



16. Dezember 2010

Leitfaden für die Erarbeitung der Rechtsgrundlagen für den Betrieb eines Systems zur automatisierten Bearbeitung von Personendaten (ersetzt die Fassung vom 16. März 2010)

Der vorliegende Leitfaden richtet sich in erster Linie an Juristinnen und Juristen, die entsprechend den Anforderungen des Bundesgesetzes über den Datenschutz (DSG, SR 235.1) die Rechtsgrundlagen für den Betrieb eines Systems zur automatisierten Bearbeitung von Personendaten (nachfolgend «System») erarbeiten. Im ersten Teil (A. Problemdefinition und Lösungssuche) werden die vorgängigen Fragen behandelt, die sich noch vor der Ausarbeitung der Rechtsgrundlagen bei der Konzipierung des Systems stellen. Der zweite Teil (B. Normkonzept) befasst sich mit der eigentlichen Ausarbeitung der Rechtsgrundlagen, insbesondere auch den Grundsätzen des Datenschutzes und der zu wählenden Normstufe.

Diese Anleitung dient als Hilfsmittel, das bei der Einrichtung eines neuen Systems einzubeziehen ist. Sie konzentriert sich auf Fragen des Datenschutzes im Zusammenhang mit der Einrichtung eines Systems, doch erübrigt sich damit keineswegs ein Vorgehen gemäss der Rechtsetzungsmethodik, wie es im [Gesetzgebungsleitfaden](#), insbesondere im Modul Gesetz, empfohlen wird.

Zu berücksichtigen sind auch:

- die [anderen legistischen Hilfsmittel](#)
- die [Methode zum Führen und Abwickeln von Projekten der Informations- und Kommunikationstechnik](#) (HERMES)
- der [Führungsleitfaden Geschäftsverwaltung](#) (GEVER).

A. Problemdefinition und Lösungssuche

Im Rahmen der Rechtsetzungsmethodik ist meistens ein Problemlösungszyklus zu durchlaufen (vgl. →Vorbereitung der Arbeiten und Informationsbeschaffung [Modul Gesetz]). Die folgenden Punkte können bei der Problemdefinition und der Suche nach Lösungen hilfreich sein.

1. Dateneigenschaften

1.1 Werden Personendaten bearbeitet?

Zunächst stellt sich die Frage, ob in dem System Personendaten im Sinne des DSG bearbeitet werden sollen, d. h. Angaben, die sich auf eine natürliche oder juristische Person beziehen und mit denen diese bestimmt werden kann. Die Definition von «Personendaten» ist sehr weit gefasst, weil sie sämtliche Angaben umfasst, die sich auf eine bestimmte oder auch nur bestimmbar Person beziehen. Werden zum Beispiel Daten über «den grössten Schweizer Tennisspieler» erhoben, gelten diese als Personendaten, weil sich damit die betreffende Person bestimmen lässt, ohne dass ihre Identität bekannt gegeben wird. Dagegen bilden Informationen über die verschiedenen Arten von Falschgeld keine Personendaten.

Werden in dem System keine Personendaten bearbeitet, gelten die Anforderungen des DSG nicht. Denn das DSG bezweckt den Schutz der Persönlichkeit von natürlichen und juristischen Personen, nicht aber den Schutz der Daten an sich.

Wenn das DSG auf den betreffenden Bereich nicht anwendbar ist, d. h. dieser Bereich zu den Ausnahmen vom Geltungsbereich des DSG gehört, wie z. B. öffentliche Register des Privatrechtsverkehrs, so bedeutet dies nur, dass nach Ansicht des Gesetzgebers für den betreffenden Bereich dessen eigene Datenschutzregeln massgebend sind. Der vorliegende Leitfaden gilt somit mutatis mutandis.

Rechtsgrundlagen: Art. 1, Art. 2 Abs. 2 und 3 Bst. a DSG.

Beispiele: Art. 12 Abs. 3 Bst. a und c des Bundesgesetzes über die polizeilichen Informationssysteme des Bundes (BPI, SR 361) sieht vor, dass ein System Daten über Personen enthält, die fedpol als Tatverdächtige oder Geschädigte oder im Zusammenhang mit der Suche nach vermissten Personen gemeldet worden sind.

1.2 Werden besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet?

Werden mit dem System Personendaten bearbeitet, ist die Art dieser Daten zu bestimmen, d. h. festzustellen, ob es sich um besonders schützenswerte Personendaten oder um Persönlichkeitsprofile handelt.

Unter besonders schützenswerten Personendaten versteht man Daten über die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten, die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit, Massnahmen der sozialen Hilfe, administrative oder strafrechtliche Verfolgungen und Sanktionen. Die Definition ist abschliessend.

Unter einem Persönlichkeitsprofil versteht man eine Zusammenstellung von Daten, die eine Beurteilung wesentlicher Aspekte der Persönlichkeit einer natürlichen Person erlaubt.

Dagegen bilden der Name einer Person, ihr Geburtsdatum oder Angaben zu ihrem Vermögen (einschliesslich Angaben zum Lohn) keine besonders schützenswerten Daten.

Rechtsgrundlage: Art. 3 Bst. a, c und d DSG.

Beispiele: Die gemäss Art. 12 Abs. 3 Bst. a und c BPI bearbeiteten Daten sind besonders schützenswerte Personendaten.

1.3 Wurde die Schwere der Persönlichkeitsverletzung geprüft?

Die Schwere der Persönlichkeitsverletzung ist zu prüfen, indem nicht nur die Art der Daten (z. B. besonders schützenswerte Personendaten) berücksichtigt wird, sondern vor allem auch der Zweck der Bearbeitung (z. B. eine polizeiliche Datensammlung), die Art und Weise der Datenbeschaffung (z. B. ohne Wissen der betroffenen Person) sowie der Kreis und die Zahl der Personen, die von den Daten Kenntnis haben.

Beispiel: In der Botschaft des Bundesrates vom 29. Mai 2002 über das Informationssystem für den Ausländer- und den Asylbereich («Ausländer 2000») wird die Möglichkeit erwähnt, im Asylbereich elektronische Dossiers einzuführen, und darauf hingewiesen, dass ein solches System besonders schützenswerte Personendaten (Befragungsprotokolle, Asylentscheide usw.) enthalten werde (BBl 2002 4693 [4709]).

2. Zweck des Systems

2.1 Ist der allgemeine Zweck des Systems bestimmt?

Der Zweck des Systems muss so umschrieben werden, dass er für die betroffenen Personen genau erkennbar ist. Nicht ausreichend ist der Hinweis, dass das System zur Erfüllung der gesetzlichen Aufgaben der zuständigen Bundesbehörde dient. Die betreffenden Aufgaben müssen vielmehr möglichst abschliessend aufgelistet werden; eine bloss beispielhafte Aufzählung kann gerechtfertigt sein, wenn der Adressatenkreis eng ist, wenn wenig wichtige Daten ausgetauscht werden oder wenn die Einschränkung der Persönlichkeitsrechte nicht schwer wiegt.

Rechtsgrundlagen: Art. 3 Bst. i und Art. 4 Abs. 3 und 4 DSGVO.

Beispiel: Art. 14 Abs. 1 BPI sieht vor, dass fedpol ein Informationssystem zur Personenidentifikation im Rahmen der Strafverfolgung und der Suche nach vermissten Personen betreibt.

2.2 Handelt es sich um ein internes Geschäftsverwaltungssystem oder um ein Informationssystem mit Abrufverfahren?

Ist der Zweck des Systems bestimmt, muss geklärt werden, ob es sich bei dem geplanten System um ein Geschäftsverwaltungssystem handelt oder um ein Informationssystem, das durch ein Abrufverfahren zugänglich ist.

Unter einem Geschäftsverwaltungssystem versteht man ein Informations- und Dokumentationssystem, das zur Registrierung, Verwaltung, Indexierung und Kontrolle von Schriftverkehr und Geschäften geführt wird. In einem solchen System kann der Inhaber der Datensammlung Personendaten nur speichern, wenn sie dazu dienen, seine Geschäfte zu bearbeiten, die Arbeitsabläufe zu organisieren, festzustellen, ob er Daten über eine bestimmte Person bearbeitet, und den Zugang zur Dokumentation zu erleichtern. Zu den Personendaten haben

ausschliesslich Mitarbeiterinnen und Mitarbeiter des betreffenden Bundesorgans Zugang, und dies nur soweit sie sie zur Erfüllung ihrer Aufgaben brauchen.

Betreiben mehrere Bundesorgane dasselbe System oder haben mehrere Bundesorgane oder Dritte mittels Abrufverfahren Zugang zu den im System bearbeiteten Daten, handelt es sich um ein Informationssystem, zu welchem nach dem Selbstbedienungsprinzip online Verbindung aufgenommen wird.

Zu vermeiden ist nach Möglichkeit die Einrichtung eines gemischten Systems (Geschäftsverwaltungs- und Informationssystem). Ein Beispiel dafür ist das vorgesehene System für die internationale Rechtshilfe in Strafsachen.

Rechtsgrundlagen: Art. 57h des Regierungs- und Verwaltungsorganisationsgesetzes (RVOG, SR 172.010) und Art. 19 Abs. 3 DSG.

Beispiel: Art. 18 BPI behandelt das Geschäfts- und Aktenverwaltungssystem von fedpol.

3. Architektur des Informatiksystems

3.1 Sind die Architektur des Informatiksystems und seine Möglichkeiten definiert?

3.1.1 Im Allgemeinen

Der Begriff «*Architektur des Informatiksystems*» bezeichnet vorliegend den allgemeinen Aufbau des Informatiksystems, die Organisation seiner verschiedenen Elemente und der Beziehungen zwischen den Elementen.

Bei der Konzipierung eines Systems ist es von zentraler Bedeutung, dass gleich zu Beginn eine Zusammenarbeit zwischen den Juristinnen und den Informatikern des zuständigen Bundesorgans eingeleitet wird, damit die künftigen Erlasstexte mit der Realität vereinbar sind. Bevor der Entwurf einer Rechtsgrundlage ausgearbeitet wird, muss die Juristin oder der Jurist somit aufgrund des Austauschs mit den Informatikern und Informatikerinnen die Architektur und die Möglichkeiten des Systems in den groben Zügen erfassen. Diese Zusammenarbeit muss bis zum Ende der Konzeptphase weitergeführt werden, da das Konzept im Zug der Arbeiten technische Änderungen erfahren kann.

3.1.2 Verbindungen zwischen Systemen

Für die Systemarchitektur zentral ist die Frage, ob das Informationssystem Verbindungen zu anderen Informationssystemen haben soll, die an anderer Stelle geregelt werden.

Beispiel: Artikel 9 Absatz 2 BPI sieht vor, dass die Benutzenden im Rahmen ihrer Zugriffsrechte mit einer einzigen Abfrage prüfen können, ob bestimmte Personen oder Organisationen in einem Informationssystem oder mehreren Informationssystemen des Verbunds verzeichnet sind.

In der geltenden Gesetzgebung finden sich verschiedene Begriffe wie «*verbinden*», «*Schnittstelle*», «*Austausch*» und «*Übertragung*» von Daten, «*Vernetzung*» sowie «*Subsysteme*» oder «*Komponenten*» eines Systems.

Sollen zwei Systemen, die in den jeweiligen Erlassen an sich eine genügende gesetzliche Grundlage haben, miteinander verbunden werden, so bedarf die Verbindung zusätzlich einer spezifischen gesetzlichen Grundlage.

Beispiel: Der Kurzzugriff der Polizeibehörden der Kantone und des Grenzwachkorps auf das Informationssystem über Gewalttätigkeiten anlässlich von Sportveranstaltungen (HOOGAN) erfolgt «*via Schnittstelle im Informationssystem RIPOL*» (Art. 24a BWIS; Art. 9 Abs. 5 der Verordnung vom 4. Dezember 2009 über verwaltungspolizeiliche Massnahmen und über Informationssysteme des Bundesamtes für Polizei, SR 120.52).

Das automatisierte Polizeifahndungssystem (RIPOL) nach Artikel 15 BPI wiederum besitzt eine Schnittstelle mit dem Informationssystem für den Ausländer- und den Asylbereich (ZEMIS, SR 142.51), ohne dass der Begriff «Schnittstelle» hier verwendet würde. Es werden jedoch die Auswirkungen dieser Verbindung beschrieben: «Eine Suche in ZEMIS führt zu einer Online-Abfrage innerhalb des automatisierten Polizeifahndungssystems (RIPOL).» (Art. 3 Abs. 2 der ZEMIS-Verordnung, SR 142.513).

Eine Verbindung zwischen Systemen besteht auch im Rahmen der Übernahme und Umsetzung des Schengen/Dublin-Besitzstandes, indem dort in einem Abrufverfahren Daten zwischen dem zentralen, länderübergreifenden System und den nationalen Systemen ausgetauscht werden.

Gesetzliche Grundlagen: Art. 4 Abs. 2 und Art. 19 Abs. 3 DSG sowie die Bestimmungen des jeweils umzusetzenden Staatsvertrags.

Beispiel: Revision des Ausländergesetzes im Zusammenhang mit der Umsetzung der Verordnung (EG) Nr. 767/2008 des Europäischen Parlaments und des Rates vom 9. Juli 2008 über das Visa-Informationssystem (VIS) und den Datenaustausch zwischen den Mitgliedstaaten über Visa für einen kurzfristigen Aufenthalt (VIS-Verordnung; BBl 2009 8823).

Verschiedene Gesetzesbestimmungen sehen die «*Übernahme*» von Daten von einem Informationssystem in ein anderes vor.

Beispiel: Nach Artikel 12 des Bundesgesetzes über das Informationssystem für den Ausländer- und den Asylbereich kann das EJPD die Kantone ermächtigen, gewisse Daten aus dem genannten System in ihre eigenen Systeme zu übernehmen.

Weiter ist die «*Vernetzung*» verschiedener Systeme zu nennen.

Beispiel: Werden gleiche Daten von verschiedenen Stellen der Eidgenössischen Zollverwaltung bearbeitet, so können die entsprechenden Informationssysteme vernetzt werden, sofern dies für eine effiziente Datenbearbeitung notwendig ist (Art. 4 Abs. 2 der Datenbearbeitungsverordnung für die EZV vom 4. April 2007, SR 631.061).

Verschiedene Gesetzesbestimmungen sehen die Schaffung von «*Subsystemen*» oder von in «*Komponenten*» aufgegliederten Systemen vor, insbesondere wo die Zugriffs- und Bearbeitungsrechte der Benutzer beschränkt werden sollen.

Rechtsgrundlage: Art. 4 Abs. 2 DSG.

Beispiel: Die Artikel 2 und 5 der Verordnung über das Informationssystem der Bundeskriminalpolizei (JANUS-Verordnung, SR 360.2) sehen vor, dass das JANUS-System in zehn Subsysteme unterteilt wird. Das EDA wiederum hat sein Informationssystem zur Bearbeitung von Daten über Personaleinsatz und Versetzungen (Tangram) in zwei Komponenten aufgeteilt, die unterschiedliche Zugriffsrechte und Zielsetzungen haben (Art. 4 der Tangram-Verordnung, SR 235.23).

3.2 Ist eine Schnittstelle mit einem System des Bundesarchivs vorgesehen?

Bei der Konzipierung des Systems ist mit dem Bundesarchiv frühzeitig abzuklären, ob Daten abzuliefern sind, damit die erforderlichen technischen Anpassungen des Systems vorgenommen werden können. Für die Archivierung digitaler Daten und Unterlagen im Bundesarchiv besteht ein einheitliches Verfahren (vgl. dazu die Informationen des BAR zur [digitalen Archivierung](#) und Ziff. 10 unten).

Rechtsgrundlagen: Art. 7 des Archivierungsgesetzes (BGA, SR 152.1) und Art. 21 DSG.

4. Inhaber der Datensammlung und allfällige beteiligte Dritte

4.1 Ist der Inhaber der Datensammlung bestimmt?

Der Inhaber der Datensammlung muss genau bestimmt werden. Darunter ist das Bundesorgan zu verstehen, das dafür zu sorgen hat, dass das Informationssystem nur zu den gesetzlichen Zwecken verwendet wird, und das für den Datenschutz insgesamt verantwortlich ist. Als Bundesorgane gelten Behörden und Dienststellen des Bundes sowie Personen, die mit öffentlichen Aufgaben des Bundes betraut sind. Die Bestimmung des Inhabers der Datensammlung ist wichtig, weil das Bundesorgan, das die Personendaten in Erfüllung seiner Aufgaben bearbeitet oder bearbeiten lässt, für den Datenschutz verantwortlich ist, Auskunftsbegehren behandeln muss, die aufgrund des Auskunftsrechts gestellt werden, und Kontrollaufgaben wahrnehmen muss, indem es sich unter anderem vergewissert, dass die im System gespeicherten Daten rechtmässig und in Übereinstimmung mit den datenschutzrechtlichen Anforderungen bearbeitet werden und dass die Informatiksicherheit gewährleistet ist.

Rechtsgrundlagen: Art. 3 Bst. h und i, Art. 8, 9 und Art. 16 Abs. 1 DSG.

Beispiel: Gemäss Art. 5 des Bundesgesetzes über das Informationssystem für den Ausländer- und den Asylbereich (BGIAA, SR 142.51) ist das BFM für die Sicherheit des Informationssystems und die Rechtmässigkeit der Bearbeitung der Personendaten verantwortlich. Gemäss Art. 6 dieses Gesetzes sind Begehren um Auskunft über Personendaten und um Berichtigung an das BFM zu richten und sind auch Beschwerden, die sich nach Art. 25 DSG richten, beim BFM einzureichen.

4.2 Sind Dritte beteiligt?

Es stellt sich die Frage, ob Dritte die Berechtigung erhalten sollen, Daten in das System einzugeben und darin zu ändern, oder – anders ausgedrückt – ob das verantwortliche Bundesorgan zusammen mit anderen Bundesorganen, mit kantonalen Organen oder mit Privaten dem System Daten bearbeiten wird. Ist diese Frage geklärt, können die Rolle und die Verantwortung jedes Beteiligten hinsichtlich Datenschutz genau bestimmt werden.

Rechtsgrundlage: Art. 16 DSG.

Beispiel: Art. 15 BPI sieht vor, dass fedpol in Zusammenarbeit mit den Kantonen ein Personen- und Sachfahndungssystem betreibt.

5. Auskunftsrecht der betroffenen Person

5.1 Wie wird das Auskunftsrecht der betroffenen Person gewährleistet?

Das Auskunftsrecht der betroffenen Person ist ein Grundpfeiler des Datenschutzes. Es ermöglicht ihr, von sich aus zu überprüfen, ob in einem System Daten über sie bearbeitet werden. Die Ausübung dieses Rechts kann insbesondere dazu führen, dass die Widerrechtlichkeit einer Datenbearbeitung festgestellt wird, oder die Berichtigung von Daten nach sich ziehen. Daher ist dem Auskunftsrecht von Anfang an Rechnung zu tragen, indem der Inhaber der Datensammlung, an den sich die betroffene Person zu wenden hat, genau bestimmt wird und das System so gestaltet wird, dass die betroffene Person ihr Auskunftsrecht ausüben kann.

Rechtsgrundlagen: Art. 8, 9 und 25 DSGVO.

Beispiel: Art. 7 BPI unterscheidet Auskunftsbegehren, die an fedpol, an die Bundesanwaltschaft oder an das BFM zu richten sind.

5.2 Sind bestimmte Einschränkungen des Auskunftsrechts vorzusehen?

Grundsätzlich muss ein direktes Auskunftsrecht gewährleistet sein. In Ausnahmefällen sieht die Gesetzgebung in bestimmten Bereichen ein indirektes Auskunftsrecht oder bestimmte Einschränkungen des Auskunftsrechts vor. Somit stellt sich die Frage, ob je nach Bereich solche Einschränkungen des Auskunftsrechts vorzusehen sind, wobei die Entwicklung im jeweiligen Bereich zu berücksichtigen ist. Allgemein geht die Entwicklung dahin, Einschränkungen des Auskunftsrechts in jedem Fall auf das unbedingt Notwendige zu begrenzen (vgl. Stellungnahme des Bundesrates zur *Motion 08.3852 Leutenegger Oberholzer, Datensammlungen des Bundes. Auskunftsrecht*).

Rechtsgrundlage: Art. 9 DSGVO.

Beispiele: Art. 18 des Bundesgesetzes über Massnahmen zur Wahrung der inneren Sicherheit (BWIS, SR 120) sieht ein indirektes Auskunftsrecht vor. Art. 8 BPI sieht spezifische Einschränkungen des Auskunftsrechts beim System Bundesdelikte vor.

6. Zugriff im Abrufverfahren (Online-Zugriff)

6.1 Sind Online-Zugriffe vorzusehen?

Vor der Schaffung einer Rechtsgrundlage ist zu klären, ob der Datenempfänger auf einen Online-Zugriff angewiesen ist, um seine gesetzlichen Aufgaben erfüllen zu können. Rein praktische Gründe rechtfertigen keinen Online-Zugriff. Bei der Gewährung eines Online-Zugriffs ist Zurückhaltung angebracht, vor allem wenn der Zweck des Systems sich vom Zweck, den die künftigen Empfänger verfolgen werden, stark unterscheidet. Gegebenenfalls ist der Zugriff soweit möglich auf unverzichtbare Daten zu begrenzen. Somit sind auch andere Arten der Datenbekanntgabe als der Zugang mittels Abrufverfahren in Betracht zu ziehen. Zu nennen sind die Bekanntgabe von Dokumenten in Papierform, die im Einzelfall beantragt wird (Amtshilfe) oder von Amts wegen erforderlich ist, oder die elektronische Übermittlung bestimmter Daten, die nicht mittels Abrufverfahren, d. h. nicht nach dem Selbstbedienungsprinzip, erfolgt.

Beispielsweise enthält die Weisung des EJPD über die Einrichtung von Online-Verbindungen und die Erteilung von Zugriffsbewilligungen auf Informatikanwendungen des EJPD (Online-Weisung EJPD) vom 30. September 2004 strenge Voraussetzungen für die Einrichtung von Online-Verbindungen.

Rechtsgrundlagen: Art. 4 Abs. 2 und Art. 19 Abs. 3 DSG.

Beispiele: Gemäss Art. 9 BGIAA kann das Bundesamt für Migration bestimmten Behörden (z. B. dem Grenzwachtkorps) Daten des Ausländerbereichs für einen bestimmten Zweck (z. B. damit die Grenzwächter Personenkontrollen durchführen und Ausnahmevisa erteilen können) durch ein Abrufverfahren zugänglich machen. Gemäss Art. 13 BGIAA kann das BFM bestimmten im Gesetz genannten Behörden oder durch das Gesetz beauftragten Dritten Daten in Form von elektronischen Datensätzen oder Listen bekannt geben. Gemäss Art. 14 BGIAA kann das BFM im Einzelfall Personendaten auf schriftliches und begründetes Gesuch der Behörde, welche die Daten benötigt, bekannt geben.

6.2 Stünde der Online-Zugriff im Widerspruch zu wesentlichen öffentlichen Interessen oder offensichtlich schutzwürdigen Interessen einer betroffenen Person?

Wird die Einrichtung eines Online-Zugriffs in Betracht gezogen, so muss geprüft werden, ob dieser im Widerspruch zu wesentlichen öffentlichen Interessen oder offensichtlich schutzwürdigen Interessen einer betroffenen Person stünde.

Rechtsgrundlagen: Art. 4 Abs. 2 und Art. 19 Abs. 3 und 4 Bst. a DSG.

6.3 Stünde der Online-Zugriff im Widerspruch zu einer gesetzlichen Geheimhaltungspflicht oder besonderen Datenschutzvorschriften?

Es ist zu prüfen, ob der geplante Online-Zugriff im Widerspruch zu einer gesetzlichen Geheimhaltungspflicht oder zu besonderen Datenschutzvorschriften stünde, derentwegen es die Bekanntgabe von Daten im Einzelfall ablehnen oder begrenzen müsste. In jedem einzelnen Bereich ist somit zu klären, ob besondere Bestimmungen gelten.

Rechtsgrundlage: Art. 19 Abs. 3 und 4 Bst. b DSG.

Beispiel: Mit Art. 33 des Bundesgesetzes über den Allgemeinen Teil des Sozialversicherungsrechts (ATSG, SR 830.1) wird Personen, die an der Durchführung der Sozialversicherungsgesetze beteiligt sind, eine Schweigepflicht auferlegt.

7. Richtigkeit der Daten

7.1 Sind Massnahmen zur Kontrolle der Richtigkeit der Daten vorgesehen?

Das verantwortliche Bundesorgan hat sich zu vergewissern, dass die Daten, die es in dem System bearbeitet, korrekt sind. Zudem muss es den Nachweis für die Richtigkeit der in dem System bearbeiteten Daten erbringen, wenn diese bestritten wird. Deshalb sind, in Zusammenarbeit mit den zuständigen Informatikern und Informatikerinnen, geeignete Massnahmen

festzulegen, die getroffen werden können, um unrichtige oder unvollständige Daten zu löschen oder zu berichtigen.

Rechtsgrundlage: Art. 5 DSGVO.

Beispiele: Art. 16 der Verordnung über das Zentrale Migrationsinformationssystem (ZEMIS-Verordnung, SR 142.513) sieht vor, dass das BFM eine Datenschutz- und Informatiksicherheitsberatung bezeichnet, die regelmässig die Datenrichtigkeit und die Datensicherheit überprüft. Art. 15 der JANUS-Verordnung weist dem Kontrolldienst unter anderem die Aufgabe zu, die endgültige Aufnahme der provisorisch erfassten Daten zu bestätigen, nachdem er deren Richtigkeit überprüft hat. Ausserdem befasste sich die Eidgenössische Datenschutzkommission in ihrem Entscheid vom 7. April 2003 (VPB 67.73 E. 4c) mit einem Fall, in dem die Richtigkeit von Daten in einem Informationssystem vom betroffenen Asylsuchenden bestritten wurde und vom verantwortlichen Bundesorgan nicht nachgewiesen werden konnte.

8. Datensicherheit

8.1 Sind technische und organisatorische Massnahmen vorgesehen, um die Datensicherheit zu gewährleisten?

Das verantwortliche Bundesorgan muss bereits bei der Konzipierung des Systems mit dem zuständigen Informatikstrategieorgan Bund zusammenarbeiten, um die erforderlichen technischen und organisatorischen Massnahmen zum Schutz der Personendaten zu treffen. Zudem muss es sein Projekt dem Eidgenössischen Datenschutz- und Öffentlichkeitsbeauftragten oder dem Datenschutzverantwortlichen, den es gegebenenfalls bezeichnet hat, melden.

Diese Massnahmen müssen insbesondere dem Zweck der Datenbearbeitung, der Art und dem Umfang der Datenbearbeitung, der Einschätzung der möglichen Risiken für die betroffenen Personen und dem gegenwärtigen Stand der Technik Rechnung tragen.

Die vorgesehenen Massnahmen müssen das System insbesondere gegen folgende Risiken schützen:

- unbefugte oder zufällige Vernichtung;
- zufälligen Verlust;
- technische Fehler;
- Fälschung, Diebstahl oder widerrechtliche Verwendung;
- unbefugtes Zugreifen, Ändern, Kopieren oder andere unbefugte Bearbeitungen.

Rechtsgrundlagen: Art. 7 DSGVO; Art. 8 und 20 der Verordnung zum Bundesgesetz über den Datenschutz (VDSG, SR 235.11).

8.2 Sind besondere Massnahmen vorgesehen, um die Datensicherheit zu gewährleisten?

Da das verantwortliche Bundesorgan ein System zur automatisierten Bearbeitung von Personendaten einrichten will, muss es besondere Massnahmen vorsehen, um namentlich folgenden Zielen gerecht zu werden:

- Zugangskontrolle;
- Personendatenträgerkontrolle;

- Transportkontrolle;
- Bekanntgabekontrolle;
- Speicherkontrolle;
- Benutzerkontrolle;
- Zugriffskontrolle;
- Eingabekontrolle.

Das System ist so zu gestalten, dass die betroffenen Personen ihr Auskunftsrecht und ihr Recht auf Berichtigung wahrnehmen können.

Rechtsgrundlagen: Art. 5 Abs. 2 DSG; Art. 9 VDSG.

8.3 Muss ein Protokollierungsprozess eingerichtet werden?

Das verantwortliche Bundesorgan muss einen Prozess zur Protokollierung der automatisierten Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen vorsehen, wenn die präventiven Massnahmen den Datenschutz nicht gewährleisten können. Eine Protokollierung hat bei einem komplexen System 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. Eine Protokollierung kann je nach Bereich auch aufgrund eines internationalen Vertrags erforderlich sein.

Rechtsgrundlagen: Art. 10 VDSG. Im Bereich der polizeilichen Zusammenarbeit besteht mit Art. 10 des Rahmenbeschlusses über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden (ABl. L 350/60 vom 30.12.2008), eine direkt anwendbare Bestimmung über die Protokollierung.

Beispiel: Art. 27 der JANUS-Verordnung sieht vor, dass jede Bearbeitung von Daten im JANUS in einem Protokoll festzuhalten ist und dass die Protokolle ein Jahr lang aufzubewahren sind.

9. Aufgaben des Systemadministrators, der Kontroll- und Wartungsdienste

9.1 Sind die Aufgaben des Systemadministrators, der Kontroll- und Wartungsdienste definiert?

Der Umfang des Systemzugriffs des Systemadministrators, der Kontroll- und Wartungsdienste ist vorgängig zu klären. Er muss verhältnismässig sein.

Hinweis: Zu gegebener Zeit wird zu untersuchen sein, ob die Fragen der internen Kontrolle und der Wartungsdienste eines Informationssystems künftig in allgemeinen Bestimmungen der Datenschutzgesetzgebung geregelt werden sollten.

Rechtsgrundlage: Art. 4 Abs. 2 DSG.

Beispiel: Art. 5 BPI unterscheidet den Zugriff der verwaltungsinternen Kontrolldienste, denen die Überprüfung der Einhaltung der Datenschutzvorschriften obliegt, vom Zugriff der mit Wartungs- und Programmierungsarbeiten betrauten Personen. Für Letztere ist die Datenbearbeitung insbesondere an die Bedingung geknüpft, dass die Bearbeitung zur Erfüllung ihrer Wartungs- und Programmierungsarbeiten unbedingt erforderlich ist.

10. Archivierung der Daten

10.1 Wird das System möglicherweise archivwürdige Personendaten enthalten?

Es ist zu klären, ob die Daten, welche bearbeitet werden sollen, archivwürdig sein könnten und ob sie dem Bundesarchiv anzubieten sind, wenn das Bundesorgan sie nicht mehr ständig benötigt. Diese Überprüfung ist in Zusammenarbeit mit dem Bundesarchiv vorzunehmen, das über die erforderlichen Ressourcen und Kenntnisse verfügt, um die Archivwürdigkeit der Daten zu beurteilen und bei allen technischen Fragen im Zusammenhang mit der Datenarchivierung Unterstützung zu bieten. Diese Zusammenarbeit trägt dazu bei, die tägliche Verwaltung der Daten zu erleichtern. Damit lässt sich ein zusätzlicher Arbeitsaufwand für die spätere Archivierung der Daten vermeiden.

Rechtsgrundlagen: Art. 21 DSGVO und Art. 7 BGA.

10.2 Ist ein Archivierungsprozess vorgesehen?

Das verantwortliche Bundesorgan muss dem Bundesarchiv alle Personendaten anbieten, die es nicht mehr ständig benötigt.

Bei der Einrichtung eines neuen Systems müssen die Juristinnen und Informatiker des verantwortlichen Bundesorgans einen Archivierungsprozess festlegen, der insbesondere den folgenden Fragen Rechnung trägt: Welche technischen Massnahmen sind vorgesehen, um dem Bundesarchiv später Personendaten abzuliefern? Ist eine Schnittstelle mit dem System des Bundesarchivs vorgesehen? Wann und wie häufig müssen ihm diese Daten angeboten werden? Welche Daten sind anzubieten, und wie sind sie anzubieten?

Die Einrichtung eines Archivierungsprozesses ist besonders wichtig bei einer Migration der Daten von einem alten in ein neues System. In einem solchen Fall muss der Archivierungsprozess vor der Inbetriebnahme des neuen Systems stattfinden. Die Möglichkeit, dass die Daten eines Tages für das verantwortliche Bundesorgan erneut von Nutzen sein könnten, entbindet dieses nicht von der Verpflichtung, einen Archivierungsprozess vorzusehen.

Hinweis: Zu gegebener Zeit wird zu untersuchen sein, ob der Archivierungsprozess künftig in allgemeinen Bestimmungen der Gesetzgebung über den Datenschutz oder die Archivierung geregelt werden sollte.

Rechtsgrundlagen: Art. 7 BGA und Art. 21 Abs. 1 DSGVO; Weisungen vom 13. Juli 1999 über die Aktenführung in der Bundesverwaltung, BBl 1999 5428.

11. Verwaltung, Dauer der Aufbewahrung und Vernichtung der Daten

11.1 Lassen sich mit dem vorgesehenen System die Vorschriften über die elektronische Geschäftsverwaltung (GEVER) einhalten?

Gemäss dem Beschluss des Bundesrates vom 23. Januar 2008 müssen die Bundeskanzlei und die Departemente bis Ende 2011 die elektronische Geschäftsverwaltung (GEVER) einführen (siehe oben, S. 1). Im Hinblick darauf bietet das Bundesarchiv mehrere Informationsmittel an, insbesondere auch den Führungsleitfaden Geschäftsverwaltung.

Rechtsgrundlagen: Art. 22 der Verordnung vom 22. November 1998 über die Regierungs- und Verwaltungsorganisation (RVOV, SR 172.010.1); Weisungen vom 13. Juli 1999 über die Aktenführung in der Bundesverwaltung (s.o. Ziffer 10.2).

11.2 Ist eine Aufbewahrungsfrist vorgesehen?

Die Dauer der Aufbewahrung von Personendaten muss verhältnismässig sein. Eine lange Aufbewahrungsdauer liesse sich nicht dadurch rechtfertigen, dass die Personendaten eines Tages für das verantwortliche Bundesorgan erneut von Nutzen sein könnten. Die Aufbewahrungsdauer variiert je nach Kategorie der bearbeiteten Daten, weshalb das System so zu gestalten ist, dass mehrere Aufbewahrungsdauern vorgesehen werden können, beispielsweise durch die Schaffung von Subsystemen.

Rechtsgrundlage: Art. 4 Abs. 2 DSG.

Beispiele: Art. 45 Abs. 2 der Verordnung über den nationalen Teil des Schengener Informationssystems (N-SIS) und das SIRENE-Büro (N-SIS-Verordnung, SR 362.0) sieht vor, dass bestimmte Informationen spätestens ein Jahr nach der Löschung der zugehörigen Ausschreibung der betroffenen Person im SIS gelöscht werden. Art. 6 BPI sieht für die Löschung der Daten verschiedene Verfahren vor, je nachdem ob es sich um einzelne Einträge oder um miteinander verknüpfte Daten handelt, die als Block gelöscht werden. Darin werden Aufbewahrung, Löschung, Archivierung und Vernichtung der Daten unterschieden.

11.3 Ist ein Prozess zur Vernichtung der Daten vorgesehen?

Erachtet das Bundesarchiv die vom verantwortlichen Bundesorgan angebotenen Personendaten als nicht archivwürdig, muss das Bundesorgan diese vernichten, ausser wenn sie anonymisiert sind oder zu Beweis- oder Sicherheitszwecken aufbewahrt werden müssen.

Rechtsgrundlage: Art. 21 Abs. 2 DSG.

Beispiel: Nach Artikel 6 Absatz 5 BPI müssen zur Löschung bestimmte Daten und die dazugehörigen Unterlagen dem Bundesarchiv zur Archivierung angeboten werden; vom Bundesarchiv als nicht archivwürdig beurteilte Daten und Unterlagen werden vernichtet.

12. Checkliste der Fragestellungen beim Konzipieren des Systems

Die nachstehende Checkliste fasst die vorangehenden Abschnitte zusammen und ermöglicht eine rasche Überprüfung, ob sämtliche Probleme gelöst sind.

1. Dateneigenschaften	
1.1 Werden Personendaten bearbeitet?	<input type="checkbox"/> Nein -> DSGVO nicht anwendbar <input type="checkbox"/> Ja
1.2. Werden besonders schützenswerte Personendaten oder Persönlichkeitsprofile bearbeitet?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
1.3 Wurde die Schwere der Persönlichkeitsverletzung geprüft?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
2. Zweck des Systems	
2.1 Ist der allgemeine Zweck des Systems bestimmt?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
2.2 Handelt es sich um ein internes Geschäftsverwaltungssystem oder um ein Informationssystem mit Abrufverfahren?	<input type="checkbox"/> internes Geschäftsverwaltungssystem <input type="checkbox"/> Informationssystem mit Abrufverfahren
3. Architektur des Informatiksystems	
3.1 Sind die Architektur des Informatiksystems und seine Möglichkeiten klar definiert?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
3.2 Ist eine Schnittstelle mit einem System des Bundesarchivs vorgesehen?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
4. Inhaber der Datensammlung und allfällige beteiligte Dritte	
4.1 Ist der Inhaber der Datensammlung bestimmt?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
4.2 Sind Dritte beteiligt?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
5. Auskunftsrecht der betroffenen Person	
5.1 Wie wird das Auskunftsrecht der betroffenen Person gewährleistet?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
5.2 Sind bestimmte Einschränkungen des Auskunftsrechts vorzusehen?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja

6. Zugriff im Abrufverfahren (Online-Zugriff)	
6.1 Sind Online-Zugriffe vorzusehen?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
6.2 Stünde der Online-Zugriff im Widerspruch zu wesentlichen öffentlichen Interessen oder offensichtlich schutzwürdigen Interessen einer betroffenen Person?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
6.3 Stünde der Online-Zugriff im Widerspruch zu einer gesetzlichen Geheimhaltungspflicht oder besonderen Datenschutzvorschriften?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
7. Richtigkeit der Daten	
7.1 Sind Massnahmen zur Kontrolle der Richtigkeit der Daten vorgesehen?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
8. Datensicherheit	
8.1 Sind technische und organisatorische Massnahmen vorgesehen, um die Datensicherheit zu gewährleisten?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja, gegen folgende Risiken: <ul style="list-style-type: none"> <input type="checkbox"/> unbefugte oder zufällige Vernichtung; <input type="checkbox"/> zufälligen Verlust; <input type="checkbox"/> technische Fehler; <input type="checkbox"/> Fälschung, Diebstahl oder widerrechtliche Verwendung; <input type="checkbox"/> unbefugtes Zugreifen, Ändern, Kopieren oder andere unbefugte Bearbeitungen; <input type="checkbox"/> andere Risiken.
8.2 Sind besondere Massnahmen vorgesehen, um die Datensicherheit zu gewährleisten?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja, mit folgenden Zielen: <ul style="list-style-type: none"> <input type="checkbox"/> Zugangskontrolle; <input type="checkbox"/> Personendatenträgerkontrolle; <input type="checkbox"/> Transportkontrolle; <input type="checkbox"/> Bekanntgabekontrolle; <input type="checkbox"/> Speicherkontrolle; <input type="checkbox"/> Benutzerkontrolle; <input type="checkbox"/> Zugriffskontrolle; <input type="checkbox"/> Eingabekontrolle; <input type="checkbox"/> andere Ziele.
8.3 Muss ein Protokollierungsprozess eingerichtet werden?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja

9. Aufgaben des Systemadministrators, der Kontroll- und Wartungsdienste	
9.1 Sind die Aufgaben des Systemadministrators, der Kontroll- und Wartungsdienste definiert?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
10 Archivierung der Daten	
10.1 Wird das System möglicherweise archivwürdige Personendaten enthalten?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
10.2 Ist ein Archivierungsprozess vorgesehen?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
11. Verwaltung, Dauer der Aufbewahrung und Vernichtung der Daten	
11.1 Lassen sich mit dem vorgesehenen System die Vorschriften über die elektronische Geschäftsverwaltung (GEVER) einhalten?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
11.2 Ist eine Aufbewahrungsfrist vorgesehen?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja
11.3 Ist ein Prozess zur Vernichtung der Daten vorgesehen?	<input type="checkbox"/> Nein <input type="checkbox"/> Ja

Erst in diesem Stadium kann man sich der Frage zuwenden, was in einem Gesetz im formellen Sinn behandelt werden muss und was in einer Rechtsgrundlage im materiellen Sinn behandelt werden kann.

B. Normkonzept

Bevor der Entwurf eines Gesetzes über den Betrieb eines Systems zur automatisierten Bearbeitung von Personendaten verfasst werden kann, ist ein Normkonzept zu erarbeiten.

Vgl. → [Ein Normkonzept erarbeiten](#) (Modul Gesetz) und die [Weisung betreffend die Unterbreitung von Normkonzepten für Gesetzgebungsvorhaben des Bundesamtes für Justiz](#).

Da es sich um einen ausgesprochen technischen Bereich handelt, wird im Folgenden auf die einzelnen Rubriken des Normkonzepts näher eingegangen.

1. Zusammenfassung der Inhalte des Erlasses

In der Zusammenfassung der Inhalte des Rechtserlasses werden insbesondere die Identität des Inhabers der Datensammlung, der Zweck des Systems, das Auskunftsrecht der betroffenen Person, die Art der Bearbeitung, die Art der Daten und etwaige Zugriffe im Abrufverfahren (Online-Zugriffe) festgelegt. Es handelt sich somit um eine Zusammenfassung der Antworten auf die im ersten Teil dieser Anleitung formulierten Fragen.

2. Grobstruktur des Erlasses

Die Grobstruktur des Erlasses, der den Betrieb eines Informationssystems regelt, muss insbesondere folgende Unterteilungen aufweisen: allgemeine Bestimmungen, in denen vor allem auch der Zweck des Systems und dessen Architektur festgelegt werden, die Bearbeitung von Personendaten, der Zugang durch ein Abrufverfahren und die Bekanntgabe von Personendaten.

3. Erlassform

Die geeignete Erlassform ist zu bestimmen, indem insbesondere geklärt wird, ob ein neuer Erlass geschaffen oder ein bereits bestehender Erlass geändert werden soll.

In diesem Stadium stellt sich auch die Frage, ob ein Erlasstext ausgearbeitet werden soll, der sich ausschliesslich auf Informationssysteme bezieht, oder ob die erforderlichen Bestimmungen in einen Erlass eingefügt werden können, der den betreffenden Bereich regelt. Es ist jedoch darauf zu achten, dass ein Gesetz durch das Einfügen einer Reihe von Bestimmungen über ein Informationssystem nicht aus dem Gleichgewicht gerät. Gegebenenfalls empfiehlt es sich, den Betrieb des Informationssystems in einem separaten Gesetz zu regeln.

Beispiele: Das Bundesgesetz über das Informationssystem für den Ausländer- und den Asylbereich ist ein separater Erlass, ebenso das Bundesgesetz über die militärischen Informationssysteme (BBI 2008 7505).

4. Normstufe und normativer Inhalt

Grundsätzlich darf ein Bundesorgan Personendaten nur bearbeiten und bekannt geben, wenn dafür eine Rechtsgrundlage besteht (Art. 17 Abs. 1 und Art. 19 Abs. 1 DSG). Eine formellgesetzliche Grundlage ist erforderlich, wenn es um besonders schützenswerte Daten und Persönlichkeitsprofile geht (Art. 17 Abs. 2 DSG). Macht das Bundesorgan Personendaten durch ein Abrufverfahren zugänglich, ist stets eine gesetzliche Grundlage erforderlich. Bei besonders schützenswerten Personendaten und Persönlichkeitsprofilen muss dies in einem formellen Gesetz ausdrücklich vorgesehen sein (Art. 19 Abs. 3 DSG). Beabsichtigt das Bundesorgan keine Bearbeitung von besonders schützenswerten Daten oder Persönlichkeitsprofilen und auch keinen Zugriff im Abrufverfahren für diese Art von Daten, genügt grundsätzlich ein materielles Gesetz. Die Normstufe hängt auch davon ab, wie schwer die Persönlichkeit der betroffenen Personen verletzt wird.

Betreibt ein Bundesorgan ein internes Geschäftsverwaltungssystem, gilt dafür Art. 57h RVOG als Rechtsgrundlage.

Eine formellgesetzliche Grundlage für die Bearbeitung von besonders schützenswerten Personendaten und Persönlichkeitsprofilen sowie den Online-Zugriff darauf muss im Wesentlichen Antwort auf die folgenden Fragen geben:

- Wer bearbeitet welche Datenkategorien zu welchem Zweck?
- Wer hat Zugriff auf welche Datenkategorien und zu welchem Zweck?

4.1 Inhalt eines formellen Gesetzes

Das formelle Gesetz muss insbesondere Folgendes regeln:

- Der Zweck des Systems muss so umschrieben werden, dass er für die betroffenen Personen genau erkennbar ist. Je schwerer die Eingriffe in die Persönlichkeitsrechte sein können, umso höher muss der Detailgrad sein. Unabhängig von der Natur der bearbeiteten Daten genügt es nicht, anzugeben, der Zweck des Systems bestehe darin, dem verantwortlichen Bundesorgan die Erfüllung seiner gesetzlichen Aufgaben zu ermöglichen. Vielmehr müssen die Aufgaben aufgezählt werden, für welche eine automatische Datenbearbeitung vorgesehen ist (vgl. oben Ziff. 2.1).
Beispiel: Art. 3 BGIAA.
- Identität des Inhabers der Datensammlung: In der gesetzlichen Bestimmung muss angegeben sein, welches Bundesorgan für die Sicherheit des Systems und die Rechtmässigkeit der Datenbearbeitung verantwortlich ist. Dieser Angabe muss die betroffene Person entnehmen können, bei welcher Behörde sie ihre Rechte, insbesondere ihr Auskunftsrecht, geltend machen kann.
Beispiele: Art. 2 und 5 BGIAA.
- Beteiligte Dritte: Diese müssen für die betroffene Person erkennbar sein.
Beispiel: Art. 15 BPI.
- Inhalt des Informationssystems: Die Kategorien der bearbeiteten Daten müssen definiert sein. Klarzustellen ist auch, ob das System besonders schützenswerte Personendaten oder Persönlichkeitsprofile enthält.
Beispiel: Art. 4 BGIAA.
- Kategorien von besonders schützenswerten Personendaten und Persönlichkeitsprofile: In der gesetzlichen Bestimmung sind die für die Datenbearbeitung in dem System zuständige(n) Behörde(n), die Kategorien der bearbeiteten Daten und der Zweck der Bearbeitung anzugeben. Daraus muss die betroffene Person entnehmen können, welche Behörde zuständig ist, welche Daten über sie bearbeitet wurden und zu welchem Zweck die Bearbeitung vorgenommen wurde.
Beispiele: Art. 4 und 5 BPI.
- Allfällige Einschränkungen des Auskunftsrechts der betroffenen Person: Die vorgesehenen Einschränkungen müssen durch ein überwiegendes öffentliches oder privates Interesse gerechtfertigt und verhältnismässig sein.
Beispiel: Art. 8 BPI.
- Architektur des Informatiksystems: Diese muss in ihren Grundzügen beschrieben sein. Aus der gesetzlichen Bestimmung muss für die betroffene Person ersichtlich sein, wie das System aufgebaut ist, ob Subsysteme oder Schnittstellen mit anderen Systemen bestehen.
Beispiel: Art. 9 BPI.
- Zugriff im Abrufverfahren: In der gesetzlichen Bestimmung ist festzulegen, welches Bundesorgan für die Gewährung eines Zugriffs im Abrufverfahren zuständig ist und welchen Behörden ein solcher Zugriff gewährt werden kann. Zudem ist anzugeben, welche Kategorien von Daten durch ein Abrufverfahren zugänglich sind und welchem Zweck dieser Zugang dient. Für die betroffene Person muss klar ersichtlich sein, welche Daten über sie durch ein Abrufverfahren zugänglich sind, welchen Kategorien von Empfängern und zu welchem Zweck sie zugänglich sind. Der Grundsatz der Verhältnismässigkeit ist zu wahren. Ein Zugriff mittels Abrufverfahren darf nicht nur deshalb gewährt werden, weil er für

eine Behörde nützlich sein könnte. Er muss für die Erfüllung ihrer gesetzlichen Aufgaben erforderlich sein.

Beispiele: Art. 9–11 BGIAA.

- Bekanntgabe von besonders schützenswerten Personendaten und Persönlichkeitsprofilen: In der gesetzlichen Bestimmung ist festzulegen, welches Bundesorgan für die Bekanntgabe der Daten zuständig ist und welchen Behörden die Daten bekannt gegeben werden dürfen. Zudem sind die Datenkategorien und der Zweck der Bekanntgabe anzugeben. In der gesetzlichen Bestimmung ist auch zu präzisieren, ob es sich um eine unaufgeforderte Bekanntgabe oder um eine Bekanntgabe auf Antrag handelt. Der Grundsatz der Verhältnismässigkeit ist zu wahren. So dürfen nur die Daten bekannt gegeben werden, welche die empfangende Behörde zur Erfüllung ihrer gesetzlichen Aufgaben benötigt.

Beispiele: Art. 12–15 BGIAA.

- Rechtsetzungsdelegation, durch die der Bundesrat ermächtigt wird, Primärnormen zu erlassen: Die gesetzliche Bestimmung muss eine klare Rechtsetzungsdelegation an den Bundesrat vorsehen. Darin sind Zweck, Gegenstand und Umfang der Delegation festzulegen. Von dieser Möglichkeit ist zurückhaltend Gebrauch zu machen.

Beispiel: Art. 17 BGIAA.

4.2 Inhalt eines materiellen Gesetzes

Je nach der vorgesehenen Rechtsetzungsdelegation sind insbesondere folgende Punkte in einer Verordnung zu regeln:

- Genauere Angaben zur Architektur des Informationssystems (vgl. oben Ziff. 3.1; es müssen nicht die technischen Details geregelt werden, sondern die Art und Weise der Datenbearbeitung sowie die allfälligen Verbindungen zwischen verschiedenen Systemen).

Beispiel: Art. 3 der Verordnung ZEMIS.

- Katalog der im System bearbeiteten Daten.

Beispiel: Art. 4 der ZEMIS-Verordnung.

- Einzelheiten der Verantwortlichkeit des verantwortlichen Bundesorgans für den Datenschutz, gegebenenfalls die Verantwortlichkeit beteiligter Dritter oder sogar die Verpflichtung des Inhabers der Datensammlung, ein Bearbeitungsreglement im Sinne von Art. 21 VDSG zu erstellen.

Beispiel: Art. 7 der N-SIS-Verordnung.

- Modalitäten des Zugriffs mittels Abrufverfahren, einschliesslich der genauen Bezeichnung der Behörden, die auf die Informationssysteme Zugriff haben.

Beispiel: Art. 7 der N-SIS-Verordnung.

- Modalitäten der Bekanntgabe bestimmter Daten ohne Abrufverfahren.

Beispiel: Art. 9 und 10 der Asylverordnung 3 über die Bearbeitung von Personendaten (SR 142.314).

- Modalitäten der Ausübung des Auskunftsrechts der betroffenen Person.

Beispiel: Art. 19 der ZEMIS-Verordnung.

- Technische und organisatorische Schutzmassnahmen.

Beispiel: Art. 16 und 17 der ZEMIS-Verordnung.

- Fristen für die Aufbewahrung, Archivierung und Vernichtung der Daten.

Beispiel: Art. 18 der ZEMIS-Verordnung.