Anhang zu den Richtlinien über die Mindestanforderungen an das DSMS

(Version vom 15.04.2014)

Inhaltsverzeichnis

Inhaltsverzeichnis **1**
Leitfaden für das Datenschutz-Management **2**
a. Rechtmässigkeit (Art. 4 Abs. 1 DSG) **2**
a.1 Rechtfertigungsgründe (Art. 13 DSG; Bearbeitung durch private Personen) 2
a.2 Gesetzliche Grundlage (Art. 17, 19 und 20 DSG; Bearbeitung durch Bundesorgane) 3
a.3 Datenbearbeitung durch Dritte (Art. 10a Abs. 1 DSG; Datenbearbeitung durch private Personen und/oder durch Bundesorgane) 3
b. Transparenz **4**
b.1 Treu und Glauben (Art. 4 Abs. 2 DSG) 4
b.2 Erkennbarkeit (Art. 4 Abs. 4 DSG) 4
b.3 Informationspflicht (Art. 7a Abs. 1 DSG) 4
c. Verhältnismässigkeit **5**
c.1 Verhältnismässigkeit der Bearbeitung (Art. 4 Abs. 2 DSG) 5
d. Zweckbindung (Art. 4 Abs. 3 DSG) **6**
d.1 Festlegung und Änderung des Zwecks (Art. 3 Bst. i DSG) 6
d.2 Nutzungsbeschränkung 6
e. Richtigkeit der Daten **7**
e.1 Datenrichtigkeit (Art. 5 Abs. 1 DSG) 7
e.2 Berichtigung von Daten (Art. 5 Abs. 2 DSG) 7
f. Grenzüberschreitende Bekanntgabe (Art. 6 Abs. 1 DSG) **8**
f.1 Angemessener Schutz (Art. 6 Abs. 2 DSG) 8
g. Datensicherheit (Art. 7 DSG) **9**
g.1 Datenvertraulichkeit 9
g.2 Datenintegrität 9
g.3 Datenverfügbarkeit 10
g.4 Datenbearbeitung durch Dritte (Art 10a Abs. 2 DSG) 10
h. Registrierung der Datensammlungen (Art. 11*a* Abs. 1 DSG u. Art. 12*b* Abs. 1 VDSG) **10**
h.1 Anmeldepflicht (Art. 11a Abs. 2 und 3 DSG; Ausnahmen Art. 11a Abs. 5 Bst. f-e DSG) 10
h.2 Liste der nicht angemeldeten Datensammlungen (Art. 12b Abs. 1 Bst. b VDSG) 11
i. Auskunftsrecht und Verfahren **12**
i.1 Auskunftsrecht (Art. 8 Abs. 1 DSG) 12
i.2 Rechtsansprüche und Verfahren (Art. 15 und 25 DSG) 12

Leitfaden für das Datenschutz-Management

Dieser Leitfaden für das Datenschutz-Management (Leitfaden DS-M) setzt sich aus den 9 Grundprinzipien des Bundesgesetzes über den Datenschutz (DSG; SR 235.1) zusammen und führt Ziffer 5 der „Richtlinien über die Mindestanforderungen an das Datenschutzmanagementsystem“ aus. Er übernimmt in nicht abschliessender Art[1] die wichtigsten Anforderungen nach DSG und dessen Ausführungsverordnung (VDSG). Je nach Bereich (Gesundheit, Telekommunikation, Statistik, usw.) sind zusätzlich die spezialgesetzlichen Datenschutzbestimmungen zu berücksichtigen. Um die Lesbarkeit und die Verständlichkeit zu erleichtern, ist jede Massnahme analog dem „Leitfaden für das Informationssicherheits-Management (ISO/IEC 27002:2013[2])“ strukturiert, auf den sich im Übrigen die Massnahmen betreffend die Datensicherheit (Grundsatz Nr. 7) beziehen. Im Unterschied zu ISO 27002, die auf einer Risikoanalyse beruht, wurden die Massnahmen im Leitfaden DS-M als zwingende Massnahmen (muss, benötigt, verlangt, braucht) formuliert, da diese aufgrund einer Nicht-Konformitätsanalyse erfolgen und sich direkt aus dem DSG und der VDSG ergeben.

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

Ziel des Grundsatzes

Sicherstellen, dass die *Bearbeitung* der Personendaten in einer rechtmässigen Art und Weise erfolgt

a.1 Rechtfertigungsgründe (Art. 13 DSG; Bearbeitung durch private Personen)

Massnahme

Private Personen brauchen für das Bearbeiten (Art. 3 Bst. e DSG) von Personendaten (Art. 3 Bst. a DSG) einen Rechtfertigungsgrund, d. h. 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“ ist nur dann *gültig*, wenn sie aufgrund einer *angemessenen Information freiwillig* erfolgt. Mit anderen Worten muss die Einwilligung ohne direkten oder indirekten Zwang und aufgrund einer objektiven und schlüssigen Information 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* stattfinden. Die Einwilligung ist ausdrücklich, wenn die „betroffene Person“ das gelieferte Dokument eigenhändig oder elektronisch unterschrieben hat.

Im Einzelfall muss die Glaubwürdigkeit des überwiegenden privaten oder öffentlichen Interesses oder das Vorhandensein einer gesetzlichen Grundlage dargelegt werden können. Bei der gesetzlichen Grundlage kann es sich um eine solche auf Bundesebene (Gesetz im formellen Sinn oder Verordnung oder andere) oder auf kantonaler Ebene handeln. Der Rechtfertigungsgrund gilt nur für den gesetzlich vorgesehenen Zweck.

[1] Die Leitfäden und Merkblätter des EDÖB sowie die Erläuterungen und FAQ des BJ bilden dabei eine Auslegungshilfe die dazu dienen, die in diesem Leitfaden aufgeführten Ziele und Massnahmen zu konkretisieren.

[2] Änderung vom 15.04.2014

a.2 Gesetzliche Grundlage (Art. 17, 19 und 20 DSG; Bearbeitung durch Bundesorgane)

Massnahme

Bundesorgane dürfen Personendaten nur bearbeiten, wenn dafür eine *gesetzliche Grundlage* besteht. Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen sie nur bearbeiten, wenn ein Gesetz *im formellen Sinn* (Art. 3 Bst. j DSG) es ausdrücklich vorsieht.

Umsetzung

- Das für die Bearbeitung verantwortliche Bundesorgan muss identifiziert werden können.
- Eine gesetzliche Grundlage – für besonders schützenswerte Personendaten oder Persönlichkeitsprofile eine gesetzliche Grundlage „im formellen Sinn" – muss vorliegen. Diese muss alle notwendigen Elemente, insbesondere das verantwortliche Organ und der Zweck der Bearbeitung, die Kategorien der bearbeiteten Daten, die Datenempfänger und/oder der Beteiligten enthalten.
- Ausnahmsweise dürfen Personendaten in den in Art. 17 Abs. 2 Bst. a bis c und Art. 19 Abs. 1 bis 2 DSG bearbeitet resp. bekannt gegeben werden.
- Personendaten dürfen nur durch Abrufverfahren zugänglich gemacht werden, wenn dies ausdrücklich vorgesehen ist. Besonders schützenswerte Personendaten sowie Persönlichkeitsprofile dürfen nur durch ein Abrufverfahren zugänglich gemacht werden, wenn ein Gesetz im formellen Sinn es ausdrücklich vorsieht.
- Personendaten dürfen mittels automatisierter Informations- und Kommunikationsdienste zugänglich gemacht werden, wenn die Voraussetzungen von Art. 19 Bs. 3^{bis} DSG erfüllt sind.
- Bei automatisierten Datenbearbeitungen im Rahmen von Pilotversuchen müssen die in Art. 17*a* DSG aufgeführten Voraussetzungen erfüllt sein.
- Die Instrumente zur Umsetzung der Sperrung der Bekanntgabe von bestimmten Personendaten gemäss Art. 20 DSG müssen bestehen und brauchbar sein.

Andere Information (Art. 22 DSG)

Bundesorgane dürfen unter bestimmten Voraussetzungen Personendaten für nicht personenbezogene Zwecke, insbesondere für *Forschung*, *Planung* und *Statistik* bearbeiten.

a.3 Datenbearbeitung durch Dritte (Art. 10a Abs. 1 DSG; Datenbearbeitung durch private Personen und/oder durch Bundesorgane)

Massnahme

Das Bearbeiten von Personendaten kann durch Vereinbarung oder Gesetz *Dritten übertragen* werden wenn die folgenden Voraussetzungen erfüllt sind:

- die Daten werden nur so bearbeitet, wie der Auftraggeber selbst es tun dürfte;
- keine gesetzliche oder vertragliche Geheimhaltungspflicht verbietet es.

Umsetzung

- Eine Vereinbarung oder ein Gesetz muss die Bearbeitung durch Dritte vorsehen und die Voraussetzungen von Artikel 10*a* DSG müssen erfüllt sein.
- Der Dritte darf die Daten nur so bearbeiten, wie dies der Auftraggeber selbst tun dürfte. Somit muss jede durch den Dritten getätigte Bearbeitung für den Auftraggeber selbst rechtmässig sein.

- Es muss speziell sichergestellt werden, dass keine gesetzliche oder vertragliche Geheimhaltungspflicht die Bearbeitung verbietet.
- Die Glaubwürdigkeit des Rechtfertigungsgrundes muss gegebenenfalls überprüft werden können.
- Die Massnahmen in A.15.1 „Sicherheit in Lieferantenbeziehungen“ vom Anhang A der Norm ISO/IEC 27001:2013 („Anforderungen an ISMS“) finden ergänzend Anwendung[3].

Andere Information[4]

Siehe Massnahme g.4 zur Gewährleistung der Datensicherheit bei der Bearbeitung durch Dritte.

b. Transparenz

Ziel des Grundsatzes

Sicherstellen, dass die Bearbeitung der Personendaten rechtmässig und transparent erfolgt d.h. in keinem Fall ohne Kenntnis der betroffenen Person oder für andere als bei der Beschaffung angegebene Zwecke.

b.1 Treu und Glauben (Art. 4 Abs. 2 DSG)

Massnahme

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

Umsetzung

- Die Bearbeitung darf nicht ohne Wissen der betroffenen Person erfolgen, ausser wenn ein Gesetz dies ausdrücklich vorsieht (beispielsweise im Polizeibereich).
- Die Bearbeitung muss ohne Zwang und ohne irreführende Elemente erfolgen.
- Die betroffene Person muss genügend und korrekt über Bearbeitungszweck und –art informiert werden.

b.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

Die der betroffenen Person zur Verfügung stehenden konkreten Informationen müssen so ausgestaltet sein, dass die Erkennbarkeit der Beschaffung der Daten und des Zwecks ihrer Bearbeitung gewährleistet ist.

b.3 Informationspflicht (Art. 7a Abs. 1 DSG)

Massnahme

Der *Inhaber der Datensammlung* (Art. 3 Bst. i DSG) ist verpflichtet, die betroffene Person über die Beschaffung von sie betreffenden besonders schützenswerten Personendaten oder

[3] Änderung vom 15.04.2014

[4] Änderung vom 15.04.2014

Persönlichkeitsprofilen zu informieren, unabhängig davon ob die Beschaffung direkt bei der betroffenen Person oder bei einem Dritten erfolgt.

Umsetzung (Art. 7*a* Abs. 2-3 DSG)

- Der Inhaber der Datensammlung muss der betroffenen Person mindestens Folgendes mitteilen:
  - seine Identität (Dateninhaber);
  - die Zwecke des Bearbeitens, für welche die Daten beschafft werden;
  - die Kategorien der Datenempfänger, wenn eine Datenbekanntgabe vorgesehen ist.
- Wenn die Daten nicht bei der betroffenen Person beschafft werden, hat deren Information spätestens bei Beginn der Speicherung der Daten oder, wenn auf die Speicherung verzichtet wird, mit der ersten Bekanntgabe an Dritte zu erfolgen.

Andere Information (Art. 7a Abs. 4 DSG)

Die Informationspflicht des Inhabers der Datensammlung entfällt, wenn die betroffene Person bereits informiert wurde, oder, wenn die Daten nicht bei der betroffenen Person beschafft wurden, wenn:

- die Speicherung oder die Bekanntgabe der Daten ausdrücklich durch das Gesetz vorgesehen ist;
- die Information nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

c. Verhältnismässigkeit

Ziel des Grundsatzes

Sicherstellen, dass die Bearbeitung der Personendaten verhältnismässig ist, das heisst, *geeignet* ist, um den Zweck zu erreichen oder die Aufgabe zu erfüllen, diesbezüglich *notwendig* ist und in Bezug auf die Verletzung der Persönlichkeit der betroffenen Person *zumutbar* ist.

c.1 Verhältnismässigkeit der Bearbeitung (Art. 4 Abs. 2 DSG)

Massnahme

Es dürfen nur diejenigen Daten bearbeitet werden, die für die Erfüllung der Aufgabe bzw. die Erreichung des Zweckes unbedingt notwendig und dafür geeignet sind (*Datensparsamkeit* und/oder *Datenvermeidung*). Bei *besonders schützenswerten Personendaten* ist eine besondere Aufmerksamkeit geboten. Nicht 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 oder anonymisierter Form zu erfolgen.

Umsetzung

- Die *Anonymisierung* von Personendaten besteht darin, sämtliche Elemente, die eine Identifizierung ermöglichen, zu *entfernen*, so dass die Daten überhaupt nicht mehr oder nur noch mit ausserordentlichem Aufwand[5] mit einer bestimmten oder bestimmbaren Person verknüpft werden können (und somit nicht einmal mehr dem DSG unterstellt sind).
- Die *Pseudonymisierung* von Personendaten besteht darin, sämtliche Elemente, die eine Identifizierung ermöglichen, durch einen neutralen Identifikator, ein so genanntes *Pseudonym,* zu *ersetzen*; dieses Pseudonym wird parallel in einer separaten *Korrespondenztabelle* zusammen mit den Identifizierungselementen gespeichert und ermöglicht es den Berechtigten im Bedarfsfall, eine Verknüpfung mit der betroffenen Person (die dadurch bestimmbar im

[5] Ergänzung vom 10.03.2010

Sinne des DSG ist) herzustellen. Der Vorteil dieser Methode 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 exemplarischen Schutz geniesst, also nur durch berechtigte und authentifizierte Personen verwaltet wird, nur in chiffrierter Form gespeichert wird und eine Reidentifizierung grundsätzlich nur im Einzelfall und mit einer umfassenden Protokollierung der ausgeführten Depseudonymisierungen erlaubt.

- Bei *biometrischen Daten*, die aufgrund physiologischer Eigenschaften des Menschen, wie dem Fingerabdruck, der Hand, dem Gesicht, der Iris oder dem genetischen Abdruck oder aufgrund von Verhaltenseigenschaften wie der Unterschrift, der Stimme oder der Tasteneingabe *erfasst* wurden, muss das Verhältnis zwischen dem Bearbeitungszweck und der Verletzung der Persönlichkeit der betroffenen Personen zumutbar bleiben. Diese Abwägung muss insbesondere dem einmaligen und unersetzbaren Charakter der biometrischen Daten Rechnung tragen und berücksichtigen, ob es Daten primärer Natur (Rohdaten) oder sekundärer Natur (abgeleitete Daten; Templates) sind. Zu bevorzugen sind grundsätzlich die Verwendung von biometrischen Merkmalen, die keine physischen Spuren hinterlassen (z. B. Handumriss), die Benutzung von biometrischen sekundären Daten (Templates bedeuten in der Regel einen weniger grossen Eingriff in die Persönlichkeit ein als die entsprechenden primären Daten) und bei Verifizierungszwecken die dezentrale Speicherung der biometrischen Daten (im alleinigen Besitz der betroffenen Personen).

d. 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.

d.1 Festlegung und Änderung des Zwecks (Art. 3 Bst. i DSG)

Massnahme

Der „Inhaber der Datensammlung“ muss den Zweck der Bearbeitung in ein dafür vorgesehenes Dokument eintragen.

Umsetzung

- Der Zweck der Bearbeitung muss in einem speziell dafür vorgesehenen Dokument präzis und in einer klaren und für die betroffenen Personen leicht verständlichen Sprache umschrieben sein. Dieses Dokument muss datiert sein und vom „Inhaber der Datensammlung“ unterschrieben werden.
- Jede nachträgliche Änderung des ursprünglichen Zwecks muss nachvollziehbar sein, ebenso alle gegenüber den betroffenen Personen unternommenen Informationshandlungen (amtliche Veröffentlichungen, neue Einwilligungen, etc.),

d.2 Nutzungsbeschränkung

Massnahme

Sicherstellen, dass die „Bearbeitung“ von „Personendaten“ ausschliesslich im Rahmen des definierten Zwecks erfolgt.

Jede Datenbearbeitung, die über die bei der Datenbeschaffung festgelegten Zwecke hinausgeht, stellt eine Zweckentfremdung dar, die angezeigt und sanktioniert werden kann.

Umsetzung (Art. 10 VDSG)

- Der Inhaber der Datensammlung *protokolliert* die automatisierte Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen, wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten können. 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 Bearbeitungen empfehlen.
- Die Protokolle sind *während eines Jahres* revisionsgerecht festzuhalten. Sie sind ausschliesslich den Organen oder privaten Personen zugänglich, denen die Überwachung der Datenschutzvorschriften obliegt, und dürfen *nur für diesen Zweck verwendet* werden.

e. Richtigkeit der Daten

Ziel des Grundsatzes

Sicherstellen, dass die bearbeiteten „Personendaten“ richtig sind und dass ihre Richtigkeit bestehen bleibt.

e.1 Datenrichtigkeit (Art. 5 Abs. 1 DSG)

Massnahme

Wer „Personendaten“ bearbeitet muss sich über deren Richtigkeit vergewissern und alle angemessenen Massnahmen treffen um sicherzustellen, dass die Daten vernichtet oder berichtigt werden, die im Hinblick auf den Zweck ihrer Beschaffung oder Bearbeitung unrichtig oder unvollständig sind.

Umsetzung

- Beim Beschaffen von Personendaten müssen alle angemessenen Massnahmen ergriffen werden, damit die betroffene Person *authentifiziert* werden kann und sich die *Stichhaltigkeit* der erhaltenen Informationen überprüfen lässt. Mit angemessenen Vorgaben in den Masken (vordefinierte Formate etc.) lassen sich zahlreiche Tippfehler oder andere falsche Eingaben vermeiden.
- Personendaten, deren Richtigkeit nicht durch angemessene Massnahmen sichergestellt werden kann, dürfen nicht bearbeitet werden oder müssen nach einer bestimmten Zeit zwingend berichtigt oder vernichtet werden. Mit Hilfe kryptografischer Lösungen liesse sich jegliche Entschlüsselung nach einem Verfalldatum verhindern.
- Der Inhaber der Datensammlung muss die Aktualisierung der beschafften Daten sicherstellen.

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

Massnahme

Wer Personendaten bearbeitet muss sicherstellen, dass unrichtige Daten berichtigt werden können, insbesondere auf Verlangen der betroffenen Person.

Umsetzung

Übt eine betroffene Person ihr Auskunftsrecht aus oder hat sie einen direkten Zugriff (im Lesemodus) auf ihre eigenen Daten, so stellt sie möglicherweise fest, dass vom Inhaber der Datensammlung unrichtige Daten beschafft wurden und/oder bearbeitet werden. Gestützt auf Art. 15/25 DSG kann sie daraufhin verlangen, dass diese Daten berichtigt oder vernichtet werden, oder dass deren Weitergabe eingestellt wird. Kann weder die Richtigkeit noch die Unrichtigkeit der Daten dargetan werden, so

kann der Gesuchsteller oder die Gesuchstellerin verlangen, dass ein Vermerk über die Bestreitung angefügt wird.

Es obliegt dem Inhaber der Datensammlung Werkzeuge einzurichten, die die Berichtigung, die Vernichtung von Daten oder das Anbringen eines Vermerks ermöglichen sowie allfällige Datenübermittlungen unterbrechen.

f. Grenzüberschreitende 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.

f.1 Angemessener Schutz (Art. 6 Abs. 2 DSG)

Massnahme

Die Bekanntgabe von Personendaten darf für die Persönlichkeit der betroffenen Personen keine schwerwiegende Gefährdung darstellen. Eine solche Gefährdung wird vermutet, wenn die Datenempfänger keiner Gesetzgebung unterstellt sind, die einen angemessenen Schutz gewährleistet.

Umsetzung (Art. 6 Abs. 1 DSG)

Der Empfängerstaat muss auf der unverbindlichen Liste des Beauftragten der Staaten mit angemessener Datenschutzgesetzgebung aufgeführt sein, die auf folgender Internetsite publiziert ist: www.derbeauftragte.ch.

Fehlt eine solche Gesetzgebung, die im Ausland eine angemessene Datenschutzgesetzgebung garantiert, muss eine der folgenden Garantien gegeben sein:

- **hinreichende Garantien**, die insbesondere durch Vertrag einen angemessenen Schutz im Ausland gewährleisten (Art. 6 Abs. 2 Bst. a DSG);
- Garantie, dass die Beteiligten **Datenschutzregeln** unterstehen, welche einen angemessenen Schutz gewährleisten, wenn die Bekanntgabe innerhalb derselben juristischen Person oder Gesellschaft oder zwischen juristischen Personen oder Gesellschaften, die einer einheitlichen Leitung unterstehen, stattfindet (Art. 6 Abs. 2 Bst. g DSG).

Falls keine der vorgenannten Garantien vorliegt, muss eine der folgenden Voraussetzungen erfüllt sein:

- die betroffene Person hat im Einzelfall eingewilligt (Art. 6 Abs. 2 Bst. b DSG);
- die Bearbeitung steht in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags und es handelt sich um Personendaten des Vertragspartners (Art. 6 Abs. 2 Bst. c DSG);
- die Bekanntgabe ist im Einzelfall entweder für die Wahrung eines überwiegenden öffentlichen Interesses oder für die Feststellung, Ausübung oder Durchsetzung von Rechtsansprüchen vor Gericht unerlässlich (Art. 6 Abs. 2 Bst. d DSG);
- die Bekanntgabe ist im Einzelfall erforderlich, um das Leben oder die körperliche Integrität der betroffenen Person zu schützen (Art. 6 Abs. 2 Bst. e DSG);
- die betroffene Person hat die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt (Art. 6 Abs. 2 Bst. f DSG).

g. Datensicherheit (Art. 7 DSG)

Ziel des Grundsatzes

Sicherstellen, dass die „Personendaten“ durch angemessene technische und organisatorische Massnahmen gegen unbefugtes Bearbeiten geschützt werden.

g.1 Datenvertraulichkeit

Massnahme

Sicherstellen, dass die „Personendaten“ unbefugten Personen, Stellen oder Prozessen nicht zur Verfügung gestellt oder bekannt gegeben werden.

Umsetzung[6] (Anhang A von ISO 27001, der vollumfänglich auf ISO 27002 verweist)

A.6.1.5[neu]	Informationssicherheit im Projekt-Management (=>„Privacy by Design“)
A.6.2[neu]	Mobilgeräte und Telearbeit
A.8.x	Wertemanagement
A.9.x	Zugriffskontrollen
A.10.x[neu]	Kryptographie
A.11.x[7]	Schutz vor physischem Zugang und Umwelteinflüssen
A.12.4	Protokollierung und Überwachung
A.13.1	Netzwerksicherheitsmanagement
A.13.2	Informationsübertragung

Die Kontrolle A.8.2 betrifft die *Klassifikation* der Informationen: Das für die bearbeiteten Daten anwendbare Datenschutzniveau kann gemäss ihrem Sensibilitätsgrad bewertet werden. Eine Datenschutzklassifikation muss mindestens unterscheiden zwischen einem *„normalen Datenschutzniveau“* für Personendaten, deren Missbrauch die betroffene Person nur minimal beeinträchtigen würde und einem *„hohen Datenschutzniveau“* für besonders schützenswerte Personendaten und Persönlichkeitsprofile, deren Missbrauch die betroffene Person erheblich beeinträchtigen würde oder sogar ihr Leben gefährden könnte. Dazwischen lassen sich beliebige andere Datenschutzniveaus definieren, aber es empfiehlt sich, insgesamt nicht mehr als 4 Schutzniveaus festzulegen.

g.2 Datenintegrität

Massnahme

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

Umsetzung[8]

A.12.2	Schutz vor Malware
A.14.x	Anschaffung, Entwicklung und Instandhaltung von Systemen

[6] Änderung vom 15.04.2014

[7] Ergänzung vom 10.03.2010

[8] Änderung vom 15.04.2014

g.3 Datenverfügbarkeit

Massnahme

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

Umsetzung[9]

A.12.3 Datensicherungen
A.17.x Informationssicherheitsaspekte des Business Continuity Managements
A.18.1.3 Schutz dokumentierter Informationen

g.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 zur Gewährleistung der Datensicherheit muss den erwarteten Voraussetzungen genügen (vgl. oben genannte Massnahmen).

Die Massnahmen in A.15.2 „Management der Dienstleistungserbringung durch Lieferanten“ vom Anhang A der ISO 27001 finden ergänzend Anwendung[10].

Andere Information[11]**:**

Siehe Massnahme a.3 zu den gesetzlichen Voraussetzungen bei der Bearbeitung durch Dritte.

h. Registrierung der Datensammlungen (Art. 11*a* Abs. 1 DSG u. Art. 12*b* Abs. 1 VDSG)

Ziel des Grundsatzes

Das Register der Datensammlungen ist der Schlüssel für die Ausübung des Auskunftsrechts und der anderen Rechte durch die betroffenen Personen. Der Beauftragte führt ein *Register der Datensammlungen*, das über *Internet* zugänglich ist. Jede Person kann das Register einsehen. Zudem dient das Register dem Beauftragten dazu, eine Übersicht der bestehenden nationalen Datensammlungen zu haben, was ihm seine Aufsichtstätigkeit erleichtert.

h.1 Anmeldepflicht (Art. 11a Abs. 2 und 3 DSG; Ausnahmen Art. 11a Abs. 5 Bst. f-e DSG)

Massnahme

Bundesorgane müssen sämtliche „Datensammlungen“ beim Beauftragten anmelden, währenddem Private Datensammlungen nur anmelden müssen, wenn sie regelmässig besonders schützenswerte

[9] Änderung vom 15.04.2014

[10] Änderung vom 15.04.2014

[11] Änderung vom 15.04.2014

Personendaten oder Persönlichkeitsprofile bearbeiten oder wenn sie regelmässig Personendaten an Dritte bekannt geben.

Datensammlungen müssen beim Beauftragten namentlich dann 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 Beauftragte stellt den Bundesorganen sowie den Privatpersonen eine neue Anwendung ‚WebDatareg' zur Verfügung, damit die Anmeldung und die Aktualisierung der Einträge webbasiert erfolgen können. Über WebDatareg kann das Publikum zudem die *Informationen des Registers* der angemeldeten Datensammlungen direkt vom Internet abfragen und kann sich so an die Person wenden, die für Auskünfte zuständig ist oder bei der das Auskunftsrecht geltend gemacht werden kann.

h.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

Die notwendigen Massnahmen sind zu treffen, damit dem Beauftragten oder den betroffenen Personen auf Gesuch hin die Angaben zu den nicht der Anmeldepflicht unterstehenden Datensammlungen mitgeteilt werden können und damit die Liste dieser Datensammlungen auf dem aktuellen Stand gehalten werden kann. Dafür ist eine Liste der *nicht angemeldeten Datensammlungen* zu erstellen und zu verwalten, die folgende Informationen beinhaltet:

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;
f. Kategorien der Datenempfänger;
g. Kategorien der an der Datensammlung Beteiligten, das heisst der Dritten, die Daten in die Datensammlung eingeben und verändern dürfen.

Andere Information (Art. 28 Abs. 3 VDSG)

Der Beauftragte führt ein *Verzeichnis der Inhaber von Datensammlungen*, die ihrer Pflicht zur Anmeldung der Datensammlungen nach Art. 11*a* Abs. 5 Bst. e (Ernennung eines unabhängigen Datenschutzverantwortlichen) und Bst. f (aufgrund eines Zertifizierungsverfahrens erworbenes Qualitätszeichen) DSG enthoben sind. Dieses Verzeichnis ist online zugänglich, damit das Publikum daraus schliessen kann, dass diese grundsätzlich Datensammlungen nicht im Register der Datensammlungen des Beauftragten angemeldet sind.

i. Auskunftsrecht und Verfahren

Ziel des Grundsatzes

Der Inhaber einer Datensammlung muss jedes Auskunftsgesuch behandeln. Liegt eine unrechtmässige Bearbeitung vor, kann die betroffene Person die Berichtigung, Vernichtung oder Sperrung (Verbot der Bekanntgabe an Dritte) der Daten verlangen.

i.1 Auskunftsrecht (Art. 8 Abs. 1 DSG)

Massnahme

Der Inhaber einer Datensammlung muss jedes Auskunftsgesuch behandeln und der gesuchstellenden Person antworten.

Umsetzung (Art. 8 Abs. 2 und 3, Art. 9 und 10 DSG)

Der Inhaber der Datensammlung muss seine Datensammlung so gestalten, dass er eingehende Auskunftsgesuche behandeln kann. Er muss ebenfalls Suchwerkzeuge aufstellen, die es erlauben, alle betreffend die gesuchstellende Person bearbeiteten Daten zu finden. Der Inhaber der Datensammlung muss zudem in der Lage sein, der betroffenen Person alle Informationen zu unterbreiten.

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 der Bearbeitung sowie die Kategorien der bearbeiteten Personendaten, der an der Sammlung Beteiligten und der Datenempfänger mitteilen. *Daten über die Gesundheit* kann der Inhaber der Datensammlung der betroffenen Person durch einen von ihr bezeichneten Arzt mitteilen lassen.

Um die richtige Gewährung des Auskunftsrechts überprüfen zu können, müssen die Informatikapplikationen (in ihrem Menü) eine **vordefinierte Routine** enthalten, die alle Daten zur identifizierten Person in klarer Art aufführt.

Der Inhaber der Datensammlung muss Prozesse aufstellen, die es ihm ermöglichen, die Rechte der betroffenen Personen sicherzustellen. Das Auskunftsrecht darf nur in den gesetzlich vorgesehenen Fällen *verweigert, eingeschränkt* oder *aufgeschoben* werden. In diesen Fällen muss der Inhaber der Datensammlung angeben, aus welchem Grund er die Auskunft verweigert, einschränkt oder aufschiebt.

Wird die Auskunft aufgeschoben, muss der Inhaber der Datensammlung ein Erinnerungssystem vorsehen. Die Rückverfolgbarkeit, insbesondere von allfälligen Auskunftsverweigerungen und –einschränkungen muss ebenfalls sichergestellt sein.

Andere Information (Art. 10 DSG)

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.

i.2 Rechtsansprüche und Verfahren (Art. 15 und 25 DSG)

Massnahme

Im Rahmen der Bestimmungen betreffend Rechtsansprüche und Verfahren kann die betroffene Person vom Zivilrichter (Bearbeitung durch private Personen) oder vom Bundesverwaltungsgericht (Bearbeitung durch Bundesorgane) verlangen, dass die Daten *berichtigt*, *vernichtet* oder *gesperrt* (Verbot der Bekanntgabe an Dritte) werden. Kann weder die Richtigkeit noch die Unrichtigkeit von Personendaten dargetan werden, so kann der Kläger verlangen, dass bei den Daten ein *entsprechender Vermerk* angebracht wird.

Umsetzung (Art. 15 Abs. 4 und Art. 25 Abs. DSG)

Die Instrumente und Verfahren für die Ausübung des Berichtigungs-, Vernichtungs- und Sperrungsrechts sowie das Recht auf die Anbringung eines Bestreitungsvermerks müssen geschaffen werden. Instrumente für die Sperrung der Bekanntgabe an Dritte gemäss Art. 20 DSG (Datenbearbeitung durch Bundesorgane) müssen bestehen und umgesetzt werden können.

Andere Information

Mit der Einführung der Informationspflicht (Art. 7*a* DSG) ist das Recht, eine Sperrung der Datenbearbeitung zu verlangen, griffiger geworden.