



Erläuterungen zur Verordnung über den Datenmarkt (DMV, SG Ziffer)

1. Ausgangslage

Zweck des Datenmarkts der kantonalen Verwaltung ist es, öffentlichen Organen tagesaktuell Daten auf einer zentralen Plattform zur Verfügung zu stellen. Aktuell ist dieser in der Verordnung über den Datenmarkt vom 12. Juli 2005 (SG 153.310) geregelt. Beim Datenmarkt handelt es sich um einen Datenpool gemäss § 1a der Informations- und Datenschutzverordnung (IDV) vom 9. August 2011 (SG 153.270).

Gestützt auf den Beschluss des Regierungsrates vom 11. Februar 2014 wurde in der Informations- und Datenschutzverordnung (IDV) eine Bestimmung über die Vorgaben der rechtlichen Grundlagen von Datenpools aufgenommen. Darüber hinaus ist vorgesehen, im Informations- und Datenschutzgesetz (IDG) vom 9. Juni 2010 (SG 153.260) eine gesetzliche Grundlage für die interne Verwendung einer Personenidentifikationsnummer (Personen-ID) für den Austausch und die Verknüpfung von Personendaten zwischen und innerhalb von öffentlichen Organen zu schaffen. Der Entwurf dieser gesetzlichen Grundlage sieht vor, dass eine zentrale Stelle die Personen-ID zuweist und dass die zuständige Stelle die Vorgaben für die korrekte Verwendung der Personen-ID festlegt und deren Einhaltung kontrolliert.

Mit dem vorliegenden Entwurf einer totalrevidierten Verordnung über den Datenmarkt werden die genannten Vorgaben der IDV und des IDG umgesetzt. Im Zentrum der Revision gestützt auf die IDV stehen die Bezeichnung des Inhalts des Datenpools gemäss § 1b Abs. 3 lit. b IDV sowie die Bezeichnung des verantwortlichen Organs und dessen Aufgaben gemäss § 1b Abs. 3 lit. c IDV. Ausserdem werden vor allem aufgrund der technischen Entwicklung im Bereich der Informatik überholte Bestimmungen an die aktuellen Gegebenheiten angepasst.

2. Erläuterungen zu den einzelnen Bestimmungen

§ 1. Gegenstand

Die Verordnung regelt Organisation, Betrieb und Weiterentwicklung des Datenmarktes der kantonalen Verwaltung.

Erläuterungen zu § 1 Gegenstand

Gemäss § 1b Abs. 2 IDV wurde neben dem Betrieb des Datenmarktes dessen Organisation aufgenommen. Darüber hinaus wird neu auch die Weiterentwicklung des Datenmarktes erwähnt. Die Weiterentwicklung bezieht sich auf die Entwicklung neuer Funktionalitäten (vgl. auch Kommentar zu § 6 Abs. 1 lit. b).

§ 2. Zweck und Inhalt des Datenmarkts

Im Datenmarkt werden den öffentlichen Organen gemäss § 3 Abs. 1 IDG Personen- und Sachdaten, die von mehr als einem öffentlichen Organ zur Erfüllung seiner gesetzlichen Aufgaben benö-

tigt werden, tagesaktuell auf einer zentralen Plattform zur Verfügung gestellt.

Erläuterungen zu § 2 Zweck und Inhalt des Datenmarkts

Öffentliche Organe gemäss § 3 Abs. 1 IDG sind: die Organisationseinheiten des Kantons und der Gemeinden, die eine öffentliche Aufgabe erfüllen (lit. a), die Organisationseinheiten der juristischen Personen des kantonalen und kommunalen öffentlichen Rechts, die eine öffentliche Aufgabe erfüllen (lit. b) sowie Private, soweit ihnen von Kanton oder Gemeinden die Erfüllung öffentlicher Aufgaben übertragen ist (lit. c). Ein Beispiel für lit. c ist die Krebsliga beider Basel, welche für den Kanton Basel-Stadt ein Mammografie-Screening-Programm durchführt.

Personendaten zeichnen sich im Unterschied zu Sachdaten dadurch aus, dass sie einen Bezug zu einer oder mehreren Personen aufweisen und diese Personen bestimmt oder bestimmbar sind. Die Daten im kantonalen Datenmarkt umfassen insbesondere: Steuerdaten, Erbschaftsdaten, Betreibungsdaten, MFK-Daten, Sozialdaten, Verwendungsnachweise (wer bezieht welche Daten), Gebäudedaten, bspw. Gebäudemodell, sowie Grundbuchdaten. Der Ersatz von „Personen-, Gebäude- und Grundstücksdaten sowie weiteren personenbezogenen Daten aus anderen Datensammlungen“ gemäss § 2 der geltenden Verordnung über den Datenmarkt vom 12. Juli 2005 durch „Personen- und Sachdaten“ trägt dem Umstand Rechnung, dass auch personenbezogene Daten Personendaten sind. Inhaltlich ist keine Änderung damit verbunden.

Im Datenmarkt wird sichergestellt, dass die betroffenen Daten gemäss den gesetzlichen Grundlagen, insbesondere dem IDG, und den Anforderungen der IKT Basis Services gehalten und ausgetauscht werden. Zudem wird sichergestellt, dass die Bewirtschaftungssysteme gemäss den vorab erwähnten Rahmenbedingungen verfügbar sind und die Voraussetzungen für die vorgesehene Nutzung im technischen und funktionalen Umfang erfüllen. Bei Abweichungen zwischen dem Datenbestand des Datenmarkts und jenem in der Fachanwendung gelten stets diejenigen des Fachamts. Bei inhaltlichen Erweiterungen des Datenmarkts sind die dateneinliefernden Stellen einzubeziehen.

Die kantonale Geodateninfrastruktur ergänzt den kantonalen Datenmarkt. Gemäss § 10 Geoinformationsverordnung (SG 214.305) sind Geobasisdaten an die Geodateninfrastruktur zu liefern.

§ 3. Gesamtverantwortung

¹ Die Konferenz für Organisation und Informatik (KOI) trägt als Vertreterin der dateneinliefernden Organe die Verantwortung für den kantonalen Datenmarkt.

² Die KOI koordiniert die Nutzung des Gesamtsystems und erlässt Vorgaben für die Nutzung.

³ Die KOI hat insbesondere folgende Aufgaben:

- a) Festlegung der Anforderungen, welche das Gesamtsystem erfüllen muss und Sicherstellung der Einhaltung dieser Anforderungen;
- b) Festlegung der Qualitätsstandards;
- c) Sicherstellung des Verfahrens zur Vernichtung von Daten;
- d) Festlegung des vorzuhaltenden Schutzes des Gesamtsystems;
- e) Risikomanagement;
- f) Sicherstellung der Gewährleistung der Rechte der betroffenen Personen;
- g) Sicherstellung der Berücksichtigung von Sperrcodes;
- h) Sicherstellung, dass allen Daten eine Dateneignerin oder ein Dateneigner zugewiesen wird;
- i) Sicherstellung eines bedarfsgerechten Abrufverfahrens;
- j) Sicherstellung der Einhaltung der Rechte und Pflichten der Dateneignerin oder des Dateneigners.

Erläuterungen zu § 3 Gesamtverantwortung

§ 3 Abs. 1

Die zentrale Plattform steht den öffentlichen Organen gemäss § 3 Abs. 1 IDG (vgl. Kommentar zu § 2 DMV) zur Verfügung. Vor diesem Hintergrund soll die Gesamtverantwortung für den kantonalen Datenmarkt einem departementsübergreifenden Gremium zukommen. Aktuell besteht bereits eine Leistungsvereinbarung zwischen der Konferenz für Organisation und Informatik Basel-Stadt (KOI) und den Zentralen Informatikdiensten (ZID). Dies hat sich bewährt und soll nicht geändert werden.

Abs. 2

Gegenstand solcher Vorgaben kann z.B. die Form, in welcher Daten geliefert werden müssen, sein. Das Gesamtsystem umfasst mehr als die zentrale Plattform gemäss § 2 DMV, z.B. auch Infrastruktur wie Server, Datenbanken und Sicherheitskomponenten.

Abs. 3

lit. a

Hierzu gehört insbesondere auch der Entscheid über die zu erbringenden Leistungen wie z.B.:

- Pflege und Weiterentwicklung der Softwareprogramme, der Extract, Transform and Load (ETL) - Prozedur (Prozess, bei welchem Daten aus mehreren gegebenenfalls unterschiedlich strukturierten Datenquellen in einer Zieldatenbank vereinigt werden), der Datenbank-Prozedur, sowie der Schnittstellen und Services,
- Implementierung von Anschlüssen für Datenbezüger und Datenlieferanten als Service,
- Sicherstellen von Qualitätssicherung und Datenintegration,
- Sicherstellen der Einhaltung der Anforderungen gemäss den Bestimmungen über den Datenschutz und die Informationssicherheit,
- Aktuelle Dokumentation des Datenmarktes und dessen Nutzung,
- Release-/Change Planung in Absprache mit dem Anwendungskoordinator,
- Beratung von Departementen und Dienststellen in Fragen der Nutzung des Datenmarkts und bezüglich Schnittstellen/Anschlüssen.

lit. b

Die KOI legt im Rahmen des Servicemanagements messbare Qualitätsmerkmale fest, welche in der Servicevereinbarung dokumentiert werden. Der Leistungserbringer rapportiert halbjährlich in Form eines QS-Berichtes über den Erreichungsgrad.

lit. c

Die KOI erarbeitet ein Konzept für die Vernichtung der Personendaten im Datenmarkt (siehe Erläuterungen zu § 8) und macht den ZID die entsprechenden Vorgaben.

lit. d

Die Festlegung des vorzuhaltenden Schutzes des Gesamtsystems richtet sich nach der Einteilung in die Schutzbedarfsstufen Grundschatz, erhöhter Schutzbedarf und sehr hoher Schutzbedarf (vgl. Verordnung über die Informationssicherheit vom 13. Dezember 2016 sowie die Weisung der Konferenz für Organisation und Informatik Kanton Basel-Stadt zur Umsetzung des Schutzes von Informationen in der kantonalen Verwaltung [Grundschatz] vom 31. Oktober 2016).

lit. e

Eine weitere Aufgabe der KOI ist das Risikomanagement im Zusammenhang mit dem kantonalen Datenmarkt. Das Risikomanagement im hier verstandenen Sinn umfasst auch die Übernahme des Restrisikos.

lit. f

Gemäss § 26 IDG hat jede Person Anspruch darauf zu wissen, ob bei einem öffentlichen Organ Personendaten über sie vorhanden sind, und gegebenenfalls auf Zugang zu diesen eigenen Personendaten. Die Voraussetzungen für die Verweigerung des Zugangs oder eines Aufschubs dieses Rechts richten sich nach § 29 IDG.

Gemäss § 27 IDG kann jede betroffene Person vom öffentlichen Organ verlangen, dass es unrichtige Personendaten berichtigt oder, falls die Berichtigung nicht möglich ist, vernichtet (lit. a), das widerrechtliche Bearbeiten von Personendaten unterlässt (lit. b), die Folgen des widerrechtlichen Bearbeitens von Personendaten beseitigt (lit. c) oder die Widerrechtlichkeit des Bearbeitens von Personendaten schriftlich feststellt (lit. d). Für die Wahrung dieser weiteren Rechte ist die Dateneignerin oder der Dateneigner verantwortlich.

lit. g

Gemäss § 28 IDG kann eine betroffene Person beim öffentlichen Organ die Bekanntgabe ihrer Personendaten an Private schriftlich sperren lassen. Die verantwortliche Stelle ist verpflichtet, die Einhaltung der gesetzlichen Vorgaben im Zusammenhang mit diesem Sperrecht sicherzustellen.

lit. h

Alle Daten müssen einer Dateneignerin oder einem Dateneigner zugewiesen werden. Das betrifft Bundesdaten und kantonale Daten.

lit. i

Für den Bezug von Daten aus dem Datenmarkt ist eine Autorisierung durch die Dateneignerin oder den Dateneigner notwendig, welche mit dem Abrufverfahren erfolgt. Damit wird der Zugriff eines öffentlichen Organs («zugriffsbeantragendes Organ») auf Daten anderer öffentlicher Organe («Dateneignerinnen») geregelt. Die Zugriffsgewährung stellt eine Datenbekanntgabe im Sinne von § 21 IDG dar und ist der oder dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen (§ 13 IDG i.V.m. § 2 Abs. 1 lit. a der Verordnung vom 9. August 2011 über die Information und den Datenschutz, IDV, SG 153.270).

lit. j

Zur Sicherstellung der Rechte der Dateneignerin oder des Dateneigners gehört z.B., dass die Vorgaben der dateneinliefernden Fachämter für die Nutzung ihrer Daten eingehalten werden. Vgl. zu den Pflichten der dateneinliefernden öffentlichen Organe § 4 Abs. 2 DMV.

§ 4. Dateneinlieferung

¹ Die öffentlichen Organe gemäss § 3 Absatz 1 des Informations- und Datenschutzgesetzes sind verpflichtet, Daten, die sie aufgrund eines gesetzlichen Auftrages in einer Fachanwendung generieren und die auch von einem anderen öffentlichen Organ oder von mehreren anderen öffentlichen Organen zur Erfüllung ihrer gesetzlichen Aufgaben benötigt werden, dem Datenmarkt kostenlos zur Verfügung zu stellen.

² Die dateneinliefernden öffentlichen Organe haben insbesondere folgende Aufgaben:

- a) Festlegung des Schutzbedarfs der gelieferten Daten;

- b) Sicherstellung der inhaltlichen Richtigkeit der Daten und der geforderten Qualität der Daten;
- c) Entscheid über Autorisierungsgesuche gemäss § 5 Absatz 2.

Erläuterungen zu § 4 Dateneinlieferung

Titel

Eine Datenlieferung kann grundsätzlich sowohl eine Auslieferung als auch eine Einlieferung bedeuten. In § 4 DMV wird daher im Sinne einer Präzisierung der Begriff „Dateneinlieferung“ verwendet.

§ 4 Abs. 1

Eine Fachanwendung ist eine Softwarelösung, welche die Abwicklung der kantonalen Geschäftsprozesse eines bestimmten Fachbereichs gemäss dem gesetzlichen Auftrag unterstützt resp. sicherstellt, z.B. die Steuerlösung NEST, die MFK-Lösung Avedris, die Einwohnerlösung Loganto sowie die Baubegehlenlösung BBG. Bei Uneinigkeit über die Einlieferungspflicht übernimmt die KOI eine vermittelnde Funktion.

Abs. 2

lit. a - c

Genannt sind hier die wichtigsten Aufgaben. Es können weitere hinzukommen. Die dateneinliefernden öffentlichen Organe sind verpflichtet, die Daten in geeigneter Form zur Verfügung zu stellen. Die ZID informieren die Dateneignerin oder den Dateneigner über die entsprechenden Standards und Strukturen, welche einzuhalten sind.

§ 5. Datenauslieferung

¹ Die Datenauslieferung erfolgt:

- a) im Abrufverfahren
 1. als Datenbekanntgabe über eine Benutzungsoberfläche (Onlinezugriff),
 2. durch Zurverfügungstellen von Daten via Webservice oder
 3. durch periodisches und automatisiertes Zurverfügungstellen von Listen;
- b) durch eine Einzelauslieferung im Auftrag des dateneinliefernden Organs.

² Datenauslieferungen im Sinne von Absatz 1 lit. a bedürfen einer Autorisierung durch die Dateneignerin oder den Dateneigner.

³ Autorisierungen sind der oder dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

⁴ Für den Zugriff auf im Datenmarkt gespeicherte oder vom Datenmarkt bezogene Daten müssen sich Benutzerinnen und Benutzer mittels eines dem Schutzbedarf entsprechenden Verfahrens authentisieren.

⁵ Sie dürfen die Daten ausschliesslich zu dem Zweck verwenden, der in der Autorisierung durch die Dateneignerin oder den Dateneigner angegeben ist.

Erläuterungen zu § 5 Datenauslieferung

Titel

Als Folge der Präzisierung des Titels in § 4 wird hier von „Datenauslieferung“ an Stelle von „Datenbezug“ gesprochen.

§ 5 Abs. 1

lit. a

Bei der Datenauslieferung im Abrufverfahren über eine Benutzeroberfläche (Onlinezugriff) erfolgt der Online-Zugang zu Daten im Datenmarkt durch diverse autorisierte und berechnigte Verwaltungseinheiten und Personen mittels Webportal. Dies betrifft z.B. Auskünfte über Personen, Gebäude oder Motorfahrzeuge.

Darüber hinaus kann die Datenauslieferung durch Zurverfügungstellen von Daten mittels Webservice erfolgen. Der Webservice stellt einen direkten Datenaustausch zwischen zwei Systemen sicher (Maschine zu Maschine Interaktion), ist eindeutig identifizierbar und über eine technische User-ID und Passwort geschützt. Das maschinenlesbare Format ist jeweils in einer Schnittstellenbeschreibung spezifiziert. Es bestehen zahlreiche Webservices vom Datenmarkt zu den kantonalen Fachanwendungen. Beispiele dafür sind die Steuerlösung NEST, die MFK-Lösung Avedris, die Einwohnerlösung Loganto sowie die Baubegehrenlösung BBG.

Auf Wunsch von Kundinnen und Kunden innerhalb der kantonalen Verwaltung werden dedizierte Auswertungen und Listen erstellt, welche periodisch im Dauerauftrag aufbereitet werden. Beispiele sind die monatliche Auflistung und Lieferung der Zuzüge und Wegzüge im Kanton als Basis für den Versand des kantonalen Abfuhrkalenders durch Gebäude- und Abwasserreinigung, die jährliche Lieferung der Gebäudedaten an das Hochbau- und Planungsamt, die jährliche Lieferung der Steueratlas-Daten an die Steuerverwaltung und die jährliche Aufbereitung der Daten für die Auszahlung der Gutschriften im Zusammenhang mit dem Stromsparfonds.

lit. b

Die Datenauslieferung durch eine Einzelauslieferung im Auftrag des dateneinliefernden Organs betrifft einzelne Anfragen für einmalige Datenlieferungen von kantonalen Verwaltungsstellen.

Abs. 2

Datenauslieferungen im Abrufverfahren bedürfen einer Autorisierung durch die Dateneignerin. Im Rahmen des Autorisierungsverfahrens werden die Voraussetzungen für die Datenbekanntgabe gemäss IDG (§§ 9, 21, und 29) geprüft.

In den meisten Fällen werden Berechtigungen für die Abfrage von Daten oder den Datenbezug erteilt. Für gewisse Funktionen besteht die Möglichkeit, Daten zu bearbeiten und zu verändern. Dies erfolgt mit einer spezifischen Berechnigung. Beispiele sind der Adresswechsel bei wirtschaftlich zugehörigen Personen oder die Beziehungsverwaltung (Anpassung des Zivilstands oder Setzen von Sterbedatum). Der Umfang der Zugriffsberechnigung bestimmt sich nach Massgabe des IDG.

Abs. 3

Gemäss § 13 Abs. 1 IDG muss die Bearbeitung von Personendaten vorab der oder dem Datenschutzbeauftragten zur Kontrolle vorgelegt werden, wenn sie aufgrund der Art der Bearbeitung oder der zu bearbeitenden Daten geeignet ist, besondere Risiken für die Rechte und Freiheit der betroffenen Personen mit sich zu bringen. Die oder der Datenschutzbeauftragte gibt die Beurteilung in Form einer Empfehlung gemäss § 46 ab (§ 13 Abs. 2 IDG).

Abs. 4

Das Authentisierungsverfahren ist das Verfahren, in welchem eine Person Nachweise vorlegt, die ihre Identität bestätigen sollen (z.B. Passwort). Davon abzugrenzen ist das Authentifizierungsverfahren, welches die Prüfung der behaupteten Authentisierung umfasst.

Abs. 5

Die Benutzerinnen und Benutzer dürfen die Daten ausschliesslich zu dem Zweck verwenden, der in der Autorisierung durch die Dateneignerin oder den Dateneigner angegeben ist. Dies dient auch der Kontrollierbarkeit des Datenflusses.

§ 6. Leistungserbringerin

¹ Die Zentralen Informatikdienste (ZID) sind als Leistungserbringerin des Datenmarktes insbesondere zuständig für

- a) den technischen Betrieb und die technische Sicherheit der zentralen Plattform;
- b) den Aufbau und die Weiterentwicklung der zentralen Plattform;
- c) die Qualitätssicherung, insbesondere Dublettenbereinigung;
- d) die Freischaltung von Daten gestützt auf ein genehmigtes Gesuch um Abruf.

² Zur Erfüllung der Aufgaben gemäss Abs. 1 wird eine Servicevereinbarung zwischen den ZID und der KOI abgeschlossen.

³ Die Funktionen Entwicklung, Systemadministration und Qualitätssicherung dürfen nicht durch die für die Zugriffsverwaltung und das Autorisierungsverfahren zuständigen Personen wahrgenommen werden.

Erläuterungen zu § 6 Leistungserbringerin

§ 6 Abs. 1

lit. a

Dies umfasst insbesondere auch die Sicherheit der technischen Integrität der Daten innerhalb des Datenmarktes. Unter der technischen Integrität wird verstanden, dass es zu keinen unkontrollierten Änderungen der Daten durch den Systemprozess kommt.

lit. b

Der Aufbau der zentralen Plattform bezieht sich auf das Datenmodell. Die Dateneignerin wird in das Verfahren betreffend Modelländerungen einbezogen und informiert die Datenbezüger über Modelländerungen. Zu diesem Zweck teilen die ZID der Dateneignerin die von Modelländerungen betroffenen Stellen mit.

Die Weiterentwicklung der zentralen Plattform bezieht sich, wie unter § 1 erwähnt, auf die Entwicklung neuer Funktionalitäten.

lit. c

Die Qualitätssicherung umfasst die Sicherstellung der Datenintegrität und die Vermeidung von Dubletten und fehlerhaftem Input durch gezielte Massnahmen. Mittels Bereinigungsmassnahmen werden fehlerhafte Inhalte korrigiert und somit die Richtigkeit und das Vertrauen in die Daten sichergestellt.

lit. d

Aufgrund der genehmigten Gesuche im Abrufverfahren wird der Zugang zu den Daten den berechtigten Personen und Personenkreisen freigeschalten. Die Berechtigung ist auf max. 5 Jahre befristet und muss periodisch erneuert werden. Die Verwaltung und Freigabe der Berechtigungen erfolgt in einem Organisationsbereich der ZID, der getrennt ist von den Funktionen für die Entwicklung, Systemadministration und Qualitätssicherung.

Abs. 2

Die KOI ist als Gesamtverantwortliche Auftraggeberin für die Leistungen, welche durch die ZID als Auftragnehmerin im Bereich des Datenmarkts zu erfüllen sind. Die von den ZID zu erbringenden Leistungen werden in der Servicevereinbarung zwischen der KOI und der ZID für die zentralen IKT-Basisleistungen geregelt. Inhaltlich umfasst diese insbesondere auch die Themen Servicequalität, Leistungsbezüger, Rollenbesetzung, Qualitätsmanagement und Verrechnung.

Abs. 3

Die Kernaufgaben und Funktionen für Entwicklung, Systemadministration und Qualitätssicherung sind in der Servicevereinbarung für die zentralen IKT-Basisleistungen definiert. Das Autorisierungsverfahren sowie Freigabe und Verwaltung der Berechtigungen sind organisatorisch und personell getrennt von diesen Kernaufgaben und Funktionen.

§ 7. Personenidentifikationsnummer (Personen-ID)

¹ Die Leistungserbringerin weist allen Personen, die im kantonalen Datenmarkt erfasst sind, eine Personen-ID zu.

² Die öffentlichen Organe gemäss § 3 Absatz 1 lit. a und b IDG sind verpflichtet, die PersonenID in ihren Fachsystemen zu führen und bei Datenein- und auslieferung zu übermitteln.

³ Die Personen-ID darf nicht ausserhalb der kantonalen Verwaltung kommuniziert und verwendet werden.

⁴ Für den Austausch mit öffentlichen Organen gemäss § 3 Absatz 1 lit. c IDG muss ein anderer Identifikator als die Personen-ID verwendet werden.

Erläuterungen zu § 7 Personenidentifikationsnummer (Personen-ID)

§ 7 Abs. 1-3

Die Personenidentifikationsnummer ist im *Entwurf* § 15a IDG geregelt. Gemäss Erläuterungen zum *Entwurf* § 15a Abs. 3 IDG erfolgt die Vergabe der Personen-ID zentral im kantonalen Datenmarkt. Für ihre Zuweisung sind die ZID zuständig. Gemäss *Entwurf* § 15a Abs. 4 IDG legt die zuständige Stelle Vorgaben für die korrekte Verwendung der Personen-ID fest und kontrolliert deren Einhaltung. Im Ratschlag wird diesbezüglich ausgeführt, dass das Finanzdepartement beauftragt ist, die korrekte Verwendung der Personen-ID durch Vorgaben sicherzustellen und deren Einhaltung zu überwachen. Dies solle auf Verordnungsstufe geschehen. § 7 stellt die Umsetzung dieser Vorgaben dar.

Abs. 4

Es gibt Situationen, in denen Daten periodisch an Dritte weitergeleitet werden müssen. Ein Beispiel ist die regelmässige Lieferung von Daten an die Krebsliga beider Basel, welche für den Kanton Basel-Stadt ein Mammografie-Screening Programm durchführt. Damit eine Identifikation und Zuordnung der Dateninhalte bei der Datenbezügerin ohne die Personen ID erfolgen kann, wird ein anderer Identifikator verwendet, welcher es der Datenbezügerin ermöglicht, eine eindeutige Zuordnung in ihrem Datenbestand vorzunehmen. Ein Rückschluss auf die Personen-ID durch die Datenbezügerin ist nicht mehr möglich.

§ 8. Umgang mit nicht mehr benötigten Personendaten

¹ Nicht mehr benötigte Personendaten sind zu vernichten.

Erläuterungen zu § 8 Umgang mit nicht mehr benötigten Personendaten

Gemäss § 1b Abs. 3 lit. f IDV ist der Umgang mit nicht mehr benötigten Informationen mindestens auf Verordnungsstufe zu regeln. Die KOI erlässt ein Konzept zur Vernichtung der Daten im Datenmarkt (vgl. § 3 DMV).

Die Sicherstellung der Einhaltung von Aufbewahrungsfristen und der Historisierung von Personendaten ist nicht Sache des Datenmarktes. Dies muss innerhalb der Fachanwendungen im Rahmen der Verantwortung des dateneinliefernden öffentlichen Organs (§ 4 DMV) respektive des öffentlichen Organs, dem die Daten ausgeliefert werden (§ 5 DMV) sichergestellt werden. Zudem besteht aktuell keine Möglichkeit, abschliessend festzustellen, ob Personen in den Bezügersystemen des Datenmarktes nicht mehr benötigt werden. Dennoch müssen Personendaten auch im Datenmarkt nach einer verhältnismässigen Frist vernichtet werden (§ 16 IDG). Hierbei ist es möglich, dass eine «Personenhülle», die beispielsweise aus der Personenidentifikationsnummer (§ 7 DMV), dem Namen, Vornamen, Geburtsdatum und Geschlecht besteht, im Datenmarkt bestehen bleibt. Idealerweise wird der Zugriff auf diese stark eingeschränkt. Mit einem solchen Verfahren könnten Personen aus den Fachanwendungen reaktiviert werden – zumindest mit den Informationen, deren Aufbewahrungsfrist bei den datenausliefernden Organen nicht abgelaufen ist. Zudem könnte auch sichergestellt werden, dass Personenidentifikationsnummern nicht nochmals vergeben und somit Kollisionen in den Fachanwendungen verhindert werden. Die KOI hat ein Konzept auszuarbeiten und den ZID entsprechende Vorgaben zu machen (§ 3 Abs. 3 lit. c DMV).

§ 9. Auflösung des Datenmarkts

¹ Wird der Datenmarkt aufgelöst, sind die darin enthaltenen Informationsbestände zu vernichten.

Erläuterungen zu § 9 Auflösung des Datenmarkts

Gemäss § 1b Abs. 3 lit. h IDV ist bei der Auflösung von Datenpools § 1 Abs. 3 lit. c IDV zu beachten. Auf die Regelung der Rückgabe der Daten kann verzichtet werden, da sie in der jeweiligen Fachanwendung erhalten bleiben. Für die Einhaltung der gesetzlichen Grundlagen über die Archivierung sind die Dateneignerin oder der Dateneigner verantwortlich.

II. Änderung anderer Erlasse

Die Verordnung über die Information und den Datenschutz (Informations- und Datenschutzverordnung, IDV) vom 9. August 2011 wird wie folgt geändert:

§ 9a Abs. 1 erhält folgende neue Fassung:

¹ Als Datenbekanntgabe im Abrufverfahren gelten:

- e) die Bekanntgabe über Daten via eine Benutzungsoberfläche (Onlinezugriff),
- f) das Zurverfügungstellen von Daten via einen Webservice und
- g) das periodische und automatisierte Zurverfügungstellen von Listen.

§ 9b erhält folgende neue Fassung:

Autorisierung

¹ Die Bekanntgabe von Personendaten mittels Abrufverfahren bedarf einer Autorisierung durch die Dateneignerin oder den Dateneigner, d.h. durch das verantwortliche öffentliche Organ im Sinne von § 6 IDG.

² Die Autorisierung ist der oder dem Datenschutzbeauftragten zur Vorabkontrolle vorzulegen.

³ Hat das verantwortliche Organ die Personendaten, auf welche sich das Gesuch bezieht, seinerseits vollständig oder teilweise mittels Abrufverfahren bezogen, ist es nicht befugt, diese ohne Einwilligung des öffentlichen Organs, von dem es die beantragten Personendaten bezogen hat, mittels Abrufverfahren weiterzugeben.

§ 9c Abs. 1 erhält folgende neue Fassung:

¹ Für die Gesuchstellung bzw. die Autorisierung im Sinne von § 9b Abs. 1 und 2 sind die kantonalen Mustervorlagen zu verwenden.

Erläuterungen zu II. Änderung anderer Erlasse

§ 9a Abs. 1

Bei den Änderungen von § 9a Abs. 1 IDV handelt es sich um terminologische Anpassungen an § 5 Abs. 1 DMV.

Titel § 9b

Der Titel von § 9b „schriftliches Gesuch“ wird entsprechend den inhaltlichen Änderungen des Paragraphen (vgl. nachfolgende Ausführungen) durch „Autorisierung“ ersetzt.

§ 9b Abs. 1

Bei der Änderung handelt es sich einerseits um eine Anpassung an § 5 Abs. 2 DMV. Mit dem zweiten Satzteil wird der inzwischen verbreitet und auch in der DMV verwendete Begriff der Dateneignerin bzw. des Dateneigners erklärt.

Dass der Autorisierung durch die Dateneignerin oder den Dateneigner ein Gesuch vorangeht, ergibt sich auch aus § 9c IDV.

§ 9b Abs. 2

Dass die Dateneignerin oder der Dateneigner das Gesuch um Einräumung einer Datenbekanntgabe im Abrufverfahren auf die Recht- und Verhältnismässigkeit prüfen und das Resultate dem gesuchstellenden öffentlichen Organ mitteilen muss, ergibt sich aus den allgemein geltenden Grundsätzen und muss nicht ausdrücklich geregelt werden.

Die Absicht einer Dateneignerin oder eines Dateneigners, eine Bekanntgabe mittels Abrufverfahren zu autorisieren, stellt ein vorabkontrollpflichtiges Vorhaben im Sinne von § 13 IDG dar. In Übereinstimmung mit § 5 Abs. 3 DMV soll dies hier festgehalten werden, auch wenn sich die Pflicht aus § 2 Abs. 1 lit. a IDV ableiten lässt.

Das Erfordernis der Schriftform muss nicht mehr in der Verordnung festgehalten werden. Erstens ergibt es sich faktisch aus § 9c IDV (Verwendung von Mustervorlagen). Zweitens soll das Autorisierungsverfahren für den Datenmarkt in naher Zukunft auf digitalem Weg abgewickelt werden können. Dort wird nicht mehr «Schriftlichkeit» in Papierform, sondern eine gleichwertige Form auf elektronischem Weg gemeint sein.

§ 9b Abs. 3

Beim Ersatz von „beantragter Zugriff“ durch „Gesuch“ handelt es sich um eine sprachliche Anpassung.

§ 9c Abs. 1

Beim Ersatz von „Gesuchsgenehmigung“ durch „Autorisierung“ handelt es sich um eine Anpassung an § 5 Abs. 2 DMV.

III. Aufhebung anderer Erlasse

Keine Aufhebung anderer Erlasse.

Erläuterungen zu III. Aufhebung anderer Erlasse

Die vorliegende Revision hat keine Auswirkungen auf den Bestand anderer Erlasse.

IV. Schlussbestimmung

¹Diese Verordnung ist zu publizieren; sie tritt mit Ausnahme von § 7 am fünften Tag nach der Publikation in Kraft. Auf den gleichen Zeitpunkt hin wird die Verordnung über den Datenmarkt vom 12. Juli 2005 aufgehoben.

Bezüglich § 7 bestimmt der Regierungsrat den Zeitpunkt des Inkrafttretens.

Erläuterungen zu IV. Schlussbestimmung

Da der Einsatz einer Personen-ID mit dem Recht auf informationelle Selbstbestimmung kollidieren kann, bedarf er einer formellgesetzlichen Grundlage (vgl. Entwurf des Ratschlags zu einer Änderung des Gesetzes über die Information und den Datenschutz vom 9. Juni 2010 betreffend die Revision der §§ 15a und 30 IDG). § 7 DMV kann daher erst mit der Inkraftsetzung der entsprechenden Bestimmung im IDG in Kraft treten.