkonformitäten.

   4.2.3 d) 6) Grundlegende Klausel.

   4.3.1 j)^{Neu} Verzeichnis der nicht angemeldeten Datensammlungen (vgl. Massnahme 8.2 des Anhangs)!

5. Verantwortung des Managements

   5.2.1 c) Grundlegende Klausel.

6. Interne DSMS-Audits

   6. a) Grundlegende Klausel.

7. Managementbewertung des DSMS

   7.3 c) 4-5) Grundlegende Klausel.

   7.3 c) 6) Nicht anwendbar auf die Nichtkonformitäten.

8. Verbesserung des DSMS

Art. 4 Inkrafttreten

Diese Richtlinien treten am xxxxxxx 2008 in Kraft.

Eidgenössischer Datenschutz und Öffentlichkeitsbeauftragter

Hanspeter Thür

Anhang: Leitfaden für die Umsetzung der DSMS-Richtlinien
(Vorabversion 0.9 vom 30.10.2007)

1. **Rechtmässigkeit** (Art. 4 Abs. 1 DSG)

Ziel des Grundsatzes: sicherstellen, dass die *Bearbeitung* der Personendaten in einer rechtmässigen Art und Weise erfolgt.

1.1 Rechtfertigungsgründe (Art. 13 DSG)

Massnahme
Private Personen brauchen für das „Bearbeiten" (Art. 3 Bst. e DSG) von „Personendaten" (Art. 3 Bst. a DSG) einen Rechtfertigungsgrund, mit anderen Worten die *Einwilligung* der „betroffenen Person" (Art. 3 Bst. b DSG), ein *überwiegendes* privates oder öffentliches *Interesse* oder eine *gesetzliche Grundlage.*

Umsetzung (Art. 4 Abs. 5 DSG)
Die *Einwilligung* der „betroffenen Person" muss *nach angemessener Information freiwillig* erfolgen. Bei der Bearbeitung von „besonders schützenswerten Personendaten" (Art. 3 Bst. c DSG) oder „Persönlichkeitsprofilen" (Art. 3 Bst. d DSG) muss die Einwilligung zudem ausdrücklich erfolgen. Mit anderen Worten handelt es sich darum zu überprüfen, dass keinerlei direkter oder indirekter Zwang resp. Druck vorliegt, und dass die gegebene Information relevant ist. Die Einwilligung ist ausdrücklich, wenn die „betroffene Person" das gelieferte Dokument eigenhändig oder elektronisch unterschrieben hat.
Im Einzelfall muss überprüft werden, ob das private oder öffentliche Interesse tatsächlich überwiegt, oder ob eine gesetzliche Grundlage vorliegt. Als gesetzliche Grundlage kann es sich um eine solche auf Bundesebene (formelles Gesetz oder Verordnung oder andere) oder auf kantonaler Ebene handeln. Ausländische gesetzliche Vorschriften stellen hingegen grundsätzlich keinen gesetzlichen Rechtfertigungsgrund im Sinne dieser Bestimmung dar.
Der Rechtfertigungsgrund gilt nur für den gesetzlich vorgesehen Zweck.

1.2 Gesetzliche Grundlage (Art. 17, 19 und 20 DSG)

Massnahme
Bundesorgane brauchen für die Bearbeitung von Personendaten eine *gesetzliche Grundlage*; bei der Bearbeitung von besonders schützenswerten Personendaten sowie von Persönlichkeitsprofilen ein Gesetz im *formellen Sinn* (Art 3 Bst. j DSG), das die Bearbeitung ausdrücklich vorsieht.

Umsetzung
Prüfen, welches Bundesorgan für die Bearbeitung der Personendaten verantwortlich ist, sowie das Vorhandensein einer gesetzlichen Grundlage prüfen, darüber hinaus, bei besonders schützenswerten Personendaten oder Persönlichkeitsprofilen prüfen, ob es sich um ein „formelles Gesetz" handelt.
Prüfen, ob die gesetzliche Grundlage alle notwendigen Elemente enthält.
Werden Personendaten durch ein Abrufverfahren zugänglich gemacht, ist zu überprüfen, dass dies ausdrücklich vorgesehen ist. Bei besonders schützenswerten Personendaten sowie Persönlichkeitsprofilen muss das Abrufverfahren in einem Gesetz im formellen Sinn ausdrücklich vorgesehen sein.

Betreffend besonders schützenswerte Personendaten oder Persönlichkeitsprofile, bei denen kein Gesetz im formellen Sinn die Bearbeitung ausdrücklich vorsieht, ist zu prüfen, ob eine Ausnahme gemäss Art. 17 Abs. 2 DSG vorliegt.
Bei der automatisierten Datenbearbeitung im Rahmen von Pilotversuchen muss geprüft werden, ob die Voraussetzungen gemäss Art. 17a DSG erfüllt sind.
Betreffend die Bekanntgabe von Personendaten, bei der keine gesetzliche Grundlage im vorgenannten Sinn existiert, ist zu prüfen, ob die Voraussetzungen von Art. 19 DSG erfüllt sind.
Es muss geprüft werden, ob die nötigen Instrumente bereitgestellt wurden um eine allfällige Sperrung der Bekanntgabe gemäss Art. 20 DSG durchführen zu können.

Andere Information (Art. 22 DSG)
Bundesorgane dürfen unter bestimmten Voraussetzungen Personendaten für nicht personenbezogene Zwecke, insbesondere für *Forschung*, *Planung* und *Statistik* bearbeiten.

1.3 Datenbearbeitung durch Dritte (Art. 10a Abs. 1 DSG)

Massnahme
Das Bearbeiten von Personendaten kann durch *Vereinbarung* oder *Gesetz Dritten übertragen* werden, wenn der Auftraggeber die nötigen Massnahmen ergriffen hat, damit die Daten nur so bearbeitet werden, wie er es selbst tun dürfte. Zudem darf keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbieten.

Umsetzung
Prüfen, ob eine Vereinbarung oder ein Gesetz vorliegt, das die Bearbeitung durch Dritte vorsieht, sowie Prüfung, ob die Voraussetzungen von Art. 10a DSG gegeben sind.
Insbesondere muss geprüft werden, ob die vorgesehenen Massnahmen, die sicherstellen, dass die Daten tatsächlich so bearbeitet werden, wie dies der Auftraggeber selber tun dürfte, und dass keine gesetzliche oder vertragliche Geheimhaltungspflicht es verbietet.
Die Glaubwürdigkeit des Rechtfertigungsgrundes muss gegebenenfalls überprüft werden.

2. Transparenz

Ziel des Grundsatzes: sicherstellen, dass die Bearbeitung der Personendaten in einer loyalen und transparenten Art erfolgen, d.h. in keinem Fall ohne Kenntnis der betroffenen Person oder für andere, als bei der Beschaffung der Personendaten angegebene Zwecke.

2.1 Treu und Glauben (Art. 4 Abs. 2 DSG)

Massnahme
Sicherstellen, dass die Bearbeitung der Personendaten nach Treu und Glauben.

Umsetzung
Prüfen, dass die Bearbeitung nicht geheim erfolgt, ausser wenn ein Gesetz dies ausdrücklich vorsieht (beispielsweise im Polizeibereich).
Prüfen, dass kein Zwang oder täuschende Elemente gegeben sind. Sicherstellen, dass die betroffene Person genügend und nicht falsch über Bearbeitungszweck und –art informiert wurde.

2.2 Erkennbarkeit (Art. 4 Abs. 4 DSG)

Massnahme
Sicherstellen, dass die *Beschaffung* der Personendaten und insbesondere der *Zweck ihrer Bearbeitung* für die betroffene Person erkennbar sind.

Umsetzung
Prüfen, dass die konkreten, der betroffenen Person zur Verfügung stehenden Informationen genügen, um die Erkennbarkeit sicherzustellen.

2.3 Informationspflicht (Art. 7a Abs. 1 DSG)

Massnahme
Der *Dateninhaber* (Art. 3 Bst. i DSG) ist verpflichtet, die betroffene Person über die Beschaffung von sie betreffende besonders schützenswerten Personendaten oder Persönlichkeitsprofilen zu informieren, unabhängig davon ob die Beschaffung direkt bei der betroffenen Person oder bei einem Dritten erfolgt ist.

Umsetzung (Art. 7a Abs. 2 DSG)
Die betroffene Person muss mindestens folgende Informationen erhalten:
a. Identität des Inhabers der Datensammlung;
b. der Zweck der Bearbeitung, für welchen die Daten beschafft worden sind;
c. die Kategorien der Datenempfänger, wenn eine Datenbekanntgabe vorgesehen ist.

3. Verhältnismässigkeit

Ziel des Grundsatzes: sicherstellen, dass die Bearbeitung der Personendaten verhältnismässig ist, das heisst, *geeignet* um den Zweck zu erreichen oder die Aufgabe zu erfüllen, diesbezüglich *notwendig* ist und in einem vernünftigen Verhältnis betreffend den Eingriff in die Persönlichkeit der betroffenen Person steht.

3.1 Verhältnismässige Bearbeitung (Art. 4 Abs. 2 DSG)

Massnahme
Es dürfen nur diejenigen Daten bearbeitet werden, die für die Erfüllung der Aufgabe resp. die Erreichung des Zweckes unbedingt notwendig und geeignet sind (*Datensparsamkeit* und/oder *Datenvermeidung*). Bei *besonders schützenswerten Personendaten* ist eine besondere Aufmerksamkeit geboten. Nicht mehr benötigte Personendaten müssen vernichtet oder anonymisiert werden, sofern keine Archivierungs- oder Aufbewahrungspflichten bestehen. In den Fällen, in denen die Identität der Person für den verfolgten Zweck nicht benötigt wird, hat die Bearbeitung in pseudonymisierter Form zu erfolgen.

Umsetzung
Die *Anonymisierung* von Personendaten besteht darin, sämtliche Elemente, die eine Identifikation ermöglichen, zu *entfernen*, derart, dass diese überhaupt nicht mehr mit einer bestimmten oder bestimmbaren Person verknüpft werden können (somit nicht einmal mehr dem DSG unterstellt).
Die *Pseudonymisierung* von Personendaten besteht darin, sämtliche Elemente, die eine Identifizierung ermöglichen, durch einen neutralen Identifikator, so genanntes *Pseudonym,* zu *ersetzen*, der parallel in einer *angehängten Korrespondenztabelle* mit den

Identifizierungselementen gespeichert wird, der es den Berechtigten erlaubt im Bedarfsfall eine Verknüpfung mit der betroffenen Person (bestimmbar im Sinne des DSG) herzustellen. Der strategische Vorteil besteht darin, dass die derart pseudonymisierten Daten gegenüber allen Personen, die keinen Zugang zur Korrespondenztabelle haben, als « anonym » betrachtet werden können. Ein solches Vorgehen macht nur Sinn, wenn die *Korrespondenztabelle* einen *beispielhaften Schutz* geniesst, sei es, dass sie nur durch berechtigte und authentifizierte Personen verwaltet wird, nur in chiffrierter Form gespeichert wird und im Prinzip nur eine Reidentifizierung im Einzelfall und unter einer abschliessenden Protokollierung der ausgeführten „Depseudonymisierungen“ erlaubt.
Betreffend *biometrische Daten*, die aus menschlichen physiologischen Eigenschaften wie der Fingerabdruck, die Hand, das Gesicht, die Iris oder der genetische Abdruck, oder aber Verhaltenseigenschaften wie die Unterschrift, die Stimme oder der „Tasteneingabe“ (keystroke) erhoben werden, muss das Verhältnis zwischen dem verfolgten Bearbeitungszweck und dem Eingriff in die Persönlichkeit der betroffenen Personen vernünftig bleiben. Diese Abwägung muss insbesondere den *einmaligen und unersetzbaren Charakter* der biometrischen Daten berücksichtigen, sowie ihre primäre Natur (Rohdaten) oder ihre sekundäre Natur (abgeleitete Daten; Templates). In einer ersten Analyse bevorzugen wir eine Verwendung von biometrischen Merkmalen, die keine physischen Spuren hinterlassen (bspw. Handumriss), eine *Dezentralisierung* der biometrischen Daten (im alleinigen Besitz der betroffenen Personen) und eine Benutzung von *biometrischen Templates* (weniger eingreifend als die entsprechenden primären Daten).

4. **Zweckbindung** (Art. 4 Abs. 3 DSG)

Ziel des Grundsatzes: sicherstellen, dass die Personendaten nur zu dem Zweck bearbeitet werden, der bei der Beschaffung angegeben wurde; gesetzlich vorgesehen ist oder aus den Umständen ersichtlich ist.

4.1 Spezifikation/Änderung der Zweckmässigkeit (Art. 3 Bst. i DSG)

Massnahme
Der „Inhaber der Datensammlung“ muss den Zweck der „Bearbeitung“ und ein ad-hoc-Dokument eintragen.

Umsetzung
Der Zweck der Bearbeitung muss in einem spezifischen und konzisen Dokument umschrieben sein, in schriftlicher Form und in einer klaren und für die betroffenen Personen leicht verständlichen Sprache. Dieses Dokument muss datiert sein und durch den „Inhaber der Datensammlung“ unterschrieben werden.
Jede nachträgliche Änderung des ursprünglichen Zwecks muss nachvollziehbar sein, desgleichen wie alle gegenüber den betroffenen Personen gemachten informationellen Handlungen (Veröffentlichungen, neue Einwilligungen, etc.).

4.2 Einschränkung der Bearbeitung

Massnahme
Sicherstellen, dass die „Bearbeitung“ der Personendaten im Rahmen des definierten Zwecks bleibt.

Umsetzung
Jede Datenbearbeitung, die weiter als die ursprünglich definierten Zwecke geht stellt eine **Umgehung der Zweckbindung** dar, die denunziert und sanktioniert werden kann.

Andere Information (Art. 10 Abs. 1 VDSG)
Der Inhaber der Datensammlung *protokolliert* die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen, wenn die präventiven Massnahmen den Datenschutz nicht gewähren. Eine Protokollierung hat insbesondere dann zu erfolgen, wenn *sonst nicht nachträglich festgestellt werden kann, ob die Daten für diejenigen Zwecke bearbeitet wurden, für die sie erhoben* oder bekannt gegeben wurden. Der Beauftragte kann die Protokollierung auch für andere Bereicht empfehlen.

5. Richtigkeit der Daten

Ziel des Grundsatzes: sicherstellen, dass beim Bearbeiten der „Personendaten" die Richtigkeit gegeben ist und gewahrt wird.

5.1 Richtigkeit der Daten (Art. 5 Abs. 1 DSG)

Massnahme
Sicherstellen, dass beim Bearbeiten der „Personendaten" die Richtigkeit gewahrt wird und alle angemessenen Massnahmen treffen, damit im Hinblick auf die Zwecke für die sie beschafft oder bearbeitet werden, nicht zutreffende oder unvollständige Daten gelöscht oder berichtigt werden.

Umsetzung
Beim Beschaffen von Personendaten müssen alle angemessenen Massnahmen ergriffen werden und die betroffene Person *authentifizieren* zu können und die Plausibilität der erhaltenen Informationen zu überprüfen. Angemessene Anforderungen (vordefinierte Formate, etc.) in den Masken helfen, zahlreiche Tippfehler oder andere falsche Eingaben zu vermeiden.
Personendaten, deren Richtigkeit nicht garantiert werden kann, darf nicht beschafft werden oder muss nach einer vorbestimmten Zeit zwingend berichtigt oder gelöscht werden. Kryptografische Lösungen könnten helfen, jegliche Entschlüsselung nach einem Verfalldatum zu verhindern. Der Dateninhaber muss sicherstellen, dass die beschafften Daten aktuell sind resp. aufdatiert werden.

5.2 Berichtigung von Daten (Art. 5 Abs. 2 DSG)

Massnahme
Jede „betroffene Person" kann die Berichtigung von nicht zutreffenden Daten verlangen.

Umsetzung
Beim Ausüben ihres Auskunftsrechts oder mit dem direkten Leserecht auf ihre eigenen Daten, kann die betroffene Person feststellen, dass Daten durch den Dateninhaber unrichtig beschafft und/oder bearbeitet worden sind. Gestützt auf Art. 15 kann sie darauf verlangen, dass diese Daten berichtigt oder vernichtet werden, oder dass die Weitergabe von diesen unterbrochen wird. Kann die Unrichtigkeit der Daten nicht festgestellt werden, kann der oder die GesuchstellerIn verlangen, dass ein Vermerk über die Bestreitung angefügt wird.

6. **Grenzüberschreitenden Bekanntgabe** (Art. 6 Abs. 1 DSG)

Ziel des Grundsatzes: Personendaten dürfen nicht ins Ausland bekannt gegeben werden, wenn dadurch die Persönlichkeit der betroffenen Personen schwerwiegend gefährdet würde, namentlich weil eine Gesetzgebung fehlt, die einen angemessenen Schutz gewährleistet.

6.1 Angemessenes Schutzniveau (Art. 6 Abs. 2 DSG)

Massnahme
Fehlt eine Gesetzgebung, die einen angemessenen Schutz gewährleistet, so können Personendaten ins Ausland nur bekannt gegeben werden, wenn:

a. *hinreichende Garantien*, insbesondere durch Vertrag, einen angemessenen Schutz im Ausland garantieren;
b. die betroffene Person im Einzelfall *eingewilligt* hat;
c. die Bearbeitung in *unmittelbaren Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrages* steht und es sich um Personendaten des Vertragspartners handelt;
d. die Bekanntgabe im Einzelfall entweder für die *Wahrung eines überwiegenden öffentlichen Interesses* oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich ist;
e. die Bekanntgabe im Einfall *erforderlich ist, um das Leben oder die körperliche Integrität* der betroffenen Person zu schützen;
f. die betroffene Person die *Daten allgemein zugänglich gemacht* und eine Bekanntgabe nicht ausdrücklich untersagt hat;
g. die Bekanntgabe *innerhalb derselben juristischen Person oder Gesellschaft* oder zwischen juristischen Personen und Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet, sofern die Beteiligten Datenschutzregeln unterstehen, welche einen angemessenen Schutz gewährleisten.

Umsetzung (Art. 6 Abs. 1 DSG)
Überprüfen, dass die Datenempfänger einer Gesetzgebung unterstehen, die einen angemessenen Schutz gewährleistet (vgl. die unverbindliche Liste der Staaten mit angemessener Datenschutzgesetzgebung, auf der Internetseite www.derbeauftragte.ch publiziert), sowie Überprüfung der Qualität der gelieferten Garantien für die Buchstaben a und g.

7. **Datensicherheit** (Art. 7 DSG)

Ziel des Grundsatzes: sicherstellen, dass die „Personendaten“ durch angemessene technische und organisatorische Massnahmen gegen unbefugtes „Bearbeiten“ geschützt werden.

7.1 Datenvertraulichkeit

Massnahme
Sicherstellen, dass die „Personendaten“ nicht anderen Personen, Einheiten oder nicht erlaubten Prozessen zur Verfügung gestellt oder bekannt gegeben werden.

Umsetzung (Anhang A von ISO 27001, vollumfänglich auf ISO 27002 verweisend)
A.7.x Management von organisationseigenen Werten
A.10.6.x Management der Netzsicherheit

A.10.7.x Handhabung von Speicher- und Aufzeichnungsmedien
A.10.8.x Austausch von Informationen
A.10.10.x Überwachung
A.11.x Zugangskontrolle

Die Kontrolle 7.2 betrifft die *Klassifikation* der Informationen: Das Datenschutzniveau der bearbeiteten Daten kann gemäss ihrem Sensibilitätsgrad bewertet werden. Eine Datenschutzklassifikation muss mindestens zwischen « *normalem Datenschutzniveau* », bei welchem ein Datenmissbrauch der betroffenen Person nur eine minimale Beeinträchtigung verursachen würde und einem « *hohen Niveau* » der besonders schützenswerten Personendaten und Persönlichkeitsprofile, dessen Missbrauch eine erhebliche Beeinträchtigung oder Gefährdung des Lebens der betroffenen Person verursachen könnte. Jedes dazwischen liegende Niveau kann definiert werden, aber es empfiehlt sich, insgesamt nicht mehr als 4 Schutzniveaus zu überschreiten.

7.2 Datenintegrität

Massnahme
Sicherstellen, dass die Personendaten vollständig, gültig und aktuell sind.

Umsetzung
A.10.4.x Schutz vor Schadsoftware und mobilem Programmcode
A.12.x Beschaffung, Entwicklung und Wartung von Informationssystemen

7.3 Datenverfügbarkeit

Massnahme
Sicherstellen, dass die „Personendaten“ auf Anfrage einer berechtigten Stelle zugriffsbereit und benutzbar sind.

Umsetzung
A.10.5.1 Backup
A.14.x Sicherstellung des Geschäftsbetriebes (BCMS)
A.15.1.3 Schutz von organisationseigenen Aufzeichnungen

7.4 Datenbearbeitung durch Dritte (Art. 10a Abs. 2 DSG)

Massnahme
Der Auftraggeber muss sich insbesondere vergewissern, dass der *Dritte die Datensicherheit gewährleistet*.

Umsetzung
Die Qualität der vom Auftraggeber dem Auftragnehmer abgegebenen Instruktionen dahingehend prüfen, damit festgestellt werden kann, ob sie den erwarteten Voraussetzungen genügen (vgl. oben stehende Massnahmen).

8. **Registrierung der Datensammlungen** (Art. 11a Abs. 1 DSG)

Ziel des Grundsatzes: Der Beauftragte führt ein *Register der Datensammlungen, das über Internet zugänglich ist*. Jede Person kann das Register einsehen.

8.1 Anmeldepflicht (Art. 11a Abs. 2 und 3 DSG; Ausnahmen Art. 11a Abs. 5 Bst. f-e DSG)

Massnahme
Bundesorgane müssen sämtliche "Datensammlungen“ beim EDÖB anmelden, währenddem Private Datensammlungen nur anmelden müssen, wenn sie regelmässig besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeiten oder wenn sie regelmässig Personendaten an Dritte bekannt geben.
Datensammlungen müssen beim EDÖB namentlich nicht angemeldet werden, wenn sämtliche Datenbearbeitungsverfahren, denen eine Datensammlung dient, *zertifiziert* wurden und das Ergebnis der Bewertung dem Beauftragten mitgeteilt wurde; sowie wenn ein *unabhängiger Datenschutzverantwortlicher bezeichnet wurde*.

Umsetzung
Der EDÖB wird den Bundesorganen sowie den Privatpersonen bald die neue Anwendung „WebDatareg“ zur Verfügung stellen, damit die Anmeldung und/oder Aktualisierung der Datensammlungen web-basiert erfolgen kann. Alle damit gehenden Weisungen und Vorschriften werden auch online geliefert. Das Publikum wird später die Informationen des Registers der angemeldeten Datensammlungen direkt vom Internet abfragen können, um sich an die Person für eine einfache Auskunftserteilung oder bei welcher das Auskunftsrecht geltend gemacht werden kann, wenden zu können.

8.2 Liste der nicht angemeldeten Datensammlungen (Art. 12b Abs. 1 Bst. b VDSG)

Massnahme
Der Inhaber der Datensammlungen trifft die erforderlichen Massnahmen, um die Angaben zu den nicht der Anmeldepflicht unterliegenden Datensammlungen auf Gesuch hin dem Beauftragten oder den betroffenen Personen mitteilen zu können.

Umsetzung
Sicherstellen der Instandstellung der notwendigen Massnahmen um dem Beauftragten oder den betroffenen Personen auf Gesuch die Liste der nicht der Anmeldepflicht untersehenden Datensammlungen abgeben zu können und um diese Liste aktualisiert halten zu können.
Erstellen und verwalten eines Inventars der nicht angemeldeten Datensammlungen, die folgende Informationen beinhalten:

a. Name und Adresse des Inhabers der Datensammlung;
b. Name und genaue Bezeichnung der Datensammlung;
c. Person, bei welcher das Auskunftsrecht ausgeübt werden kann;
d. Zweck der Datensammlung;
e. Kategorien der bearbeiteten Personendaten; die Kategorien der Datenempfänger;
f. Kategorien der an der Datensammlung Beteiligten, d.h. der Dritten, die Daten in die Datensammlung eingeben oder Mutationen vornehmen können.

9. Auskunfts- und Verfahrensrecht

Ziel des Grundsatzes: Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden. Liegt eine unrechtmässige Bearbeitung von Personendaten vor, kann die betroffene Person die Berichtigung, Vernichtung oder Sperrung (Verbot der Bekanntgabe an Dritte) verlangen.

9.1 Auskunftsrecht (Art. 8 Abs. 1 DSG)

Massnahme
Jede Person kann vom Inhaber einer Datensammlung Auskunft darüber verlangen, ob Daten über sie bearbeitet werden.

Umsetzung (Art. 8 Abs. 2 und 3 DSG)
Der Inhaber der Datensammlung muss der betroffenen Person alle über sie in der Datensammlung vorhandenen Daten, einschliesslich der verfügbaren Angaben über die Herkunft der Daten, den Zweck und gegebenenfalls die Rechtsgrundlagen sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger. *Daten über die Gesundheit* kann der Inhaber der Datensammlung der betroffenen Person durch einen von ihr bezeichneten Arzt mitteilen lassen.
Um die Durchsetzbarkeit dieses Rechts überprüfen zu können, müssen die Applikationen (in ihrem Menü) eine **vordefinierte Auskunftsrechtsroutine** beinhalten, die in einer klaren/übersichtlichen Weise alle eine identifizierte Person betreffenden Daten liefert.

Andere Informationen (Art. 9 und 10 DSG)
Das Auskunftsrecht kann nur in den im formellen Gesetz vorgesehenen Fällen das Auskunftsrecht *verweigern, einschränken oder aufschieben*.
Der Inhaber der Datensammlung muss angeben, aus welchem Grund er die Auskunft verweigert, einschränkt oder aufschiebt.
Der Inhaber einer Datensammlung, die ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums verwendet wird, kann unter bestimmten Voraussetzungen die Auskunft verweigern, einschränken oder aufschieben.

9.2 Rechtsansprüche und Verfahren (Art. 15 Abs. 1 und 2 DSG)

Massnahme
Liegt eine unrechtmässige Bearbeitung vor, kann die betroffene Person verlangen, dass die Daten *berichtigt, vernichtet* oder dass ihre Bekanntgabe an Dritte *gesperrt* wird. Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann der Kläger verlangen, dass bei den Daten ein *Vermerk über die Bestreitung* angebracht wird.

Umsetzung (art. 15, al. 4 DSG)
Überprüfen der eingesetzten Instrumente und Verfahren für die Ausübung des Berichtigungs-, Vernichtungs- und Sperrungsrecht sowie für die Anbringung des Vermerks über die Bestreitung. Insbesondere ist die Informationspflicht (Art. 7a DSG) zu beachten.
Es muss überprüft werden, ob die notwendigen Instrumente installiert wurden, um eine allfällige Sperrung der Bekanntgabe gemäss Art. 20 DSG sicherzustellen.