



EOS Forum 17

Datenschutz versus Forderungsmanagement

EOS. FOR A DEBT-FREE WORLD



Datenschutz – Eine Betrachtung aus unterschiedlichen Perspektiven

Prof. Dr. iur. Bernhard Waldmann
Dekan der Rechtswissenschaftlichen Fakultät
Co-Direktor des Instituts für Föderalismus



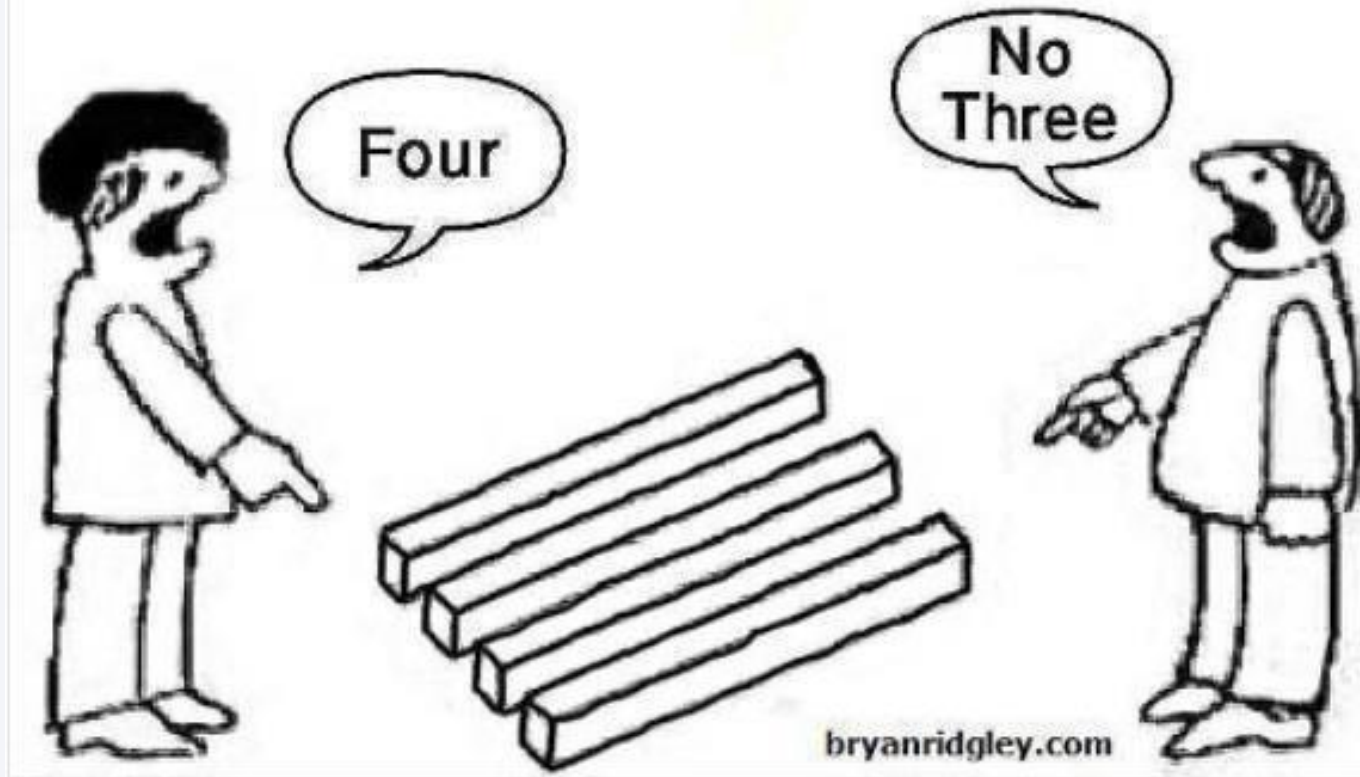
EOS Forum 2017
Zürich, 16. November 2017

Datenschutz - Eine Betrachtung aus unterschiedlichen Perspektiven

Prof. Dr. Bernhard Waldmann

Alles eine Frage der Perspektive?

Reality can be so complex that equally valid observations from differing perspectives can appear to be contradictory.



ÜBERSICHT

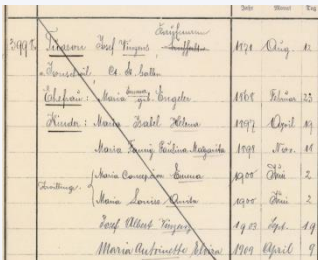
- I. Einleitung
- II. **Entwicklungsgeschichtliche Betrachtung**
- III. **Konzeptionelle Betrachtung**
- IV. **Blick in die Zukunft**
- V. **Schluss**

II. ENTWICKLUNGSGESCHICHTLICHE BETRACHTUNG

1. Datenhunger

- Daten ► Informationen ► Wissen ► Macht und Einfluss

- Vom Zensus zu Big Data



1897	Person: Paul Hugo	1871	Aug. 11
	Person: Et de l'Etat		
	Person: Marie Louise	1868	Feb. 25
	Person: Marie Babel	1897	April 19
	Person: Marie Louise	1891	Nov. 11
	Person: Marie Louise	1891	Nov. 2
	Person: Marie Louise	1891	Nov. 2
	Person: Josef Albert	1891	April 19
	Person: Maria	1891	April 9



2. Datenschutz: Eine Entwicklung in mehreren Phasen



- 1960er/1970er Jahre: Schutz der **Geheimsphäre** – Regelungen zum Schutz vor **missbräuchlicher (maschineller)** Datenbearbeitung durch den Staat
 - Hessisches Datenschutzgesetz (1970)
 - Freedom of Information Act (1966), «Privacy Act» (1974)
- Urteil des BVerfG zum Volkszählungsgesetz (15.12.1983): **Recht auf informationelle Selbstbestimmung**

■ Internationalisierung und Europäisierung des Datenschutzes

■ OECD

■ Europarat

- Rechtsprechung zu Art. 8 EMRK (Recht auf Privat- und Familienleben)
- Übereinkommen vom 28.1.1981 zum Schutz des Menschen bei der automatisierten Verarbeitung von Personendaten (SEV Nr. 108); Zusatzprotokoll vom 8.11.2001 (SEV Nr. 181)
- Revision SEV Nr. 108

■ EU

- RL 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- Rahmenbeschluss 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden
- Neu: RL (EU) 2016/680 vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten
- Neu: Verordnung (EU) 2016/679 vom 27.4.2016 («Datenschutz-Grundverordnung»)

3. Datenschutz: Entwicklung in der Schweiz

- «Fundament»
 - Grund- und menschenrechtliches Fundament

Art. 10 BV Recht auf Leben und persönliche Freiheit	1 ... 2 Jeder Mensch hat das Recht auf persönliche Freiheit, insbesondere auf körperliche und geistige Unversehrtheit und auf Bewegungsfreiheit. 3 ...
Art. 13 BV Schutz der Privatsphäre	1 Jede Person hat Anspruch auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihres Brief-, Post- und Fernmeldeverkehrs. 2 Jede Person hat Anspruch auf Schutz vor Missbrauch ihrer persönlichen Daten.
Art. 8 EMRK Recht auf Achtung des Privat- und Familienlebens	1 Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung und ihrer Korrespondenz.

- Zivilrechtliches Fundament: Art. 28 ZGB

- Allgemeine und besondere Datenschutzgesetze

Allgemeine Datenschutzgesetze	
<i>Bundesgesetz über den Datenschutz (DSG) vom 19. Juni 1992</i> Art. 2: Dieses Gesetz gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch: a. private Personen; b. Bundesorgane	<i>Kantonale Datenschutzgesetze</i> (gestützt auf Mustergesetz der KKJPD 1980)
Besondere Datenschutzvorschriften	
Ergänzung oder Modifizierung der allgemeinen Vorschriften	
Gesetzliche Erlaubnistatbestände für die Datenbearbeitung	

BIG DATA



BIG REGULATION



III. KONZEPTIONELLE BETRACHTUNG

1. Zuständigkeit

Bund	Kantone
Datenschutzgesetz (DSG) für die Bearbeitung von Personendaten <ul style="list-style-type: none">- durch Bundesorgane- durch Private	Kantonale Zuständigkeit für die Bearbeitung von Personendaten <ul style="list-style-type: none">- durch kantonale Organe

2. Richtiges Mass der Regulierung: Orientierungspunkte

▪ Grundrechte (BV)/Menschenrechte (EMRK)

Recht der Privaten,
Personendaten zu bearbeiten
(Art. 10, 26, 27 BV)



Schutz der Privaten, deren
persönliche Daten bearbeitet
werden
(Art. 35 BV i.V.m. Art. 10, 13 BV)

- Persönlichkeit (Ruf, Ehre, Ansehen)
- Privat- und Geheimsphäre
- Persönliche Freiheit (Selbstbestimmungsrecht)
- Informationelle Selbstbestimmung

- **Völkerrechtliche Minimalgarantien**
 - **Europarat**
 - Übereinkommen vom 28.1.1981 zum Schutz des Menschen bei der automatisierten Verarbeitung von Personendaten (SEV Nr. 108)
 - Zusatzprotokoll vom 8.11.2001 (SEV Nr. 181)
 - **Abkommen mit EU/EG über die Assoziierung der Schweiz am Schengen-Besitzstand vom 26.10.2004 (SR 0.362.1)**
 - Rahmenbeschluss 2008/977/JI des Rates vom 27.11.2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden
 - RL (EU) 2016/680 vom 27.4.2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten

■ EU-Recht

- Art. 8 EU-Grundrechtscharta vom 12.12.2007
- Art. 16 AEUV vom 9.5.2008
- RL 95/46/EG vom 24.10.1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr
- **Verordnung (EU) 2016/679 vom 27.4.2016 («Datenschutz-Grundverordnung»)**

Art. 3 Abs. 2 (Räumlicher Anwendungsbereich)

Diese Verordnung findet Anwendung auf die Verarbeitung personenbezogener Daten von betroffenen Personen, die sich in der Union befinden, durch einen nicht in der Union niedergelassenen Verantwortlichen oder Auftragsverarbeiter, wenn die Datenverarbeitung im Zusammenhang damit steht

a) betroffenen Personen in der Union Waren oder Dienstleistungen anzubieten, unabhängig davon, ob von diesen betroffenen Personen eine Zahlung zu leisten ist;

b) das Verhalten betroffener Personen zu beobachten, soweit ihr Verhalten in der Union erfolgt.

3. Datenschutzgesetz (DSG) des Bundes

- **Allgemeines**

- In Kraft seit 1.7.1993
- Zweck

Art. 1 **Zweck**

Dieses Gesetz bezweckt den Schutz der Persönlichkeit und der Grundrechte von Personen, über die Daten bearbeitet werden.

- «Querschnittsgesetz»
- «Rahmengesetz»

■ Geltungsbereich: Bearbeiten von Personendaten durch Private und Bundesorgane

Art. 2 Geltungsbereich

¹ Dieses Gesetz gilt für das Bearbeiten von Daten natürlicher und juristischer Personen durch:

- a. private Personen;
- b. Bundesorgane.

Art. 3 Begriffe

Die folgenden Ausdrücke bedeuten:

- a. *Personendaten (Daten)*: alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen;
- c. *besonders schützenswerte Personendaten*: Daten über:
 1. die religiösen, weltanschaulichen, politischen oder gewerkschaftlichen Ansichten oder Tätigkeiten,
 2. die Gesundheit, die Intimsphäre oder die Rassenzugehörigkeit,
 3. Massnahmen der sozialen Hilfe,
 4. administrative oder strafrechtliche Verfolgungen und Sanktionen;
- e. *Bearbeiten*: jeder Umgang mit Personendaten, unabhängig von den angewandten Mitteln und Verfahren, insbesondere das Beschaffen, Aufbewahren, Verwenden, Umarbeiten, Bekanntgeben, Archivieren oder Vernichten von Daten;

■ Allgemeine Bearbeitungsgrundsätze

- Grundsatz der Rechtmässigkeit (Art. 4 Abs. 1 und 5 DSG)

⁵ Ist für die Bearbeitung von Personendaten die **Einwilligung** der betroffenen Person erforderlich, so ist diese Einwilligung erst gültig, wenn sie nach angemessener Information freiwillig erfolgt. Bei der Bearbeitung von besonders schützenswerten Personendaten oder Persönlichkeitsprofilen muss die Einwilligung zudem ausdrücklich erfolgen.⁹

- Grundsatz von Treu und Glauben (Art. 4 Abs. 2 DSG)
- Grundsatz der Verhältnismässigkeit (Art. 4 Abs. 3 DSG)
- Grundsatz der Transparenz/Erkennbarkeit (Art. 4 Abs. 4 DSG)
- Grundsatz der Zweckbindung (Art. 4 Abs. 3 DSG)
- Grundsatz der Richtigkeit (Art. 5 Abs. 1 DSG)
- Grundsätze für die grenzüberschreitende Datenbekanntgabe (Art. 6 DSG)
- Grundsätze für die Datensicherheit (Art. 7 DSG)

- **Besondere Bearbeitungsgrundsätze für Private**
 - Ausgangslage: Grundrecht auf Datenbearbeitung c. Grundrecht auf Datenschutz
 - Prüfprogramm
 - 1) Vorliegen einer Persönlichkeitsverletzung (Art. 12 DSGVO)

Art. 12 Persönlichkeitsverletzungen

¹ Wer Personendaten bearbeitet, darf dabei die Persönlichkeit der betroffenen Personen nicht widerrechtlich verletzen.

² Er darf insbesondere nicht:

- a. Personendaten entgegen den Grundsätzen der Artikel 4, 5 Absatz 1 und 7 Absatz 1 bearbeiten;
- b. ohne Rechtfertigungsgrund Daten einer Person gegen deren ausdrücklichen Willen bearbeiten;
- c. ohne Rechtfertigungsgrund besonders schützenswerte Personendaten oder Persönlichkeitsprofile Dritten bekanntgeben.¹⁹

³ In der Regel liegt keine Persönlichkeitsverletzung vor, wenn die betroffene Person die Daten allgemein zugänglich gemacht und eine Bearbeitung nicht ausdrücklich untersagt hat.

2) Rechtfertigungsgründe (Art. 13 DSGVO)?

Art. 13 Rechtfertigungsgründe

¹ Eine Verletzung der Persönlichkeit ist widerrechtlich, wenn sie nicht durch Einwilligung des Verletzten, durch ein überwiegendes privates oder öffentliches Interesse oder durch Gesetz gerechtfertigt ist.

² Ein überwiegendes Interesse der bearbeitenden Person fällt insbesondere in Betracht, wenn diese:

- a. in unmittelbarem Zusammenhang mit dem Abschluss oder der Abwicklung eines Vertrags Personendaten über ihren Vertragspartner bearbeitet;
- b. mit einer anderen Person in wirtschaftlichem Wettbewerb steht oder treten will und zu diesem Zweck Personendaten bearbeitet, ohne diese Dritten bekannt zu geben;
- c. zur Prüfung der Kreditwürdigkeit einer anderen Person weder besonders schützenswerte Personendaten noch Persönlichkeitsprofile bearbeitet und Dritten nur Daten bekannt gibt, die sie für den Abschluss oder die Abwicklung eines Vertrages mit der betroffenen Person benötigen;
- d. beruflich Personendaten ausschliesslich für die Veröffentlichung im redaktionellen Teil eines periodisch erscheinenden Mediums bearbeitet;
- e. Personendaten zu nicht personenbezogenen Zwecken insbesondere in der Forschung, Planung und Statistik bearbeitet und die Ergebnisse so veröffentlicht, dass die betroffenen Personen nicht bestimmbar sind;
- f. Daten über eine Person des öffentlichen Lebens sammelt, sofern sich die Daten auf das Wirken dieser Person in der Öffentlichkeit beziehen.

IV. BLICK IN DIE ZUKUNFT:

NEUES DATENSCHUTZGESETZ DES BUNDES



▪ Stand der Revision

- Vernehmlassung VE-DSG (21.12.2016–4.4.2017)
- Entwurf mit Botschaft des Bundesrats vom 15.9.2017 (BBI 2017)



▪ Ziele

- Stärkung des Datenschutzes
 - Anpassung an veränderte technologische Verhältnisse und Schutzbedürfnisse
- Gewährleistung eines den europäischen Anforderungen genügenden Datenschutzniveaus
 - Ratifikation SEV 108 (Europarat)
 - Übernahme der RL (EU) 680/2016 über den Datenschutz im Bereich der Strafverfolgung (Schengen-Besitzstand)
 - Annäherung an Verordnung (EU) 2016/679 (vergleichbares Schutzniveau)

■ **Hauptsächliche Neuerungen**

- Geltungsbereich auf die Bearbeitung von Daten natürlicher Personen beschränkt
- Informationspflichten bei der Datenbeschaffung durch private Verantwortliche auf alle Datenbearbeitungen ausgeweitet
- «Privacy by Design» und «Privacy by Default»
- Datenschutz-Folgenabschätzung
- Meldungen von Verletzungen der Datensicherheit
- Anreize zur Selbstregulierung und Selbstkontrolle
 - Verhaltenskodizes von Berufs- und Wirtschaftsverbänden
 - Datenschutzberater(in) im Unternehmen
- Stärkung Befugnisse des EDÖB
- Verschärfung der Strafbestimmungen

V. SCHLUSS



Quelle. Datenschutzbeauftragter des Kantons Basel-Stadt

ANHANG

**Auszüge aus dem Entwurf des Bundesrats für ein neues
Datenschutzgesetz (E-DSG) vom 15. September 2017**

■ Informationspflichten

Art. 17 Informationspflicht bei der Beschaffung von Personendaten

¹ Der Verantwortliche informiert die betroffene Person über die Beschaffung von Personendaten; diese Informationspflicht gilt auch, wenn die Daten nicht bei der betroffenen Person beschafft werden.

² Er teilt der betroffenen Person bei der Beschaffung diejenigen Informationen mit, die erforderlich sind, damit sie ihre Rechte nach diesem Gesetz geltend machen kann und eine transparente Datenbearbeitung gewährleistet ist; er teilt ihr mindestens mit:

- a. die Identität und die Kontaktdaten des Verantwortlichen;
- b. den Bearbeitungszweck;
- c. gegebenenfalls die Empfängerinnen und Empfänger oder die Kategorien von Empfängerinnen und Empfängern, denen Personendaten bekanntgegeben werden.

⁵ Werden die Daten nicht bei der betroffenen Person beschafft, so teilt er ihr die Informationen nach den Absätzen 2–4 spätestens einen Monat, nachdem er die Daten erhalten hat, mit. Gibt der Verantwortliche die Personendaten vor Ablauf dieser Frist bekannt, so informiert er die betroffene Person spätestens im Zeitpunkt der Bekanntgabe.

(...)

■ «Privacy by design» und «Privacy by default»



Art. 6 Datenschutz durch Technik und datenschutzfreundliche Voreinstellungen

¹ Der Verantwortliche ist verpflichtet, die Datenbearbeitung technisch und organisatorisch so auszugestalten, dass die Datenschutzvorschriften eingehalten werden, insbesondere die Grundsätze nach Artikel 5. Er berücksichtigt dies ab der Planung.

² Die technischen und organisatorischen Massnahmen müssen insbesondere dem Stand der Technik, der Art und dem Umfang der Datenbearbeitung sowie den Risiken, welche die Bearbeitung für die Persönlichkeit und Grundrechte der betroffenen Personen mit sich bringt, angemessen sein.

³ Der Verantwortliche ist verpflichtet, mittels geeigneter Voreinstellungen sicherzustellen, dass die Bearbeitung der Personendaten auf das für den Verwendungszweck nötige Mindestmass beschränkt ist, soweit die betroffene Person nicht etwas anderes bestimmt.

≤

▪ Datenschutz-Folgenabschätzung

Art. 20 Datenschutz-Folgenabschätzung

¹ Der Verantwortliche erstellt vorgängig eine Datenschutz-Folgenabschätzung, wenn eine Bearbeitung ein **hohes Risiko** für die Persönlichkeit oder die Grundrechte der betroffenen Person mit sich bringen kann. Sind mehrere ähnliche Bearbeitungsvorgänge geplant, so kann eine gemeinsame Abschätzung erstellt werden.

² Das hohe Risiko ergibt sich aus der Art, dem Umfang, den Umständen und dem Zweck der Bearbeitung. Es liegt namentlich vor:

- a. bei der umfangreichen Bearbeitung besonders schützenswerter Personendaten;
- b. bei einem Profiling;
- c. wenn systematisch umfangreiche öffentliche Bereiche überwacht werden.

³ Die Datenschutz-Folgenabschätzung enthält eine Beschreibung der geplanten Bearbeitung, eine Bewertung der Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Person sowie die Massnahmen zum Schutz der Persönlichkeit und der Grundrechte.

⁴ Von der Erstellung einer Datenschutz-Folgenabschätzung ausgenommen sind Datenbearbeitungen durch Private, die zur Erfüllung einer gesetzlichen Pflicht des Verantwortlichen erfolgen.

≤

■ Meldung von Verletzungen der Datensicherheit

Art. 22 Meldung von Verletzungen der Datensicherheit

¹ Der Verantwortliche meldet dem Beauftragten so rasch als möglich eine Verletzung der Datensicherheit, die voraussichtlich zu einem hohen Risiko für die Persönlichkeit oder die Grundrechte der betroffenen Person führt.

² In der Meldung nennt er mindestens die Art der Verletzung der Datensicherheit, deren Folgen und die ergriffenen oder vorgesehenen Massnahmen.

³ Der Auftragsbearbeiter meldet dem Verantwortlichen so rasch als möglich eine Verletzung der Datensicherheit.

⁴ Der Verantwortliche informiert die betroffene Person, wenn es zu ihrem Schutz erforderlich ist oder der Beauftragte es verlangt.

⁵ Er kann die Information an die betroffene Person einschränken, aufschieben oder darauf verzichten, wenn:

(...)

■ Verhaltenskodizes

Art. 10 Verhaltenskodizes

¹ Berufs- und Wirtschaftsverbände, die nach ihren Statuten zur Wahrung der wirtschaftlichen Interessen ihrer Mitglieder befugt sind, sowie Bundesorgane können dem Beauftragten einen Verhaltenskodex vorlegen.

² Dieser nimmt zu den Verhaltenskodizes Stellung und veröffentlicht seine Stellungnahmen.

Art. 20 Datenschutz-Folgenabschätzung

⁵ Der private Verantwortliche kann von der Erstellung einer Datenschutz-Folgenabschätzung absehen, wenn er nach Artikel 12 zertifiziert ist oder einen Verhaltenskodex nach Artikel 10 einhält, der die folgenden Voraussetzungen erfüllt:

- a. Der Verhaltenskodex beruht auf einer Datenschutz-Folgenabschätzung.
- b. Er sieht Massnahmen zum Schutz der Persönlichkeit oder der Grundrechte der betroffenen Person vor.
- c. Er wurde dem Beauftragten vorgelegt.



■ Datenschutzberaterin oder -berater

Art. 9 Datenschutzberaterin oder -berater

¹ Private Verantwortliche können eine Datenschutzberaterin oder einen Datenschutzberater ernennen.

² Sie können von der Ausnahme nach Artikel 21 Absatz 4 Gebrauch machen, wenn die folgenden Voraussetzungen erfüllt sind:

- a. Die Datenschutzberaterin oder der Datenschutzberater übt ihre oder seine Funktion fachlich unabhängig aus; sie oder er ist gegenüber dem Verantwortlichen nicht weisungsgebunden.
- b. Sie oder er übt keine Tätigkeiten aus, die mit ihren oder seinen Aufgaben als Datenschutzberaterin oder -berater unvereinbar sind.
- c. Sie oder er verfügt über die erforderlichen Fachkenntnisse.
- d. Der Verantwortliche veröffentlicht die Kontaktdaten der Datenschutzberaterin oder des Datenschutzberaters und teilt diese dem Beauftragten mit.

³ Der Bundesrat regelt die Ernennung von Datenschutzberaterinnen und Datenschutzberatern durch die Bundesorgane.



- **EDÖB: Untersuchung von Verstößen gegen Datenschutzvorschriften**

Art. 43 **Untersuchung**

¹ Der Beauftragte eröffnet von Amtes wegen oder auf Anzeige hin eine Untersuchung gegen ein Bundesorgan oder eine private Person, wenn Anzeichen bestehen, dass eine Datenbearbeitung gegen die Datenschutzvorschriften verstossen könnte.

Art. 45 **Verwaltungsmaßnahmen**

¹ Liegt eine Verletzung von Datenschutzvorschriften vor, so kann der Beauftragte verfügen, dass die Bearbeitung ganz oder teilweise angepasst, unterbrochen oder abgebrochen wird und die Personendaten ganz oder teilweise gelöscht oder vernichtet werden.

