# VERNEHMLASSUNGSBERICHT

# DER REGIERUNG

# BETREFFEND

# DIE TOTALREVISION DES DATENSCHUTZGESETZES SOWIE DIE

# ABÄNDERUNG WEITERER GESETZE

**(Datenschutzgrundverordnung)**

**Ministerium für Äusseres, Justiz und Kultur**

**Vernehmlassungsfrist:** 28. Februar 2018

# INHALTSVERZEICHNIS

Seite

**Beilagen:**

- Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)
- Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates

***ZUSAMMENFASSUNG***

*Die gegenständliche Vorlage ergänzt in erster Linie die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung, DSGVO). Aufbau und Inhalt der Vorlage folgen dem deutschen Bundesdatenschutzgesetz (BDSG) als Rezeptionsgrundlage.*

*Die DSGVO stärkt die bestehenden Rechte und soll den Bürgern mehr Kontrolle über ihre Daten geben:*

- *Es muss beispielsweise besser über die Art und Weise, wie die Daten verarbeitet werden, informiert werden. Diese Informationen müssen klar und verständlich sein.*
- *Personenbezogene Daten können einfacher von einem Anbieter auf einen anderen übertragen werden. Wenn die Betroffenen nicht möchten, dass ihre Daten weiter verarbeitet werden und es keine legitimen Gründe für deren Speicherung gibt, müssen die Daten gelöscht werden.*
- *Unternehmen und Organisationen müssen die nationale Aufsichtsbehörde so bald wie möglich über schwere Verstösse gegen den Datenschutz informieren, damit die Nutzer geeignete Massnahmen ergreifen können.*

*Durch die DSGVO wird ein einheitliches Regelwerk geschaffen, das Unternehmen die Geschäftstätigkeit im gesamten EWR erleichtert und somit Kosten und Aufwendungen reduzieren soll. Unternehmen mit Sitz ausserhalb des EWR müssen denselben Regeln folgen, wenn sie Dienstleistungen innerhalb des EWR anbieten.*

*Die DSGVO befindet sich aktuell im Übernahmeverfahren in das EWR-Abkommen. Da die gegenständliche Vorlage die DSGVO ergänzt, ist ein gemeinsames Inkrafttreten von Gesetz und DSGVO in Liechtenstein geplant.*

*Der Aufgabenbereich und die Befugnisse der nationalen datenschutzrechtlichen Aufsichtsbehörden werden unter der DSGVO erweitert und vereinheitlicht. Insbesondere ist im Rahmen des von der DSGVO festgelegten One-Stop-Shop Prinzips*

*vorgesehen, dass die nationalen Aufsichtsbehörden als federführende Aufsichtsbehörden tätig werden können.*

*Die Datenschutzstelle ist aktuell organisatorisch dem Landtag zugeordnet. Verschiedene Zuständigkeiten innerhalb des Landtags, des Landtagspräsidiums, der Geschäftsprüfungskommission und der Regierung bringen Probleme mit sich bzw. verkomplizieren das jeweilige Verfahren. Mit dieser Vorlage erfolgt daher eine Neuzuordnung der unabhängigen Datenschutzstelle zu dem für den Geschäftsbereich Justiz zuständigen Ministerium.*

*Die Vorlage dient darüber hinaus der Umsetzung der Richtlinie (EU) 2016/680 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates (DSRL-PJ) aus dem Schengen Acquis. Durch die DSRL-PJ wird der Schutz personenbezogener Daten im Bereich der Strafverfolgung ausgebaut. Personenbezogene Daten werden besser geschützt, wenn sie für Zwecke der Strafverfolgung verarbeitet werden, wozu auch die Kriminalitätsprävention gehört. Der Schutz gilt für jedermann – unabhängig davon, ob es sich um ein Opfer, einen Straftäter oder Zeugen handelt. Die Datenverarbeitung in den Polizeibehörden und Staatsanwaltschaften muss den Grundsätzen der Notwendigkeit, Verhältnismässigkeit und Rechtmässigkeit genügen und mit angemessenen Vorkehrungen zum Schutz des Einzelnen einhergehen. Sie unterliegt der Aufsicht durch unabhängige nationale Datenschutzbehörden und es muss für einen wirksamen Rechtsschutz gesorgt werden. Die DSRL-PJ enthält klare Regeln für den Transfer personenbezogener Daten aus dem Schengenraum, um zu gewährleisten, dass der dem Einzelnen garantierte Datenschutz nicht ausgehöhlt wird.*

**ZUSTÄNDIGES MINISTERIUM**

Ministerium für Äusseres, Justiz und Kultur

**BETROFFENE STELLEN**

Amtsstellen

Finanzkontrolle
Datenschutzstelle
Stiftungen und Anstalten des öffentlichen Rechts
Staatsanwaltschaft
Gerichte
Beschwerdekommissionen
Kommissionen und Beiräte
Landtag
Gemeinden

Vaduz, xx. Dezember 2017

LNR 2017-1517

## I. AUSGANGSLAGE

Die Richtlinie 95/46/EG des europäischen Parlamentes und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr[1] (im Folgenden „Datenschutzrichtlinie“) bildete gut 20 Jahre lang die Grundlage für die europaweite, fragmentierte Harmonisierung des Datenschutzrechts.

Die Datenschutzrichtlinie wurde zu einer Zeit erlassen, in der Big Data und Datenströme im grossen Stil noch kein Thema waren. Sie war sehr allgemein formuliert, was ihr eine Anwendbarkeit bis in die heutige Zeit ermöglichte. Seit dem Erlass der Datenschutzrichtlinie sind jedoch wegweisende technische, aber auch wirtschaftliche Entwicklungen und Neuerungen hinzugekommen. Smartphones oder das Internet erzeugen eine nie dagewesene Datenflut und führen zu neuen Herausforderungen für Gesetzgeber und Anwender. Die Globalisierung fördert einen weltweiten Datenaustausch. Dieser Entwicklung hinken bestehende Strukturen und rechtliche Grundlagen hinterher. Oft können weder Unternehmen noch Betroffene rechtssicher feststellen, wer als Verantwortlicher dafür sorgen muss, dass Daten rechtmässig verarbeitet werden. Zudem benötigen Unternehmen klare und vorhersehbare Vorgaben, unter welchen Voraussetzungen sie grenzüberschreitend Daten verarbeiten dürfen. Die nationale Fragmentierung des Datenschutzrechts erschwert dabei die effektive Rechtsdurchsetzung durch

---

1 ABl. Nr. L 281 vom 23.11.1995 S. 31.

Betroffene. Werden ihre Daten beispielsweise grenzüberschreitend in einer Cloud verarbeitet, dann unterliegen diese Prozesse oft nicht dem bekannten Recht ihrer Heimatstaaten. Zudem werden Personen immer häufiger von ihren heimischen Aufsichtsbehörden an die Behörden und Gerichte in anderen Mitgliedstaaten verwiesen.

Um mit diesen Entwicklungen Schritt zu halten, wurden die Verordnung (EU) 2016/679 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG[2] (Datenschutz-Grundverordnung, im Folgenden „DSGVO“) und die Richtlinie (EU) 2016/680 des europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung sowie zum freien Datenverkehr und zur Aufhebung des Rahmenbeschlusses 2008/977/JI des Rates[3] (im Folgenden „DSRL-PJ“) erlassen.

## II. BEGRÜNDUNG DER VORLAGE

### 1. DATENSCHUTZ-GRUNDVERORDNUNG UND DIE DSRL-PJ ALS ABGESTIMMTES REFORMPAKET

Wie unter Kapitel I. ausgeführt, reagiert die EU mit der DSGVO auf die technischen Veränderungen und will den Rechtsrahmen an die Realitäten der globalisierten Welt anpassen. Zudem sollen künftig die Zuständigkeiten von Behörden

---

2 ABl. Nr. L 119 vom 04.05.2016 S. 1.

3 ABl. Nr. L119 vom 04.05.2016 S. 89.

und Gerichten klarer geregelt und soll das neue Recht kohärenter von den Mitgliedstaaten durchgesetzt werden.

Mit der DSGVO schreibt die EU die doppelte Zweckrichtung der Datenschutzrichtlinie fort: Auch der neue Rechtsrahmen soll einerseits effektiv die Grundrechte der Bürger schützen und andererseits den (digitalen) Binnenmarkt fördern. Dabei setzt die EU auf Kontinuität. Bewährte Grundsätze der Datenschutzrichtlinie wurden in die DSGVO übernommen.

Trotz aller Harmonisierungsbestrebungen musste auch die DSGVO den Mitgliedstaaten Raum für eigene Wertentscheidungen lassen und sieht dafür so genannte Öffnungsklauseln in Form von Wahlrechten vor. Diese bestehen in vielen Bereichen, die einen weniger starken Bezug zum Binnenmarkt haben. Sie geben den Mitgliedstaaten die Möglichkeit, mit nationalen Regeln die Vorgaben aus der DSGVO zu konkretisieren bzw. auszugestalten (siehe zu den Schwerpunkten der Gesetzesvorlage).

Die Datenschutzrichtlinie erfasste nicht den Austausch personenbezogener Daten bei grenzüberschreitenden Strafverfolgungsmassnahmen und bei der Kriminalprävention. Hier galt bislang der – für den Schengen-Acquis relevante – Rahmenbeschluss 2008/977/JI über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden[4] (im Folgenden „Rahmenbeschluss 2008/977/JI“), der aber nur auf eine Mindestharmonisierung gerichtet war. Die Reform des Datenschutzrahmens bot dem EU-Gesetzgeber die Chance, die allgemeinen Grundsätze des Datenschutzrechts auf die polizeiliche und justizielle Zusammenarbeit zu erweitern, um diese auf hohem Niveau stärker als bisher zu harmonisieren. Mit Rücksicht auf die Souveränität der EU-Mitgliedstaaten bei der Strafverfolgung hat die EU-

---

4 ABl. Nr. L 350 vom 27.11.2008 S. 60.

Kommission diesen Bereich bereits in ihrem Entwurf aus der DSGVO ausgeklammert und zeitgleich eine – für den Schengen-Acquis relevante – eigenständige DSRL-PJ vorgeschlagen, welche mit der DSGVO ein abgestimmtes Reformpaket bildet.

Die DSRL-PJ ist nicht EWR-relevant. Sie bedarf aber einer Umsetzung ins innerstaatliche Recht aufgrund der Übernahme in den Schengen-Acquis. Nachdem der Rahmenbeschluss 2008/977/JI bisher im Datenschutzgesetz vom 14. März 2002[5] (im Folgenden „geltendes DSG“) und in Spezialgesetzen umgesetzt war, soll die DSRL-PJ in einem eigenen Teil (Teil III) in der gegenständlichen Vorlage umgesetzt werden.

Durch die DSGVO wird ein neuer Rechtsrahmen geschaffen, welcher nach erfolgter Übernahme der DSGVO in das EWR-Abkommen auch in Liechtenstein unmittelbar anwendbar wird. Aktuell befindet sich die DSGVO im Übernahmeverfahren in das EWR-Abkommen.

Das geltende DSG diente lediglich der Umsetzung der Datenschutzrichtlinie und des Rahmenbeschlusses 2008/977/JI. Das geltende DSG ist daher einer Totalrevision zu unterziehen. Dies sichert auch ein reibungsloses Zusammenspiel der DSGVO und der DSRL-PJ mit dem liechtensteinischen Datenschutzrecht. Weiterer Änderungsbedarf ergibt sich hinsichtlich der bestehenden Spezialgesetze als Folge der Änderungen im allgemeinen Datenschutzrecht.

---

5 LGBl. 2002 Nr. 55.

## 2. DAS DEUTSCHE BUNDESDATENSCHUTZGESETZ ALS REZEPTIONSGRUNDLAGE

Für die Totalrevision des DSG wird das deutsche Bundesdatenschutzgesetz[6] (im Folgenden „BDSG“) als Rezeptionsgrundlage herangezogen. Deutschland nimmt europaweit eine Vorreiterrolle im Datenschutz ein. Hessen erliess schon 1970 das erste Datenschutzgesetz der Welt. Schon 1983 schöpfte das deutsche Bundesverfassungsgericht in seinem grundlegenden Volkszählungsurteil das Recht auf informationelle Selbstbestimmung aus und schuf damit das verfassungsrechtliche Fundament für den Datenschutz in der Bundesrepublik Deutschland. Schon mit der Umsetzung der Datenschutzrichtlinie strebte Deutschland einen umfassenden Rechtsrahmen an. Auch in Zusammenhang mit der DSGVO verfolgt Deutschland den eigeschlagenen Weg weiter und hat ein mit der DSGVO und DSRL-PJ gut abgestimmtes Durchführungsgesetz erarbeitet. Hinzu kommt, dass Deutschland schon heute eine ausführliche Rechtsprechung wie auch umfangreiche Sekundärliteratur aufweist.

Es wurde auch die Abstützung auf die österreichische Rechtslage geprüft. Hierzu ist festzuhalten, dass die verabschiedeten Bestimmungen zur Umsetzung der DSGVO in Österreich in einem abgekürzten Gesetzesverfahren beraten wurden. In der Literatur haben kritische Stimmen bereits auf gewisse Mängel des österreichischen Gesetzes aufmerksam gemacht und zur Korrektur des selbigen aufgerufen.[7] Sekundärliteratur besteht nicht in einem umfangreichen Masse. Für Österreich als Rezeptionsgrundlage sprechen die gemeinsamen Regelungen des Verfahrensrechts (ZPO, StPO, LVG). Allerdings ist darauf hinzuweisen, dass es sich im Bereich des Datenschutzes nicht um „Verfahrensregelungen“ handelt, son-

---

6 Dieses Gesetz wurde noch nicht publiziert. Eine aktuelle Fassung ist auf der Internetseite der Bundesbeauftragten für den Datenschutz und die Informationsfreiheit zu finden: https://www.bfdi.bund.de.

7 Vgl. *Knyrim*, Reparatur des neuen DSG politisch möglich?, Dako 2017/60, S. 97.

dern um ein eigentliches Spezialgesetz. So stützt sich das bisherige DSG auf die vergleichbaren Regelungen in der Schweiz und nicht auf diejenigen in Österreich ab. Die Schweiz kann nicht weiterhin als Rezeptionsgrundlage für die Totalrevision des DSG dienen, da die DSGVO in der Schweiz nicht zur Anwendung kommt.

Aus diesen Gründen ist die Regierung der Auffassung, dass es sich bei der deutschen Rezeptionsvorlage um ein ausgewogenes Gesetz handelt, welches international und insbesondere auch auf EU-Ebene einen ausgezeichneten Ruf geniesst. Mit der Nutzung des deutschen BDSG als Rezeptionsvorlage soll eine Abstützung auf die fundierten Kenntnisse und die Erfahrung Deutschlands im Bereich Datenschutz ermöglicht werden. Zudem gestattet die Rezeptionsvorlage das Referenzieren auf unzählige deutsche Entscheide und Materialien.

## 3. KONTEXT DER GESETZESVORLAGE

Mit der Rechtsform der Verordnung hat der europäische Gesetzgeber zum weitreichendsten Mittel der Harmonisierung gegriffen. Mit ihrer allgemeinen Geltung schafft die DSGVO generell-abstrakte Regeln und entspricht damit den Gesetzen auf nationaler Ebene. Anders als Richtlinien sind Verordnungen nicht nur hinsichtlich des zu erreichendes Ziels, sondern in allen ihren Teilen verbindlich und gelten unmittelbar in jedem Mitgliedstaat. Durch die DSGVO wird das europäische Datenschutzrecht daher in der EU und durch Übernahme in das EWR-Abkommen auch in Liechtenstein unmittelbar geltendes Recht, ohne dass es weiterer Umsetzungsakte bedarf (Transformationsverbot).

Trotz der direkten Anwendbarkeit der DSGVO nach Übernahme in das EWR-Abkommen bestehen so genannte Öffnungsklauseln (siehe Kapitel III, Schwerpunkte der Gesetzesvorlage), welche den Mitgliedstaaten ermöglichen, im nationalen Recht entsprechende Regelungen zu treffen.

Darüber hinaus verlangt die DSRL-PJ eine nationale Umsetzung. Dabei ist es den Mitgliedstaaten gestattet, zum Schutz der Rechte und Freiheiten der betroffenen Personen bei der Verarbeitung personenbezogener Daten durch die zuständigen Behörden Garantien festzulegen, die strenger sind als die Garantien der DSRL-PJ. Um Belastungen für den Rechtsunterworfenen zu mindern, wird von dieser Möglichkeit Gebrauch gemacht. Aus Gründen der Einheitlichkeit und Kohärenz wird der Umsetzungsstandard der DSRL-PJ demjenigen der DSGVO angepasst.

Der Grundsatz, wonach gesetzliche Spezialbestimmungen, welche Datenschutzaspekte regeln, den allgemeinen Bestimmungen dieser Vorlage vorgehen (*lex specialis derogat legi generali*), gilt auch hier, solange die DSGVO die Frage nicht abschliessend regelt.

Diese verschiedenen Aspekte führen dazu, dass zu gewissen Bereichen und Fragestellungen folgende Grundlagen parallel berücksichtig werden müssen:

- DSGVO;
- Übernahmebeschluss in das EWR-Abkommen;
- Datenschutzgesetz;
- Datenschutzregelungen in Spezialgesetzen;
- DSRL-PJ für Auslegungsfragen im Bereich der polizeilichen und justiziellen Zusammenarbeit.

## III. SCHWERPUNKTE DER GESETZESVORLAGE

### 1. ALLGEMEINES

Wie ausgeführt, ist die DSGVO nach Übernahme in das EWR-Abkommen direkt anwendbar. Allerdings bestehen so genannte Öffnungsklauseln. Sie geben den

Mitgliedstaaten die Möglichkeit, mit nationalen Regeln die Vorgaben aus der DSGVO zu konkretisieren bzw. auszugestalten. Die entsprechenden Regelungen werden mit der gegenständlichen Vorlage festgelegt.

Zudem wird, wie unter Kapitel II Pkt. 3 ausgeführt, mit der gegenständlichen Vorlage eine Umsetzung der DSRL-PJ vorgenommen.

Die Vorlage beinhaltet damit folgende Schwerpunkte:

- Allgemeine Bestimmungen und Grundprinzipien, wie Begriffsbestimmungen, Rechtsgrundlagen für Verarbeitungen personenbezogener Daten, Regelungen für Datenschutzbeauftragte, Rechte betroffener Personen und Rechtsbehelfe.
- Schaffung einer unabhängigen Aufsichtsbehörde: Diese wird neu als unabhängige Stelle organisatorisch der Regierung zugeordnet. Dabei wird die Unabhängigkeit der Aufsichtsbehörde gesetzlich sichergestellt und durch eine Leistungsvereinbarung eine organisatorische Einbettung in die Liechtensteinische Landesverwaltung ermöglicht (siehe hierzu Erläuterungen zu Art. 8 ff. der Gesetzesvorlage).
- Internationale Zusammenarbeit der Aufsichtsbehörden.
- Durchführungsbestimmungen für Datenverarbeitungen, die unter die DSGVO fallen.
- Durchführungsbestimmungen für Datenverarbeitungen, die unter die DSRL-PJ fallen.
- Regelungen für Datenverarbeitungen ausserhalb des Anwendungsbereichs der DSGVO und der DSRL-PJ (z.B. Staatsschutz).
- Sanktionen und Bussen: In der DSGVO sind Bussen vorgesehen, welche wirksam, verhältnismässig und abschreckend sein müssen. Dies kann im Falle von Unternehmen bis zu 4 % des gesamten weltweit erzielten Jahres-

umsatzes des vorangegangenen Geschäftsjahres ausmachen (siehe hierzu Art. 36 ff. der Gesetzesvorlage).

- Bereinigung von Unstimmigkeiten: Beispielsweise heissen alle betrieblichen/behördlichen Datenschutzverantwortliche neu Datenschutzbeauftragte. Dieser Titel stand bisher dem Leiter der Datenschutzstelle zu, jedoch gab es in der Praxis immer wieder Fälle von falschen Benennungen (siehe hierzu Erläuterungen zu Art. 8 der Gesetzesvorlage).
- Anpassung weiterer betroffener Gesetze.

## 2. ÖFFNUNGSKLAUSELN

Die Öffnungsklauseln lassen sich wie folgt unterscheiden:

- **Allgemein:**

  Die Klausel erlaubt es einem Staat, in einem breiten Bereich eigene Bestimmungen zu setzen. Beispiel: Art. 23 DSGVO.

- **Spezifisch:**

  Die Klausel erlaubt es einem Staat, in einem genau vorgegebenen Punkt eine eigene Bestimmung zu setzen. Beispiel: Art. 8 Abs. 1 DSGVO.

- **Fakultativ:**

  Die Klausel erlaubt es einem Staat, zum Thema selbst gesetzgeberisch tätig zu werden, er muss aber nicht.

- **Obligatorisch:**

  Die Klausel verlangt vom Staat, zum Thema gesetzgeberisch tätig zu werden und eine Bestimmung zu schaffen.

- **Echt:**

  Die Klausel ermächtigt den Staat zu selbständigem Handeln und damit zur Schaffung einer eigenen Bestimmung.

- **Unecht:**

  Die Klausel ermächtigt den Staat unter Verweis auf eine anderweitig in der Verordnung angelegte Handlungsbefugnis zur begrenzten Ausgestaltung einer Bestimmung im Rahmen jener Handlungsbefugnis.

Innerhalb dieser Unterscheidung stehen je nach den Vorgaben der jeweiligen Klausel als Handlungsmöglichkeiten zur Verfügung:

- die Konkretisierung (die nähere Bestimmung der jeweiligen DSGVO-Regelung durch nationales Recht),
- die Ergänzung (eine Vervollständigung der DSGVO-Regelungen durch nationales Recht) und
- die Modifikation (die Möglichkeit der Abweichung vom Regelungsinhalt der DSGVO-Norm durch nationales Recht).

Auch Kombinationen sind möglich.

Es bestehen folgende Öffnungsklauseln:

| Bestimmung | Inhalt | echt / unecht | fakultativ / obligatorisch |
|---|---|---|---|
| Art. 4 Ziff. 7 | Zuweisung der Rolle des Verantwortlichen | echt; Einzelfall | fakultativ |
| Art. 4 Ziff. 9 | Behörden keine "Empfänger", wenn Untersuchungsauftrag nach nationalem Recht | unecht | fakultativ |
| Art. 6 Abs. 1 Bst. c i.V.m. Abs. 2 | Rechtmässigkeit der Verarbeitung bei gesetzlicher Verpflichtung | unecht | fakultativ |
| Art. 6 Abs. 1 Bst. e i.V.m. Abs. 2 | Rechtmässigkeit der Verarbeitung bei Ausübung einer Aufgabe im öffentlichen Interesse oder öffentlicher Gewalt | unecht | fakultativ |
| Art. 6 Abs. 4 | Ausnahme vom Grundsatz der Zweckbindung bei gesetzlicher Grundlage für Verarbeitung | unecht | fakultativ |
| Art. 8 Abs. 2 | Altersgrenze für Einwilligung eines Kindes | echt | fakultativ |
| Art. 9 Abs. 2 Bst. a | Grenzen der Einwilligung in die Verarbeitung sensibler Daten | echt | fakultativ |
| Art. 9 Abs. 2 Bst. b | Arbeits- und Sozialrecht als Rechtsgrundlage für die Verarbeitung sensibler Daten | unecht | fakultativ |
| Art. 9 Abs. 2 Bst. g | Nationale Rechtsgrundlage für die Verarbeitung sensibler Daten | unecht | fakultativ |
| Art. 9 Abs. 2 Bst. h i.V.m. Abs.. 3 | Normen im Bereich der Gesundheitsvorsorge und Arbeitsmedizin als Rechtsgrundlage für die Verarbeitung sensibler Daten | unecht | fakultativ |
| Art. 9 Abs. 2 Bst. i | Normen im Bereich der öffentlichen Gesundheit als Rechtsgrundlage für die Verarbeitung sensibler Daten | unecht | fakultativ |
| Art. 9 Abs. 2 Bst. j | Archivzwecke, Forschungszwecke und statistische Zwecke als Rechtsgrundlage für die Verarbeitung sensibler Daten | unecht | fakultativ |
| Art. 9 Abs. 4 | Bedingungen und Beschränkungen für die Verarbeitung von genetischen, biometrischen oder Gesundheitsdaten | echt | fakultativ |
| Art. 10 | Ausnahmen vom allgemeinen Verbot der Verarbeitung strafrechtlich relevanter Daten | echt | fakultativ |
| Art. 14 Abs. 5 Bst. c | Ausnahme von Informationspflicht, wenn Verarbeitung im nationalen Recht ausdrücklich vorgesehen | unecht | fakultativ |
| Art. 14 Abs. 5 Bst. d | Ausnahme von Informationspflicht bei Berufsgeheimnis nach nationalem Recht | unecht | fakultativ |
| Art. 17 Abs. 1 Bst. e | Besondere Löschungspflicht | unecht | fakultativ |
| Art. 17 Abs. 3 Bst. b | Ausnahmen von der Löschungspflicht | unecht | fakultativ |
| Art. 22 Abs. 2 Bst. b | Zulässigkeit von automatisierten Entscheidungen und Profiling | echt | fakultativ |
| Art. 23 | Beschränkungen der Betroffenenrechte | echt | fakultativ |

| | | | |
|---|---|---|---|
| Art. 26 Abs. 1 | Zuteilung der Aufgaben an gemeinsam Verantwortliche im Einzelfall | echt; Einzelfall | fakultativ |
| Art. 28 Abs. 3 Satz 1 | Auftragsverarbeitung auf gesetzlicher Grundlage im Einzelfall | echt; Einzelfall | fakultativ |
| Art. 28 Abs. 3 Bst. a HS 1 | Pflichten zur Datenverarbeitung für Auftragsverarbeiter | unecht | fakultativ |
| Art. 28 Abs. 3 Bst. a HS 2 | Untersagung der Information des Verantwortlichen über Verarbeitung durch Auftragsverarbeiter | unecht | fakultativ |
| Art. 28 Abs. 3 Bst. g | Speicherpflicht für Auftragsverarbeiter | unecht | fakultativ |
| Art. 28 Abs. 4 | Sub-Auftragsverarbeitung auf gesetzlicher Grundlage im Einzelfall | echt; Einzelfall | fakultativ |
| Art. 29 und Art. 32 Abs. 4 | Ausnahme von Weisungsgebundenheit des Auftragsverarbeiters und unterstellter Personen | unecht | fakultativ |
| Art. 35 Abs. 10 | Ausnahme von Pflicht zur Folgenabschätzung bei gesetzlicher Grundlage der Verarbeitung | echt; Einzelfall | fakultativ |
| Art. 36 Abs. 5 | Besondere Pflicht zur Konsultation der Aufsichtsbehörde sowie Genehmigungsvorbehalt | echt | fakultativ |
| Art. 37 Abs. 4 | Besondere Pflicht zur Benennung eines Datenschutzbeauftragten (DSBA) | echt | fakultativ |
| Art. 43 Abs. 1 | Benennung einer Akkreditierungsstelle | echt | obligatorisch |
| Art. 49 Abs. 1 Bst. d i.V.m. Abs. 4 | Anerkennung eines öffentlichen Interesses an einer Datenübermittlung in ein Drittland | unecht | fakultativ |
| Art. 49 Abs. 1 Bst. g | Übermittlung aus öffentlichen Registern | unecht | fakultativ |
| Art. 49 Abs. 5 | Beschränkungen der Übermittlung bestimmter Datenkategorien an Drittländer | echt | fakultativ |
| Art. 51 Abs. 3 i.V.m. Art. 68 Abs. 4 | Regelungen im Falle einer Mehrzahl von Aufsichtsbehörden | echt | obligatorisch |
| Art. 52 Abs. 4 | Sicherstellung der erforderlichen Ressourcen für die Aufsichtsbehörde | echt | obligatorisch |
| Art. 52 Abs. 5 | Personal der Aufsichtsbehörde | echt | obligatorisch |
| Art. 52 Abs. 6 | Finanzkontrolle der Aufsichtsbehörde | echt | obligatorisch |
| Art. 54 Abs. 1 Bst. a i.V.m. Art. 51 Abs. 1 | Errichtung einer Aufsichtsbehörde und Zuweisung der Zuständigkeit zur Vollziehung der DSGVO | echt | obligatorisch |
| Art. 54 Abs. 2 Bst. b i.V.m. Art. 53 Abs. 2 | Voraussetzungen für die Ernennung der Mitglieder der Aufsichtsbehörde | echt | obligatorisch |
| Art. 54 Abs. 1 Bst. c i.V.m. Art. 53 Abs. 1 | Verfahren für die Ernennung der Mitglieder der Aufsichtsbehörde | echt | obligatorisch |
| Art. 54 Abs. 1 Bst. d i.V.m. Art. 53 Abs. 3 | Amtszeit der Mitglieder der Aufsichtsbehörde | echt | obligatorisch |
| Art. 54 Abs. 1 Bst. e | Wiederernennung eines Mitglieds der Aufsichtsbehörde | echt | obligatorisch |

| | | | |
|---|---|---|---|
| Art. 54 Abs. 1 Bst. f i.V.m. Art. 52 Abs. 3, Art. 53 Abs. 3 und 4 | Pflichten der Mitglieder und Bediensteten der Aufsichtsbehörde, Unvereinbarkeiten, Regeln über Beendigung des Beschäftigungsverhältnisses | echt | obligatorisch |
| Art. 54 Abs. 2 | Amtsverschwiegenheit | echt | obligatorisch |
| Art. 55 Abs. 3 i.V.m. ErwGr 20 | Einrichtung besonderer Stellen zur Aufsicht über die Datenverarbeitung durch Gerichte | echt | fakultativ |
| Art. 57 Abs. 1 Bst. c | Regelung der Beratungstätigkeit der Aufsichtsbehörde gegenüber Parlament und Regierung | echt | obligatorisch |
| Art. 58 Abs. 1 Bst. f | Zugang zu Geschäftsräumen erhalten | echt | fakultativ |
| Art. 58 Abs. 3 Bst. b | Stellungnahmen der Aufsichtsbehörde an nichtöffentliche Stellen und die Öffentlichkeit | echt | fakultativ |
| Art. 58 Abs. 4 | Verfahrensrecht und Rechtsbehelfe gegen Aufsichtsbehörde | echt | obligatorisch |
| Art. 58 Abs. 5 | Klags- und Anzeigerecht der Aufsichtsbehörde | echt | obligatorisch |
| Art. 58 Abs. 6 | Zusätzliche Befugnisse der Aufsichtsbehörde | echt | fakultativ |
| Art. 59 Satz 2 | Benennung zusätzlicher Behörden, an welche der Tätigkeitsbericht der Aufsichtsbehörde zu übermitteln ist | echt | teilw. obligatorisch / fakultativ |
| Art. 62 Abs. 3 Satz 1 HS 1 | Regelung der Übertragung von Untersuchungsbefugnissen an Bedienstete der Aufsichtsbehörden anderer Mitgliedstaaten | echt | obligatorisch |
| Art. 62 Abs. 3 Satz 1 HS 2 | Gestattung der Ausübung von Untersuchungsbefugnissen durch Aufsichtsbehörden anderer Mitgliedstaaten nach ihrem jeweiligen nationalen Recht | echt | fakultativ |
| Art. 80 Abs. 2 | Verbandsklagebefugnis | echt | fakultativ |
| Art. 83 Abs. 7 | Festlegung, ob Geldbussen gegen Behörden und öffentliche Stellen verhängt werden können | echt | fakultativ |
| Art. 83 Abs. 8 | Verfahren für die Verhängung von Geldbussen, einschliesslich Rechtsbehelfe | echt | obligatorisch |
| Art. 83 Abs. 9 | Sonderregelung für Dänemark und Estland, wo Geldbussen nicht von einer Verwaltungsbehörde verhängt werden können | echt | fakultativ |
| Art. 84 | Zusätzliche Sanktionen, insb. für in Art. 83 nicht genannte Verstösse | echt | obligatorisch |
| Art. 85 Abs. 1 | Herstellung der Konformität der DSGVO mit dem Grundrecht auf freie Meinungsäusserung und Informationsfreiheit | echt | obligatorisch |
| Art. 85 Abs. 2 | Abweichungen und Ausnahmen von der DSGVO für die Verarbeitung zu journalistischen, wissenschaftlichen, künstlerischen oder literarischen Zwecken | echt | obligatorisch |
| Art. 86 | Zulässigkeit des Zugangs zu amtlichen Dokumenten | unecht | fakultativ |

| | | | |
|---|---|---|---|
| Art. 87 | Zulässigkeit der Verarbeitung nationaler Kennziffern | echt | fakultativ |
| Art. 88 | Arbeitnehmerdatenschutz | echt | fakultativ |
| Art. 89 Abs. 2 | Ausnahmen von bestimmten Betroffenenrechten bei Verarbeitung zu wissenschaftlichen oder historischen Forschungszwecken oder statistischen Zwecken | echt | fakultativ |
| Art. 89 Abs. 3 | Ausnahmen von bestimmten Betroffenenrechten bei Verarbeitung zu Archivzwecken | echt | fakultativ |
| Art. 90 Abs. 1 | Regelung der Ausübung der Befugnisse der Aufsichtsbehörde gegenüber Berufsgeheimnisträgern | echt | fakultativ |
| Art. 91 | Schaffung spezifischer Aufsichtsbehörden für Kirchen und religiöse Vereinigungen oder Gemeinschaften | echt | fakultativ |

## 3. ARBEITSGRUPPE DSGVO

Zur Abklärung der Frage, von welchen Öffnungsklauseln und in welcher Form Gebrauch gemacht werden soll, wurde eine Arbeitsgruppe gebildet. Diese bestand aus Vertreterinnen/Vertretern der Wirtschaftskammer, des Vereins unabhängiger Vermögensverwalter, des Verbands der Personen nach Art. 180a PGR, der Treuhandkammer, der Wirtschaftsprüfer-Vereinigung, des Bankenverbands, der Rechtsanwaltskammer, des Versicherungsverbands, der Industrie- und Handelskammer, des Anlagefondsverbands, der Datenschutzstelle, der Stabsstelle EWR sowie des Amts für Justiz. In dieser Konstellation wurden die einzelnen Öffnungsklauseln in Bezug auf die nationalen Bedürfnisse und Ausgestaltungsmöglichkeiten besprochen.

Die Öffnungsklauseln wurden grundsätzlich entsprechend der Rezeptionsvorlage übernommen. Nach Absprache mit der Arbeitsgruppe wird in den folgenden Fällen von der Rezeptionsvorlage abgewichen:

- Art. 22 Abs. 2 Bst. b DSGVO: Die Arbeitsgruppe sieht hier einen Handlungsbedarf. Siehe Art. 37 der Gesetzesvorlage.
- Art. 37 Abs. 4 DSGVO: Hierzu sieht die Arbeitsgruppe keinen Handlungsbedarf. Jedoch hat die Rezeptionsvorlage hierzu in § 38 eine Durchführungs-

bestimmung eingeführt, welche im Ergebnis in der Gesetzesvorlage nicht übernommen wird.

- Art. 85 Abs. 1 DSGVO: Hierzu wird kein Handlungsbedarf bezüglich der Gesetzesvorlage gesehen, jedoch in den Spezialgesetzen.
- Art. 85 Abs. 2 DSGVO: Hierzu wird kein Handlungsbedarf bezüglich der Gesetzesvorlage gesehen. Allfällige Anpassungen sind in den Spezialgesetzen vorzunehmen.

Wo von den Bestimmungen der Rezeptionsvorlage abgewichen wird, wird im Folgenden darauf hingewiesen.

## 4. VERWEISE AUF DEUTSCHES BUNDESDATENSCHUTZGESETZ

Die Schaffung von Durchführungsbestimmungen zur DSGVO und die Umsetzung der DSRL-PJ bedingen eine Totalrevision des geltenden DSG.

Da das deutsche BDSG – die Rezeptionsvorlage (siehe Kapitel II. Pkt. 2) – sehr stark auf dem bisher geltenden Bundesdatenschutzgesetz[8] (im Folgenden „geltendes BDSG“) aufbaut, wurde in den Erläuterungen dazu jeweils auf die Änderung bzw. Neuerung verwiesen. Zudem wird in den Erläuterungen der Vollständigkeit halber und zur Erleichterung der Recherche und Auslegung in relevanten Punkten jeweils auf die Herkunft der Regelung verwiesen.

---

[8] Bundesdatenschutzgesetz in der Fassung der Bekanntmachung vom 14. Januar 2003 (BGBl. I S. 66), das zuletzt durch Art. 10 Abs. 2 des Gesetzes vom 31. Oktober 2017 (BGBl. I S. 3618) geändert worden ist.

## IV. ERLÄUTERUNGEN ZU DEN EINZELNEN ARTIKELN

### 1. Datenschutzgesetz

**Zu Art. 1**

Art. 1 regelt den Anwendungsbereich des Gesetzes.

Nach Abs. 1 Satz 1 gilt das Gesetz für jede Form der Verarbeitung personenbezogener Daten durch öffentliche Stellen (Behörden). Bisher umfasste der Geltungsbereich des DSG neben natürlichen Personen auch juristische Personen. Aufgrund der Anwendbarkeit der DSGVO wird sich der Anwendungsbereich ausschliesslich auf natürliche Personen beschränken.

Für nicht-öffentliche Stellen gilt das Gesetz nach Abs. 1 Satz 2 im Rahmen des sachlichen Anwendungsbereichs der DSGVO. Wer öffentliche Stelle und wer nicht-öffentliche Stelle ist, ergibt sich aus Art. 2 Abs. 1 bis 3 der Gesetzesvorlage.

Soweit die Verarbeitung personenbezogener Daten im Rahmen von Tätigkeiten öffentlicher Stellen erfolgt, die weder vom Anwendungsbereich der DSGVO noch der DSRL-PJ erfasst sind, richtet sich das anzuwendende Datenschutzrecht allein nach nationalem Recht (beispielsweise die Datenverarbeitung durch die Landespolizei zum Zweck ihrer Tätigkeit im Rahmen des Staatsschutzes (Art. 2 Abs. 2 Polizeigesetz, PolG)[9].

Abs. 2 Satz 1 bestimmt das Verhältnis der Gesetzesvorlage zu spezifischen datenschutzrechtlichen Vorschriften. Die gegenständliche Gesetzesvorlage hat den Charakter eines „Auffanggesetzes“. Spezifische Rechtsvorschriften geniessen gegenüber den Vorschriften dieser Gesetzesvorlage grundsätzlich Vorrang. Dies wird durch die Formulierung in Satz 1 ausdrücklich klargestellt. Satz 2 hält fest,

---

9 LR 143.0, LGBl. 1989 Nr.48.

dass – sofern in Spezialgesetzen ein Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschliessend geregelt wird – die Vorschriften dieser Gesetzesvorlage Anwendung finden. Auch eine nicht abschliessende (teilweise) Regelung oder das Schweigen eines Spezialgesetzes führt dazu, dass subsidiär auf die Vorschriften dieser Gesetzesvorlage zurückgegriffen werden muss. Wichtig ist dies insbesondere mit Blick auf die im Zweiten Teil in Kapitel 2 der Gesetzesvorlage vorgenommenen Einschränkungen der Betroffenenrechte. Auf diese Regelungen kann als Auffangregelung zurückgegriffen werden, sofern in Spezialgesetzen kein übereinstimmender Tatbestand vorhanden ist. Dies gilt allerdings nicht, wenn spezifische Regelungen für einen bestimmten Bereich insgesamt umfassend und damit abschliessend die Datenverarbeitung regeln und somit für die gegenständliche Vorlage kein Anwendungsbereich verbleibt.

Abs. 3 besagt, dass in Verwaltungsverfahren vor öffentlichen Stellen nach dem Gesetz über die allgemeine Landesverwaltungspflege[10] die Gesetzesvorlage anwendbar ist.

Nach Abs. 4 Satz 1 Ziff. 1 findet das Gesetz auf Datenverarbeitungen im Inland Anwendung. Abs. 4 Satz 1 Ziff. 2 bestimmt, dass die Vorschriften des Gesetzes nur dann zur Anwendung kommen, wenn eine Datenverarbeitung durch eine in Liechtenstein ansässige Niederlassung vorliegt. Dies entspricht dem Harmonisierungsgedanken der DSGVO. Abs. 4 Satz 1 Ziff. 3 entspricht § 1 Abs. 5 Satz 2 geltendes BDSG.

Abs. 5 bestimmt, dass für Verarbeitungen personenbezogener Daten im öffentlichen Bereich im Rahmen von Tätigkeiten, die weder dem Anwendungsbereich der DSGVO noch der DSRL-PJ unterliegen (z.B. Staatsschutz), die DSGVO sowie Erster und Zweiter Teil der Gesetzesvorlage Anwendung finden. Abs. 5 stellt da-

---

[10] LGBl. 1922 Nr. 24.

mit sicher, dass auch für die nicht unter die beiden EU-Rechtsakte fallenden Bereiche ein datenschutzrechtliches Vollregime im Geltungsbereich der Verfassung besteht. Die besondere Erwähnung der Anwendbarkeit des Ersten Teils der Gesetzesvorlage erfolgt lediglich aus Gründen der Klarstellung, da die Anwendbarkeit sich bereits aus Abs. 1 Satz 1 unmittelbar ergibt.

**Zu Art. 2**

Die Abs. 1 bis 3 bestimmen, welche öffentlichen Stellen und nicht-öffentlichen Stellen unter den Anwendungsbereich von Art. 1 Abs. 1 der Gesetzesvorlage fallen.

Abs. 2 hält fest, was als nicht-öffentliche Stelle zu verstehen ist.

Abs. 3 stellt klar, dass öffentliche Stellen dann als nicht-öffentliche Stellen im Sinne der Gesetzesvorlage gelten, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Er dient damit auch der Klarstellung, auf welche Verarbeitungsbefugnisse bzw. Ausnahmen von Betroffenenrechten abzustellen ist, wenn eine Unterscheidung nach öffentlichen und nicht-öffentlichen Stellen vorgenommen wird.

**Zu Art. 3**

Diese Vorschrift enthält eine allgemeine Rechtsgrundlage für die Verarbeitung personenbezogener Daten durch öffentliche Stellen.

Durch die Stellung im Ersten Teil des Gesetzes unter „Allgemeine Bestimmungen“ können Verantwortliche vorbehaltlich anderer bereichsspezifischer Regelungen auf diese Regelung unabhängig davon zurückgreifen, zu welchen Zwecken die Datenverarbeitung erfolgt.

Wer zum Kreis der öffentlichen Stellen gehört, wird in Art. 2 Abs. 1 bis 3 der Gesetzesvorlage bestimmt. Soweit nicht-öffentliche Stellen hoheitliche Aufgaben

der öffentlichen Verwaltung wahrnehmen (öffentliche Unternehmen), gelten sie nach Art. 2 Abs. 1 der Gesetzesvorlage als öffentliche Stellen und können ihre Datenverarbeitung daher ebenfalls auf die Befugnis in Art. 3 der Gesetzesvorlage stützen.

Soweit die gegenständliche Vorschrift für Datenverarbeitungen zu Zwecken gemäss Art. 2 DSGVO zur Anwendung kommt, wird mit ihr eine Rechtsgrundlage basierend auf Art. 6 Abs. 1 Bst. e i.V.m. Art. 6 Abs. 3 Satz 1 DSGVO betreffend Rechtmässigkeit der Verarbeitung geschaffen. Dies ist rechtlich notwendig, da Art. 6 Abs. 1 Bst. e DSGVO selbst keine Rechtsgrundlage für die Verarbeitung von Daten schafft, was sich aus der Formulierung in Art. 6 Abs. 3 Satz 1 DSGVO ergibt. Dem Regelungsauftrag nach Art. 6 DSGVO kommt damit der liechtensteinische Gesetzeber an dieser Stelle nach.

Die Verarbeitung personenbezogener Daten durch öffentliche Stellen ist nach dieser Vorschrift zulässig, wenn sie für die Wahrnehmung einer im öffentlichen Interesse liegenden Aufgabe erforderlich ist oder wenn sie in Ausübung öffentlicher Gewalt erfolgt, die dem Verantwortlichen übertragen wurde. Beides kann sich sowohl aus nationalen Rechtvorschriften als auch aus EWR-Vorgaben ergeben. Die Verarbeitung personenbezogener Daten ist allerdings nicht nur auf dieser Rechtsgrundlage zulässig, sondern auch auf der Grundlage der weiteren in Art. 6 Abs. 1 DSGVO aufgeführten Erlaubnistatbestände, einschliesslich der auf der Grundlage der DSGVO und der DSRL-PJ erlassenen spezialgesetzlichen Regelungen.

Diese Bestimmung gründet auf § 3 der Rezeptionsvorlage. In der Liechtensteinischen Gesetzesordnung entspricht die vorliegende Regelung sinngemäss Art. 21 geltendes DSG.

**Zu Art. 4**

Die Vorschrift enthält eine dem Art. 6a geltendes DSG weitgehend entsprechende Regelung zur Videoüberwachung in öffentlich zugänglichen Räumen unter Beibehaltung verschiedener Verarbeitungsstufen. Die Verarbeitungsschritte teilen sich in die Beobachtung (Abs. 1) sowie der Speicherung oder Verwendung (Abs. 3) sowie der Kennzeichnungs-, Informations- und Löschungspflichten (Abs. 2, 4 und 5) auf. Neu wird basierend auf Art. 4 Ziff. 2 DSGVO der Begriff „Bearbeitung“ durch „Verwendung“ ersetzt.

Abs. 1 Satz 2 dient der Hilfestellung für eine Verhältnismässigkeitsprüfung zwischen dem Interesse des Betreibers (berechtigte/wichtige Interessen) und den Rechten der Betroffenen (schutzwürdige Interessen). Soweit der Betreiber eine Videoüberwachung einsetzen möchte und die Schutzgüter Leben, Gesundheit oder Freiheit in den in Ziff. 1 genannten Anlagen betroffen sein können, wird durch die Formulierung „gilt als … ein besonders wichtiges Interesse“ die Abwägungsentscheidung zugunsten der Zulässigkeit des Einsatzes einer Videoüberwachungsmassnahme geprägt.

Mit Abs. 2 wird bestehendes Recht übernommen. Die Bestimmung entspricht Art. 6a Abs. 4 geltendes DSG.

Mit Abs. 3 Satz 3 wird ebenfalls bestehendes Recht übernommen. Die Bestimmung entspricht Art. 6a Abs. 2 Satz 2 geltendes DSG.

Abs. 4 regelt die Informationspflicht im Rahmen einer Videoüberwachung. Die Information hat erst dann stattzufinden, wenn die Aufzeichnungen ausgewertet und einer Person zugeordnet werden.

Abs. 5 regelt die Löschung der Daten.

Abs. 6 stellt die Installation einer Videoüberwachung unter eine Bewilligung der Datenschutzstelle. Dies entspricht bisheriger Rechtslage.

**Zu Art. 5 bis 7 – Datenschutzbeauftragte öffentlicher Stellen (Kapitel 3)**

Kapitel 3 enthält Vorschriften für die Benennung, die Stellung und die Aufgaben der Datenschutzbeauftragten öffentlicher Stellen. Die Rechtsstellung der behördlichen Datenschutzbeauftragten soll im Anwendungsbereich der DSGVO, der DSRL-PJ und für weitere Bereiche (z.B. Staatsschutz) einheitlich ausgestaltet sein.

**Zu Art. 5**

Art. 5 regelt die Vorgaben, welche bei der Benennung von Datenschutzbeauftragten öffentlicher Stellen zu beachten sind. Dies betrifft die Qualifikation, die Einordnung in die Organisation und gemeinsame Datenschutzbeauftragte. Im geltenden Recht war die Möglichkeit, einen Datenschutzbeauftragten einzusetzen, in den Art. 4a, 4b und 13a DSV geregelt.

In Abs. 1 wird Art. 37 Abs. 1 Bst. a DSGVO zur Umsetzung des Art. 32 Abs. 1 DSRL-PJ als Grundlage herangezogen.

Die Abs. 2, 3 und 5 setzen Art. 32 Abs. 2 bis 4 DSRL-PJ um. Sie bauen inhaltlich auf Art. 37 Abs. 3, 5 und 7 DSGVO auf.

Abs. 4 überträgt die Regelung des Art. 37 Abs. 6 DSGVO, nach welcher sowohl interne als auch externe Datenschutzbeauftragte zulässig sind, auf den gesamten Bereich der öffentlichen Stellen. Dies geht über die Vorgaben der DSRL-PJ hinaus.

**Zu Art. 6**

Art. 6 behandelt die Stellung des Datenschutzbeauftragten. Demnach ist dieser bei der Erfüllung seiner Aufgaben an keine Weisungen gebunden und von der öffentlichen Stelle nach Kräften zu unterstützen. Zudem sind die Voraussetzun-

gen für die Erfüllung seiner Aufgaben entsprechend zu schaffen (vgl. Art. 33 Abs. 1 und 2 DSRL-PJ und Art. 38 Abs. 1 und 2 DSGVO).

Abs. 3 und Abs. 5 Satz 1 übertragen die Vorgaben des Art. 38 Abs. 3 und 4 DSGVO auf alle öffentlichen Stellen, unabhängig davon, zu welchem Zweck die Datenverarbeitung erfolgt. Dies geht über die Vorgaben der DSRL-PJ hinaus. Durch die Erstreckung der Vorgaben der DSGVO auf den Anwendungsbereich der DSRL-PJ und der Datenverarbeitung zu Zwecken, für die der Anwendungsbereich des Rechts der EU nicht eröffnet ist (z.B. Staatsschutz), wird die Rechtsstellung des behördlichen Datenschutzbeauftragten in öffentlichen Stellen einheitlich ausgestaltet.

In Abs. 4 kommt ein besonderer Abberufungsschutz des Datenschutzbeauftragten hinzu.

Abs. 5 regelt die Verschwiegenheitspflicht des Datenschutzbeauftragten. Die Verletzung ist gemäss § 310 StGB strafbewehrt.

Das Zeugnisverweigerungsrecht in Abs. 6 sichert die Verschwiegenheitspflicht ab und stützt sich auf Art. 38 Abs. 5 DSGVO. Die Regelung geht über die Vorgaben der DSRL-PJ hinaus und erfolgt zum Zweck einer kohärenten Rechtsstellung des behördlichen Datenschutzbeauftragten in der gesamten Verwaltung.

**Zu Art. 7**

Art. 7 legt die Aufgaben des Datenschutzbeauftragten fest.

Abs. 1 Satz 1 setzt dabei Art. 34 DSRL-PJ um. Um die Aufgaben des Datenschutzbeauftragten öffentlicher Stellen für alle Verarbeitungszwecke einheitlich auszugestalten, entspricht die Norm unter lediglich redaktioneller Anpassung Art. 39 DSGVO.

Abs. 1 Satz 2 stellt klar, dass die Aufgaben eines behördlichen Datenschutzbeauftragten eines Gerichts sich nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit beziehen.

Abs. 2 stellt klar, dass der behördliche Datenschutzbeauftragte weitere Aufgaben und Pflichten wahrnehmen kann, sofern diese nicht zu einem Interessenkonflikt führen. Die Regelung entspricht Art. 38 Abs. 6 DSGVO, deren Regelungsgehalt auf den Anwendungsbereich der DSRL-PJ und der Datenverarbeitung ausserhalb des Anwendungsbereichs des Rechts der EU (z.B. Staatsschutz) erstreckt wird.

Abs. 3 legt fest, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben dem damit verbundenen Risiko Rechnung zu tragen hat. Dies entspricht Art. 39 Abs. 2 DSGVO, welcher dessen Regelungsinhalt als allgemeinen Grundsatz festschreibt. Dieser gilt somit auch im Anwendungsbereich der DSRL-PJ sowie auch ausserhalb des Anwendungsbereichs der DSGVO.

**Zu Art. 8 bis 17 – Die Datenschutzstelle (Kapitel 4 )**

Kapitel 4 passt die Regelungen der Art. 28 ff. geltendes DSG zur Datenschutzstelle an die Vorgaben der DSGVO an. Zugleich werden die Vorgaben der DSRL-PJ umgesetzt.

Die Regelungen sind basierend auf den geltenden DSG-Bestimmungen – unter Berücksichtigung der erforderlichen Anpassungen an die Vorgaben der DSGVO und der DSRL-PJ – entstanden. Aus Gründen der Lesbarkeit wurden sie mit Hinblick auf Kapitel VI der DSGVO und der DSRL-PJ neu strukturiert. Im Einzelnen geregelt werden die Errichtung, die Zuständigkeit, die Unabhängigkeit, die Wahl und Amtszeit, das Dienstverhältnis, die Rechte und Pflichten sowie die Aufgaben und Befugnisse der Datenschutzstelle und ihres Leiters.

**Zu Art. 8**

Gemäss Art. 28 geltendes DSG in der ursprünglichen Fassung wurde der Datenschutzbeauftragte von der Regierung bestellt, wobei er bei der Erfüllung seiner Aufgaben unabhängig war. Administrativ konnte der Datenschutzbeauftragte dabei einem Ressort der Regierung zugeordnet werden. Faktisch war der Datenschutzbeauftragte dem Ressort Justiz zugeordnet.

Aus Anlass des Beitritts Liechtensteins zu den Abkommen von Schengen und Dublin wurde im Jahr 2008 festgestellt, dass der damals geltende Art. 28 DSG nicht vollumfänglich den Anforderungen des Rahmenbeschlusses 2008/977/JI[11] und auch nicht ganzheitlich dem Art. 114 Schengener Durchführungsübereinkommen vom 19. Juni 1990 (SDÜ)[12] und dem Art. 30 (vormals Art. 19) der Verordnung (EU) Nr. 603/2013 (Eurodac-Verordnung)[13] entsprochen hatte, weshalb sich der Gesetzgeber im Jahr 2008[14] dazu veranlasst gesehen hat, die organisatorische Zuordnung des Datenschutzbeauftragten zu ändern und diesen neu dem Landtag zuzuordnen[15].

---

11 Rahmenbeschluss 2008/977/JI des Rates vom 27. November 2008 über den Schutz personenbezogener Daten, die im Rahmen der polizeilichen und justiziellen Zusammenarbeit in Strafsachen verarbeitet werden, ABl. L 350 vom 30.12.2008, S. 60-71.

12 ABl. L 239 vom 22.09.2000 S. 19 – 62.

13 Verordnung (EU) Nr. 603/2013 des europäischen Parlaments und des Rates vom 26. Juni 2013 über die Einrichtung von Eurodac für den Abgleich von Fingerabdruckdaten zum Zwecke der effektiven Anwendung der Verordnung (EU) Nr. 604/2013 zur Festlegung der Kriterien und Verfahren zur Bestimmung des Mitgliedstaats, der für die Prüfung eines von einem Drittstaatsangehörigen oder Staatenlosen in einem Mitgliedstaat gestellten Antrags auf internationalen Schutz zuständig ist und über der Gefahrenabwehr und Strafverfolgung dienende Anträge der Gefahrenabwehr- und Strafverfolgungsbehörden der Mitgliedstaaten und Europols auf den Abgleich mit Eurodac-Daten sowie zur Änderung der Verordnung (EU) Nr. 1077/2011 zur Errichtung einer Europäischen Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts (Neufassung), ABl. L 180 vom 29.6.2013, S. 1–30.

14 Vgl. LGBl. 2008 Nr. 273.

15 Die Details zu den damaligen Überlegungen dieser Neuzuordnung ergeben sich aus dem Bericht und Antrag Nr. 70/2008 sowie der Stellungnahme Nr. 97/2008 (und am Rande auch aus dem Bericht und Antrag Nr. 64/2011 zur Abänderung des Strafprozessordnung, des Opferhilfegesetzes und des Datenschutzgesetzes, S. 141 f.), auf welche an dieser Stelle verwiesen wird.

Die in den letzten rund zehn Jahren[16] gemachten Erfahrungen mit der organisatorischen Zuordnung der Datenschutzstelle zum Landtag haben erkennen lassen, dass diese Zuordnung in der praktischen Anwendung immer wieder zu verschiedenen Problemen führt, dies vor allem im Bereich der Personalführung und Personalbestellung. So erfolgt beispielsweise die Wahl des Datenschutzbeauftragten durch den Landtag über vorgängige Anhörung durch das Landtagspräsidium auf Vorschlag der Regierung (Art. 28a geltendes DSG). Das übrige Personal der Datenschutzstelle wird im Einvernehmen zwischen dem Datenschutzbeauftragten und dem Landtagspräsidium im Rahmen des vom Landtag bewilligten jährlichen Voranschlags angestellt (Art. 28b geltendes DSG). Der Voranschlag wiederum ist von der Datenschutzstelle nach Vorberatung durch die Geschäftsprüfungskommission bei der Regierung einzureichen, welche den Voranschlag unverändert zur Behandlung und Beschlussfassung an den Landtag weiterleitet (Art. 28c geltendes DSG). Diese verschiedenen Zuständigkeiten innerhalb des Landtags, des Landtagspräsidiums, der Geschäftsprüfungskommission und der Regierung bringen in der Anwendung Probleme mit sich bzw. verkomplizieren den jeweiligen Ablauf. So kann beispielsweise der Fall eintreten, dass das Landtagspräsidium einen Personalantrag gutheisst, die Geschäftsprüfungskommission aber das entsprechende Personalbudget nicht spricht.

Deshalb scheint es im Hinblick auf die dargestellten Probleme bzw. administrativen Abläufe bei der praktischen Anwendung der Zuordnung der Datenschutzstelle zum Landtag angebracht, diese zu überdenken bzw. abzuändern und die Datenschutzstelle organisatorisch neu wieder der Exekutive, konkret dem für den Geschäftsbereich Justiz zuständigen Ministerium, zuzuordnen. Abgesehen davon, dass es sich bei der Datenschutzstelle letztlich um ein das Gesetz vollziehendes Organ handelt und daher eine Zuordnung der Datenschutzstelle zum Landtag

---

[16] D.h. seit Inkrafttreten der Gesetzesänderung LGBl. 2008 Nr. 273.

bereits grundsätzlich dem Prinzip der Gewaltenteilung zu widersprechen scheint, lässt die DSGVO klar zu, dass die Datenschutzstelle der Exekutive zugeordnet werden kann. Im Gegensatz zur Datenschutzrichtlinie spricht die DSGVO denn auch nicht mehr von einer „Kontrollstelle“, sondern von einer „Aufsichtsbehörde“. Der Begriff „Aufsichtsbehörde“ bringt deutlich zum Ausdruck, dass es sich bei der Datenschutzstelle um eine Behörde, also ein der Exekutive zugeordnetes Organ handeln soll.

Dass es sich bei der Datenschutzstelle um eine Behörde handeln kann, zeigt sich auch im Vergleich mit der jeweils entsprechenden Rechtslage in Deutschland und Österreich.

In Deutschland ist der Bundesbeauftragte für den Datenschutz nach dem geltenden BDSG als eigenständige oberste Bundesbehörde eingerichtet, die seit anfangs 2016 keiner Aufsicht mehr unterliegt. Gewählt wird der Bundesbeauftragte vom Bundestag über Vorschlag der Bundesregierung.

In Österreich ist die Datenschutzbehörde eine dem Bundeskanzleramt organisationstechnisch angegliederte weisungsfreie Behörde. Der Leiter der Datenschutzbehörde wird auf Vorschlag der Bundesregierung vom Bundespräsidenten ernannt.

Abs. 1 der Gesetzesvorlage sieht daher neu vor, dass die Datenschutzstelle bei dem für den Geschäftsbereich Justiz zuständigen Ministerium eingerichtet ist.

Durch Art. 8 Abs. 1 und 2 werden Art. 54 Abs. 1 Bst. a DSGVO und Art. 44 Abs. 1 Bst. a DSRL-PJ durchgeführt bzw. umgesetzt. Art. 8 basiert auf § 8 der Rezeptionsvorlage.

**Zu Art. 9**

Abs. 1 legt die sachliche Zuständigkeit der Datenschutzstelle fest. Die Datenschutzstelle ist zuständig für die datenschutzrechtliche Aufsicht über alle öffentlichen Stellen und private Personen, gleich ob die Datenverarbeitung unter den Anwendungsbereich des EWR-Rechts/Schengen fällt oder nicht.

Abs. 2 regelt die Ausnahme der Aufsicht der Datenschutzstelle über die justizielle Tätigkeit der Gerichte. Die justizielle Tätigkeit der Gerichte unterliegt – wie bisher ähnlich in Art. 2 Abs. 3 Bst. c und d geltendes DSG – nicht der Aufsicht durch die Datenschutzstelle. Damit soll die Unabhängigkeit der Justiz bei der Ausübung ihrer gerichtlichen Aufgaben einschliesslich ihrer Beschlussfassung sichergestellt werden. Abs. 2 passt die bisherige Regelung, nach welcher die Gerichte nicht vom Geltungsbereich des DSG erfasst sind, an den Wortlaut der DSGVO bzw. der DSRL-PJ an. Hierdurch wird Art. 45 Abs. 2 Satz 1 DSRL-PJ umgesetzt; Art. 55 Abs. 3 DSGVO gilt hingegen unmittelbar.

Art. 9 basiert auf § 9 der Rezeptionsvorlage. Die Ausweitung auf nicht-öffentliche Stellen ist in der Rezeptionsvorlage in § 40 geregelt.

**Zu Art. 10**

Die wichtigste Vorgabe der DSGVO an die Aufsichtsbehörde – und damit für Liechtenstein an die Datenschutzstelle – besteht darin, dass die Aufsichtsbehörde bzw. die Datenschutzstelle bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig sein muss. So sieht der Erwägungsgrund 117 DSGVO vor, dass die völlige Unabhängigkeit der Aufsichtsbehörde ein wesentlicher Bestandteil des Schutzes natürlicher Personen bei der Verarbeitung personenbezogener Daten darstellt. Art. 51 Abs. 1 und Art. 52 Abs. 1 DSGVO sehen daher diese völlige Unabhängigkeit der Aufsichtsbehörde ausdrücklich vor.

Abs. 1 übernimmt die Vorgaben der DSGVO zur völligen Unabhängigkeit und sieht ausdrücklich vor, dass die Datenschutzstelle bei der Erfüllung der ihr zugewiesenen Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig und an keine Weisungen gebunden ist. Art. 52 Abs. 2 DSGVO verstärkt diese völlige Unabhängigkeit der Aufsichtsbehörde dergestalt, dass die Aufsichtsbehörde bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse weder direkter noch indirekter Beeinflussung von aussen unterliegt und sie weder um Weisungen ersucht noch Weisungen entgegennimmt. Mit diesem Abs. 1 werden die völlige Unabhängigkeit der Datenschutzstelle gewährleistenden Vorgaben aus Art. 52 Abs. 2 DSGVO übernommen und wird Art. 42 Abs. 1 und 2 DSRL-PJ zur Unabhängigkeit der Datenschutzstelle umgesetzt.

Abs. 2 trägt Art. 52 Abs. 6 erster Satzteil DSGVO und Art. 42 Abs. 6 erster Satzteil DSRL-PJ Rechnung. Demnach hat jeder Mitgliedstaat sicherzustellen, dass jede Aufsichtsbehörde einer Finanzkontrolle unterliegt, die ihre Unabhängigkeit nicht beeinträchtigt.

Wie aus Erwägungsgrund 118 DSGVO folgt, bedeutet die Unabhängigkeit der Aufsichtsbehörden nicht, dass sie hinsichtlich ihrer Ausgaben keinem Kontroll- oder Überwachungsmechanismus unterworfen sind. Als eine beim für den Geschäftsbereich Justiz zuständigen Ministerium eingerichtete Stelle untersteht die Datenschutzstelle analog einer Amtsstelle der von der Finanzkontrolle im Sinne des Gesetzes über die Finanzkontrolle ausgeübten Finanzaufsicht (Art. 11 Bst. b Ziff. 2 Gesetz vom 22. Oktober 2009 über die Finanzkontrolle (FinkG)[17].

Jedoch findet die Finanzkontrolle ihre Grenzen in der Unabhängigkeit der Datenschutzaufsicht. Die Haushalts- und Wirtschaftsführung der Datenschutzstelle unterliegt der Prüfung der Finanzkontrolle daher nur insoweit, als hierdurch die

---

[17] LGBI. 2009 Nr. 324, LR 615.0.

Unabhängigkeit nicht beeinträchtigt wird. Analog der Einsetzung der Finanzkontrolle als Revisionsstelle bei der Finanzmarktaufsicht Liechtenstein[18] gehört die Kontrolle der gesetzlichen Aufgaben der Datenschutzstelle nicht zu den Aufgaben der Finanzkontrolle. Dies obliegt den Beschwerdeinstanzen im Rahmen der Anfechtbarkeit von Entscheiden der Datenschutzstelle[19].

Durch die mit dieser Vorlage vorgesehene Einrichtung der Datenschutzstelle beim für den Geschäftsbereich Justiz zuständigen Ministerium entfallen die Vorschriften gemäss Art. 28c Abs. 1 geltendes DSG. Die Datenschutzstelle budgetiert ihre Aufwendungen im Rahmen des ordentlichen Budgetprozesses, welcher vom Landtag genehmigt werden muss. Mit dieser Bestimmung wird Erwägungsgrund 120 DSGVO und Art. 52 Abs. 6 DSGVO Genüge getan, welche regeln, dass jeder Mitgliedstaat vorsieht, dass die Aufsichtsbehörde über eigene, öffentliche, jährliche Haushaltspläne verfügt.

Art. 10 basiert auf § 10 der Rezeptionsvorlage mit den notwendigen Anpassungen hinsichtlich der liechtensteinischen Gegebenheiten.

**Zu Art. 11**

Art. 11 regelt in Durchführung der Art. 53 Abs. 1, Art. 54 Abs. 1 Bst. c und e DSGVO sowie in Umsetzung der Art. 43 Abs. 1, Art. 44 Abs. 1 Bst. c und e DSRL-PJ die Wahl und die Amtszeit des Leiters der Datenschutzstelle.

Erwägungsgrund 121 DSGVO und Art. 53 Abs. 1 DSGVO sehen vor, dass die Aufsichtsbehörde im Wege eines transparenten Verfahrens vom Parlament, der Regierung, dem Staatsoberhaupt oder von einer unabhängigen Stelle ernannt wird, die nach dem Recht des Mitgliedstaats mit der Ernennung betraut ist. Erwä-

---

18 Vgl. Art. 19 FMAG.

19 BuA 9/2004, zu Art. 20.

gungsgrund 121 DSGVO lässt ergänzend zu – setzt dies aber nicht voraus – dass die Aufsichtsbehörde von der Regierung, einem Mitglied der Regierung, dem Parlament oder einer Parlamentskammer für die Ernennung vorgeschlagen werden kann.

Aus Gründen der Vereinfachung des Ernennungsvorgangs wird das Auswahlverfahren gemäss dieser Vorlage ohne Vorschlagsrecht eines anderen Organs ausgestaltet und wird der Datenschutzbeauftragte, der – weisungsunabhängiger – Angestellter im Sinne des Staatspersonalgesetzes (StPG)[20] ist, daher von der Regierung gewählt.

Art. 28a Abs. 1 geltendes DSG sieht derzeit eine Amtszeit von acht Jahren vor. Liechtenstein kennt für gewählte Organe verschieden lange Amtszeiten, so beispielsweise eine vierjährige Amtszeit für politische Funktionen (z.B. Art. 47 Landesverfassung des Fürstentum Liechtensteins vom 5. Oktober 1921 (LV)[21] für die Landtagsabgeordneten und Art. 45 Abs. 1 Gemeindegesetz vom 20. März 1996[22] für die Mitglieder des Gemeinderats), eine fünfjährige Amtszeit für richterliche Funktionen (z.B. Art. 102 Abs. 2 LV für die Richter und Ersatzrichter des Verwaltungsgerichtshofs, Art. 3 Abs. 1 Gesetz vom 27. November 2003 über den Staatsgerichtshof (StGHG)[23] für die Richter und Ersatzrichter des Staatsgerichtshofs und Art. 16 Abs. 2 Richterdienstgesetz vom 24. Oktober 2007 (RDG)[24] für nebenamtliche Richter) und eine achtjährige Amtszeit für den Leiter der Finanzkontrolle (Art. 4 Abs. 2 FinKG). In Anlehnung an die achtjährige Amtszeit des Leiters der Finanzkontrolle – die Finanzkontrolle wird im Sinne von Art. 1 Abs. 1 und Art. 2 Abs. 2 FinKG unabhängig ausgeführt – rechtfertigt es sich, für den gleichfalls un-

---

20 LBGl. 2008 Nr. 144; LR 174.11.
21 LGBI. 1921 Nr. 15, LR 101.
22 LGBI. 1996 Nr. 76, LR 141.0.
23 LGBI. 2004 Nr. 32, LR 173.10.
24 LGBI. 2007 Nr. 347, LR 173.02.

abhängigen Datenschutzbeauftragten die in Art. 28a Abs. 1 geltendes DSG vorgesehene Amtszeit von acht Jahren beizubehalten. Eine lange Amtszeit ist dabei als Stärkung der Unabhängigkeit des Datenschutzbeauftragten zu verstehen. Aus diesem Grund soll die in Art. 28a Abs. 1 geltendes DSG vorgesehene Amtszeit von acht Jahren beibehalten werden.

Die DSGVO sieht zwar nicht ausdrücklich vor, dass eine Wiederwahl des Datenschutzbeauftragten zulässig ist, verbietet dies aber auch nicht ausdrücklich. An der in Art. 28a Abs. 1 geltendes DSG bereits vorgesehenen Möglichkeit der Wiederwahl des Datenschutzbeauftragten wird festgehalten, denn damit kann den Anforderungen an Erfahrung und einer gewissen Kontinuität für einen nachhaltigen Datenschutz Rechnung getragen werden.

Gemäss Abs. 2 muss der Leiter der Datenschutzstelle über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche persönliche und fachliche Eignung verfügen.

Art. 11 basiert auf § 11 der Rezeptionsvorlage, angepasst auf die liechtensteinischen Verhältnisse.

**Zu Art. 12**

Art. 12 regelt die Ausgestaltung, den Beginn und das Ende des Dienstverhältnisses des Leiters der Datenschutzstelle und regelt auch Fragen betreffend das übrige Personal der Datenschutzstelle.

Abs. 1 stellt klar, dass es sich sowohl beim Leiter der Datenschutzstelle als auch beim übrigen Personal um Staatsangestellte im Sinne des Staatspersonalgesetzes handelt. Gemäss Art. 8 StPG wird das Staatspersonal von der Regierung angestellt.

Abs. 1 Satz 2 stellt sicher, dass die Unabhängigkeit der Datenschutzstelle gewahrt bleibt. Das bedeutet, dass das Staatspersonalgesetz dort keine Anwendung auf den Leiter der Datenschutzstelle und das übrige Personal findet, wenn es um die Unabhängigkeit der Datenschutzstelle geht (z.B. Art. 10 Abs. 1 der Gesetzesvorlage).

Die Beendigung des Dienstverhältnisses des Leiters der Datenschutzstelle und des übrigen Personals bestimmt sich nach den Grundsätzen des Staatspersonalgesetzes, so dass es keiner weitergehender Regelungen nach Art. 54 Abs. 1 Bst. f DSGVO und Art. 44 Abs. 1 Bst. f DSRL-PJ bedarf, abgesehen von Abs. 2, 3 und 4.

Abs. 2 stellt sicher, dass der Leiter der Datenschutzstelle nur aus den im Gesetz angegebenen Gründen seines Amtes enthoben werden kann. Dies setzt Art. 43 Abs. 4 DSRL-PJ um und entspricht dabei Art. 53 Abs. 4 DSGVO. Schon jetzt regelt Art. 28a Abs. 3 geltendes DSG die vorzeitige Abberufung des Datenschutzbeauftragten. Diese bestehende Regelung ist jedoch an die strenger ausgestaltete Vorgabe der DSGVO und der DSRL-PJ anzupassen.

Abs. 3 bestimmt, dass die Regierung in begründeten Fällen das Dienstverhältnis nach Beendigung der Amtszeit um maximal sechs Monate verlängern kann.

Um der Vorgabe der DSGVO und der DSRL-PJ gerecht zu werden, wonach die Aufsichtsbehörde ihr eigenes Personal auswählt, sieht Abs. 4 vor, dass das übrige Personal der Datenschutzstelle von der Regierung auf Vorschlag des Datenschutzbeauftragten angestellt wird. Dies bedeutet im Kontext des Art. 52 Abs. 5 DSGVO und Art. 42 Abs. 6 DSRL-PJ, dass die Regierung in diesen Belangen keinen Einfluss auf die Auswahl durch den Leiter der Datenschutzstelle nehmen kann und darf. Sie hat das Personal wie vorgeschlagen anzustellen.

Art. 12 basiert auf § 12 der Rezeptionsvorlage mit entsprechenden Anpassungen im Hinblick auf die Gegebenheiten in Liechtenstein.

**Zu Art. 13**

Art. 13 regelt die Rechte und Pflichten des Leiters der Datenschutzstelle.

Abs. 1 Satz 1 enthält ein umfassendes Verbot sämtlicher nicht mit dem Amt zu vereinbarender Handlungen und Tätigkeiten, gleich ob entgeltlich oder unentgeltlich. Der Wortlaut entspricht Art. 52 Abs. 3 DSGVO, der aus Gründen der Verständlichkeit und Kohärenz auch für Art. 42 Abs. 3 DSRL-PJ gelten soll. Die Sätze 2 und 3 stellen eine Konkretisierung des allgemeinen Verbots der Ausübung mit dem Amt nicht zu vereinbarender Handlungen und Tätigkeiten nach Satz 1 dar. Hierdurch werden Art. 54 Abs. 1 Bst. f zweiter Satzteil DSGVO und Art. 44 Abs. 1 Bst. f zweiter Satzteil DSRL-PJ umgesetzt. Im Ergebnis führt die Bestimmung zu einem analogen Ergebnis wie Art. 28a Abs. 2 geltendes DSG.

Die Mitteilungspflicht des Leiters der Datenschutzstelle über Geschenke nach Abs. 2 ist eine Konkretisierung der aus Art. 52 Abs. 3 und Art. 54 Abs. 1 Bst. f zweiter Satzteil DSGVO und Art. 42 Abs. 3 und Art. 44 Abs. 1 Bst. f zweiter Satzteil DSRL-PJ folgenden Regelungsspielräume hinsichtlich Pflichten und Handlungsverbote. Diese Bestimmung ist analog zu Art. 39 StPG, wonach es den Angestellten untersagt ist, im Zusammenhang mit dienstlichen Angelegenheiten für sich oder einen Dritten Geschenke oder sonstige Vorteile zu fordern, anzunehmen oder sich versprechen zu lassen. Das Nähere ist in Art. 32 StPV geregelt, wonach die Annahme gewisser Geschenke vorbehaltlich der Zustimmung des Vorgesetzten zulässig ist. Die Unabhängigkeit der Datenschutzstelle steht einer solchen Genehmigung entgegen, doch soll wenigstens eine Mitteilungspflicht vorgesehen werden.

Abs. 3 regelt das Zeugnisverweigerungsrecht des Leiters der Datenschutzstelle und seiner Mitarbeitenden. Damit wird die effektive Aufgabenwahrnehmung der Datenschutzstelle gewährleistet.

Abs. 4 setzt Art. 54 Abs. 2 DSGVO und Art. 44 Abs. 2 DSRL-PJ zur Verschwiegenheitspflicht um.

Abs. 5 normiert, dass für den Leiter der Datenschutzstelle und das übrige Personal der Datenschutzstelle die Art. 84 (Verwaltungshilfe) und 85 (Anzeigepflicht) des Steuergesetzes nicht gelten. Eine Ausnahme hiervon besteht, soweit die Steuerbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben des Auskunftspflichtigen oder der für ihn tätigen Personen handelt.

Das Recht zur Zeugenaussage gemäss Abs. 6 steht in unmittelbarem Bezug zum Zeugnisverweigerungsrecht (Abs. 3) und der Verschwiegenheitspflicht (Abs. 4) des Leiters der Datenschutzstelle.

In Abs. 7 wird die Bestimmung des Art. 28a Abs. 4 geltendes DSG übernommen. Dies mit der Anpassung, dass das zu erlassende Organisationsreglement nunmehr von der Regierung zu genehmigen ist, zumal diese gemäss Art. 12 Abs. 6 Bst. b der Gesetzesvorlage für personalrechtliche Entscheide, die das übrige Personal betreffen, zuständig ist, sofern nicht der Datenschutzbeauftragte hierfür zuständig ist (Art. 12 Abs. 6 Bst. a der Gesetzesvorlage; das sind Angelegenheiten, die nach der Staatspersonalgesetzgebung dem Amtsstellenleiter zur selbständigen Erledigung übertragen sind).

Art. 13 basiert auf § 13 der Rezeptionsvorlage. Wiederum erfolgte eine Anpassung an liechtensteinische Gegebenheiten.

**Zu Art. 14**

Art. 14 Abs. 1 regelt die Aufgaben der Datenschutzstelle.

In Umsetzung des Art. 46 DSRL-PJ werden die in Art. 57 DSGVO vorgesehenen Aufgaben der Aufsichtsbehörden unter redaktioneller Anpassung des Wortlauts insoweit wiederholt, als sie inhaltlich deckungsgleich mit den Vorgaben der DSRL-PJ sind.

Soweit sich die Auflistung in Abs. 1 Satz 1 nicht explizit nur auf die DSGVO oder die DSRL-PJ bezieht, gelten die Aufgaben der Datenschutzstelle auch für Datenverarbeitungen, die nicht in den Anwendungsbereich des EWR-Rechts/Schengen fallen. Satz 2 setzt Art. 46 Abs. 1 Bst. g DSRL-PJ um; dieser hat in Art. 57 DSGVO keine Entsprechung.

Insofern die Datenschutzstelle im Rahmen der Aufgabenwahrnehmung nach Art. 14 Abs. 1 Ziff. 2 die Öffentlichkeit über die Risiken, Vorschriften, Garantien und Rechte in Zusammenhang mit der Verarbeitung personenbezogener Daten speziell von Kindern sensibilisiert und aufklärt, kann dies insbesondere in Zusammenarbeit mit den für den Kinder- und Jugendschutz zuständigen Stellen des Landes erfolgen. Zur Aufklärung und Sensibilisierung der Bevölkerung kann die Datenschutzstelle unter anderem Veranstaltungen durchführen, Vorträge halten, Informationsbroschüren erstellen, in Zeitungen und Sozialen Medien sowie auf Internetseiten Öffentlichkeitskampagnen durchführen.

In Bezug auf die Aufgabe der Datenschutzstelle, mit anderen Aufsichtsbehörden zusammenzuarbeiten und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung dieser Gesetzesvorlage und sonstiger Vorschriften zu gewährleisten (Abs. 1 Ziff. 7), kann für die nähere Definition der Amtshilfe auf Art. 61 DSGVO verwiesen werden, welcher direkt anwendbar ist.

Soweit die Datenschutzstelle in Abs. 1 Ziff. 8 zu Untersuchungen über die Anwendung dieser Gesetzesvorlage und sonstiger Vorschriften über den Datenschutz (Anwendung durch die Rechtsunterworfenen in der Praxis) berufen ist,

kann sie hierzu auch auf die Erkenntnisse anderer Aufsichtsbehörden oder anderer Behörden zurückgreifen.

Betreffend die Aufgabe der Datenschutzstelle gemäss Abs. 1 Ziff. 11, Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses zu leisten ist, wird auf den Katalog der Aufgaben des Datenschutzausschusses nach Art. 70 DSGVO verwiesen.

Abs. 1 Satz 2 verweist für den Bereich, welcher unter die DSRL-PJ fällt, auf Art. 55 der Gesetzesvorlage. Danach kann sich jede Person an die Datenschutzstelle richten, wenn sie der Auffassung ist, in ihren Rechten verletzt worden zu sein. Die Datenschutzstelle unterrichtet die betroffene Person über den Stand und das Ergebnis der Beschwerde.

Abs. 2 konkretisiert die Beratungsbefugnisse der Datenschutzstelle für den gesamten Anwendungsbereich des Gesetzes. Hierdurch wird Art. 47 Abs. 3 DSRL-PJ umgesetzt. Zugleich wird der Adressatenkreis des Art. 58 Abs. 3 Bst. b DSGVO konkretisiert, indem klargestellt wird, dass die Beratungsbefugnisse auch gegenüber allen sonstigen Einrichtungen und Stellen (z.B. öffentliche Stellen, die mit einem Leistungsauftrag versehen wurden (LAK, Familienhilfe etc.)) sowie den Kommissionen des Landtags bestehen.

Beispielsweise ergibt sich daraus i.V.m. Abs. 1 Satz 1 Ziff. 3, dass die Datenschutzstelle alle Vernehmlassungen auf ihre Datenschutzrelevanz hin zu prüfen hat. Des Weiteren kann der Landtag, eine seiner Kommissionen oder die Regierung die Datenschutzstelle direkt beauftragen, Nachforschungen zum Datenschutz bei öffentlichen Stellen anzustellen. Hierzu stehen der Datenschutzstelle die Möglichkeiten des Art. 58 DSGVO als auch Art. 16 der Gesetzesvorlage zur Verfügung. Diese Untersuchungsbefugnisse umfassen beispielsweise die Anweisung, Informationen bereitzustellen, Datenschutzüberprüfungen durchzuführen,

Hinweise auf vermeintliche Verstösse zu erteilen, Zugang zu allen personenbezogenen Daten und Informationen sowie zu den Geschäftsräumen, einschliesslich den Datenverarbeitungsanlagen und -geräten, zu erhalten.

Abs. 3 und 4 setzen Art. 46 Abs. 2 bis 4 DSRL-PJ in Übereinstimmung mit der Regelung des Art. 57 Abs. 2 bis 4 DSGVO um und legen fest, dass die Datenschutzstelle das Einreichen von Beschwerden etwa mit der Bereitstellung eines Beschwerdeformulars erleichtert und sich Betroffene grundsätzlich unentgeltlich an die Datenschutzstelle wenden können.

Art. 14 basiert auf § 14 der Rezeptionsvorlage, wobei eine Anpassung an die Situation in Liechtenstein erfolgt.

**Zu Art. 15**

Art. 15 bestimmt, dass die Datenschutzstelle einen jährlichen Bericht über ihre Tätigkeit zu erstellen hat. Der Bericht gilt sowohl für Datenverarbeitungen im Rahmen von Tätigkeiten, die dem EWR-Recht/Schengen unterstehen, als auch für solche, die nicht diesem Rechtsbestand unterstehen. Er hat über den Umfang und die Schwerpunkte der Tätigkeit sowie über Feststellungen und Empfehlungen und deren Umsetzung auszuführen. Der Bericht ergeht an den Landtag und die Regierung. Zudem ist er der Öffentlichkeit zugänglich zu machen. Dies entspricht auch den Vorgaben des in Art. 59 DSGVO und Art. 49 DSRL-PJ genannten Tätigkeitsberichts (Jahresbericht).

Art. 15 basiert auf § 15 der Rezeptionsvorlage, wobei eine Angleichung an Art. 31 geltendes DSG erfolgt ist.

**Zu Art. 16**

Art. 16 regelt für den gesamten Anwendungsbereich der Gesetzesvorlage die Befugnisse der Datenschutzstelle:

- Abs. 1 verweist für die Befugnisse und deren Ausübung im Anwendungsbereich der DSGVO auf Art. 58 DSGVO.
- Abs. 2 regelt die Befugnisse der Datenschutzstelle bei Datenverarbeitungen, deren Zwecke ausserhalb der DSGVO liegen.
- Abs. 3 und 4 gelten sowohl im Anwendungsbereich der DSGVO und der DSRL-PJ als auch ausserhalb der Vorgaben des EWR-Rechts/Schengen. Abs. 3 und 4 gelten somit für alle Bereiche.

Durch Abs. 1 wird sichergestellt, dass von der Datenschutzstelle festgestellte Verstösse gegen die Vorschriften des Datenschutzes der jeweils zuständigen Aufsichtsbehörde (z.B. FMA) mitgeteilt werden und diese unter Setzung einer angemessenen Frist Gelegenheit zur Stellungnahme erhält. Bei den übrigen Abhilfebefugnissen des Art. 58 Abs. 2 DSGVO[25] besteht hingegen kein Bedarf an einer vorherigen Information von Aufsichtsbehörden. Durch die Mitteilung wird insbesondere gewährleistet, dass die zuständige Aufsichtsbehörde Kenntnis von dem Verstoss erhält und vor der Ausübung weitergehender Befugnisse durch die Datenschutzstelle rechtliches Gehör findet. Die Gefahr divergierender Anweisungen zwischen Datenschutzaufsicht und der zuständigen Aufsichtsbehörden wird hierdurch reduziert. Widersprüchliche Auffassungen der Datenschutzaufsicht und der zuständigen Aufsichtsbehörden sind auf dem Gerichtsweg zu klären. Abs. 1 soll damit insbesondere das Zusammenwirken der unterschiedlichen nationalen Aufsichtsbehörden mit der Datenschutzstelle regeln. Ein solches Zusammenwirken kann sich insbesondere dann ergeben, wenn ein Verstoss gegen Daten-

[25] Die Abhilfebefugnisse sind: Die Warnung über voraussichtliche oder stattgefundene Verstösse; die Anweisung, den Rechten betroffener zu entsprechen; die Anweisung, Verarbeitungsvorgänge in Einklang mit der DSGVO zu bringen; die Anweisung der Benachrichtigung von betroffenen Personen über Verstösse; die Verhängung einer vorübergehenden oder endgültigen Beschränkung der Verarbeitung oder deren Verbot; die Berichtigung oder Löschung von Daten oder Einschränkung deren Verarbeitung samt Benachrichtigung der Empfänger; der Widerruf von Zertifizierungen; die Aussetzung der Übermittlung von Daten an Empfänger.

schutzvorschriften auch einen Verstoss gegen andere Bestimmungen, welche im Wirkungsbereich einer anderen Aufsichtsbehörde liegen, darstellt. So wäre es beispielsweise denkbar, dass ein datenschutzrechtlicher Verstoss einer Bank auch eine Aufsichtstätigkeit der FMA nach sich ziehen könnte.

Abs. 2 regelt die Befugnisse der Datenschutzstelle bei Datenverarbeitungen, deren Zwecke ausserhalb der DSGVO. Der Datenschutzstelle werden nach der Regelungssystematik in diesem Gesetz keine Durchgriffsbefugnisse gegenüber Verantwortlichen gegeben, die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Verwaltungsstraftaten (wobei die Verfolgung von Straftaten den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit umfasst) zuständig sind, soweit sie zu diesen Zwecken Daten verarbeiten. Dies folgt aus der unterschiedlichen Ausgestaltung der Abhilfebefugnisse in der DSGVO einerseits und der DSRL-PJ und den dort bestehenden fachlichen Bedürfnissen andererseits (richterliche Unabhängigkeit, Wahrung des Ermittlungsgeheimnisses etc.), weshalb die Richtlinie mehr Flexibilität eröffnet.

Im Bereich der Straftatenverhütung, -ermittlung und -verfolgung sowie der darauf bezogenen Gefahrenabwehr lassen sich Verfügungen der Datenschutzstelle nicht mit der Sensibilität und Komplexität der entsprechenden Verarbeitungen und dem Bedürfnis nach ständiger Verfügbarkeit rechtmässig erhobener Daten und Datenverarbeitungsanlagen in Einklang bringen. Dies gilt entsprechend für Verarbeitungen, die weder von der DSGVO noch von der DSRL-PJ gedeckt werden (z.B. Staatsschutz). Dem Leiter der Datenschutzstelle stehen daher anstelle von Verfügungen mit dem Instrument der Beanstandung, der Warnung und sonstigen Möglichkeiten (Telefonate, Gespräche etc.), den Verantwortlichen auf rechtswidrige Verarbeitungen aufmerksam zu machen, ausreichend andere Möglichkeiten zur Abhilfe zur Verfügung. Es bleibt dem Gesetzgeber unbenommen, in

Spezialgesetzen die in Abs. 2 genannten Befugnisse weiter auszugestalten und gegebenenfalls um Durchgriffsbefugnisse zu erweitern.

Um der Aufsicht über Datenschutz gerecht zu werden, ermöglicht Abs. 3 der Datenschutzstelle den Zugriff auf Daten, welche grundsätzlich dem Schutz von Art. 32 Abs. 1 LV unterliegen. Damit wird das Grundrecht der Privat- und Geheimsphäre eingeschränkt. Dabei sind die Grundzüge des rechtsstaatlichen Handelns, insbesondere die Verhältnismässigkeit, zu wahren. Für Berufsgeheimnisträger findet sich im Anwendungsbereich der DSGVO eine Spezialregelung in Art. 29 der Gesetzesvorlage.

Abs. 4 greift die Zugangs- und Informationsrechte der Datenschutzstelle auf. Hierdurch werden Art. 47 Abs. 1 DSRL-PJ umgesetzt und die (gemäss Art. 58 Abs. 1 Bst. f DSGVO) zur Ausübung der Untersuchungsbefugnisse notwendigen Verfahrensvorschriften für die Zugangs- und Betretensrechte von Grundstücken und Diensträumen geschaffen (Ziff. 1). Das umfassende Informationsrecht der Datenschutzstelle in Ziff. 2 erfolgt in Umsetzung des Art. 47 Abs. 1 DSRL-PJ in wortgleicher Anlehnung an Art. 58 Abs. 1 Bst. a DSGVO.

Abs. 5 legt einen Beratungs- und Unterstützungsauftrag der Datenschutzstelle gegenüber den Datenschutzbeauftragten fest. Es ergibt Sinn, dass diese von den Kenntnissen der Datenschutzstelle profitieren. Die Möglichkeit der Datenschutzbeauftragten, die Abberufung des Datenschutzbeauftragten zu verlangen, rechtfertigt sich durch die erforderliche Durchsetzung des Datenschutzes.

Abs. 6 legt eine Zweckbindung der Datenverarbeitung durch die Datenschutzstelle fest. Von dieser Zweckbindung kann unter den genannten Voraussetzungen (Interesse der betroffenen Person; erheblicher Nachteil für das Gemeinwohl, die öffentliche Sicherheit oder erheblicher Belange des Gemeinwohls; Verfolgung von Straftaten oder Verwaltungsstraftaten) abgewichen werden.

Art. 16 basiert auf § 16 der Rezeptionsvorlage, welcher auf die liechtensteinischen Gegebenheiten angepasst wird.

**Zu Art. 17**

Art. 68 DSGVO sieht die Einrichtung eines europäischen Datenschutzausschusses (im Folgenden als „Ausschuss“ bezeichnet) als Einrichtung der EU mit eigener Rechtspersönlichkeit vor. Der Ausschuss besteht aus dem Leiter der Aufsichtsbehörde jedes Mitgliedstaates sowie dem Europäischen Datenschutzbeauftragten oder ihren jeweiligen Vertretern. Nach Übernahme der DSGVO in das EWR-Abkommen werden die EWR-Staaten in diesem Ausschuss ebenfalls vertreten sind. Art. 17 der Gesetzesvorlage schafft für die Datenschutzstelle eine explizite Ermächtigung für den Einsitz in diesen Ausschuss.

Da sich die DSGVO aktuell noch im Übernahmeverfahren in das EWR-Abkommen befindet, ist die genaue Ausgestaltung der Einsitznahme noch nicht abschliessend geklärt. Es können sich hier daher noch Anpassungen ergeben.

**Zu Art. 18**

Art. 18 regelt die Zusammenarbeit der Datenschutzstelle mit anderen liechtensteinischen Aufsichtsbehörden mit Bezug auf die Einsitznahme der Datenschutzstelle im Ausschuss.

Die Datenschutzstelle vertritt Liechtenstein im Ausschuss und bringt damit im Tätigkeitsbereich des Ausschusses (siehe dazu Art. 70 DSGVO) die liechtensteinische Sichtweise ein. Da Datenschutz eine Materie ist, welche alle Lebensbereiche erfasst, können von der Tätigkeit des Ausschusses auch Bereiche erfasst sein, welche einer anderen Aufsichtsbehörde unterstellt sind. In solchen Fällen soll die Datenschutzstelle auch jene Aufsichtsbehörden einbinden können, bevor sie gegenüber dem Ausschuss ihre Stellungnahme abgibt. Der Ausschuss kann beispielsweise Leitlinien oder Empfehlungen erlassen. Betreffen diese Finanzmarkt-

akteure, welche der Aufsicht der FMA unterstehen, so kann die Datenschutzstelle nach dieser Bestimmung die FMA einbinden, bevor sie sich zu solchen Entwürfen des Ausschusses äussert.

**Zu Art. 19**

Art. 19 dient sowohl der Durchführung des Art. 78 Abs. 1 DSGVO als auch der Umsetzung des Art. 53 Abs. 1 DSRL-PJ. Danach hat jede natürliche oder juristische Person das Recht auf einen wirksamen Rechtsbehelf gegen einen sie betreffenden rechtsverbindlichen Beschluss einer Aufsichtsbehörde.

Der Klarheit halber sei an dieser Stelle erwähnt, dass Bussen und Strafen nach den dafür vorgesehenen Bestimmungen dieser Vorlage durch die ordentlichen Gerichte behandelt werden.

Der Verwaltungsrechtsweg (Abs. 1) stützt sich auf das Gesetz über die allgemeine Landesverwaltungspflege (LVG).

Gemäss Abs. 2 ist die Verwaltungsbeschwerdeinstanz als erste Beschwerdeinstanz vorgesehen. Abs. 3 sieht den Verwaltungsgerichtshof als zweite Beschwerdeinstanz vor.

Abs. 4 sieht vor, dass die Datenschutzstelle ergangene Entscheidungen anfechten kann. Dies entspricht den bisherigen Art. 29 Abs. 5 und Art. 30 Abs. 4 geltendes DSG. Diese Regelung setzt ein Erfordernis des Strassburger Übereinkommens vom 28. Januar 1981 zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten und dem dazugehörigen Zusatzprotokoll vom 8. November 2001 dar.

Nach Abs. 5 darf die Datenschutzstelle ihren Entscheiden oder Verfügungen gegenüber einer anderen Behörde die aufschiebende Wirkung nicht entziehen. Unbeschadet der Anordnungskompetenz der Datenschutzstelle stehen sich die

beteiligten Verwaltungsträger nicht in einem Subordinationsverhältnis gegenüber. Im Fall einer Verwaltungsstreitsache kann eine verbindliche Entscheidung allein durch die Verwaltungsgerichtsbarkeit getroffen werden.

**Zu Art. 20**

Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt. Art. 9 Abs. 2 DSGVO sieht jedoch Ausnahmen von diesem Verbot vor. In den Fällen des Art. 9 Abs. 2 Bst. b, g, h und i DSGVO sind die Ausnahmen durch nationale Regelungen auszugestalten. Neben einem Ausnahmetatbestand ist stets erforderlich, dass eine Rechtsgrundlage für die Verarbeitung nach Art. 6 Abs. 1 DSGVO vorliegt.

Abs. 1 legt fest, unter welchen Voraussetzungen die Verarbeitung besonderer Kategorien personenbezogener Daten ausnahmsweise zulässig ist. Durch die Stellung im zweiten Teil der Gesetzesvorlage findet die Regelung nur Anwendung für Verarbeitungen zu Zwecken gemäss Art. 2 DSGVO, also im sachlichen Anwendungsbereich der DSGVO. Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nicht nur auf dieser Rechtsgrundlage zulässig, sondern etwa auch auf der Grundlage der sich unmittelbar aus Art. 9 Abs. 2 DSGVO ergebenden Ausnahmetatbestände, einschliesslich sonstiger auf der Grundlage der DSGVO erlassener bereichsspezifischer Regelungen.

Auf Abs. 1 Ziff. 1 kann die Verarbeitung besonderer Kategorien personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen gleichermassen gestützt werden, während Abs. 1 Ziff. 2 nur Ausnahmetatbestände für öffentliche Stellen enthält. Im Einzelnen wird mit der Vorschrift von den Öffnungsklauseln des Art. 9 Abs. 2 Bst. b DSGVO (in Bezug auf Abs. 1 Ziff. 1 Bst. a), des Art. 9 Abs. 2 Bst. h i. V. m. Abs. 3 DSGOV (in Bezug auf Abs. 1 Ziff. 1 Bst. b), des Art. 9 Abs. 2 Bst. i DSGVO (in Bezug auf Abs. 1 Ziff. 1 Bst. c) und des Art. 9 Abs. 2 Bst. g DSGVO (in Bezug auf Abs. 1 Ziff. 2 Bst. a bis d) Gebrauch gemacht.

Abs. 1 Ziff. 1 Bst. b setzt Art. 9 Abs. 2 Bst. h DSGVO um. Die Verarbeitung erfolgt jeweils entsprechend den inhaltlichen Zwecken, die sich aus Bst. b oder den Spezialgesetzen ergeben. Mit der gewählten Formulierung wird klargestellt, dass ein Vertrag zwischen einem Patienten und einem Angehörigen eines Gesundheitsberufs gemeint ist. Daher findet die Regelung im Bereich der Humanmedizin beispielsweise für (Zahn-)Ärzte, Psychotherapeuten oder Kinder- und Jugendpsychotherapeuten Anwendung. Darüber hinaus werden auch Angehörige anderer Gesundheitsberufe erfasst.

Soweit es nach Abs. 1 Ziff. 1 Bst. b zulässig ist, dass „diese Daten von Fachpersonal oder unter dessen Verantwortung verarbeitet werden und dieses Fachpersonal dem Berufsgeheimnis unterliegt", sind auch die Erfüllungsgehilfen der genannten Gesundheitsberufe erfasst.

Der zweite Halbsatz in Abs. 1 Ziff. 1 Bst. c dient in Ausführung von Art. 9 Abs. 2 Bst. i DSGVO der Klarstellung: Das liechtensteinische Recht sieht bereits umfangreiche angemessene und spezifische Massnahmen zum Schutz des Berufsgeheimnisses vor, insbesondere durch Art. 121 StGB und die einschlägigen Berufsordnungen. Daneben können auch die in Abs. 2 genannten Massnahmen der Wahrung des Berufsgeheimnisses dienen.

Die Verarbeitung besonderer Kategorien personenbezogener Daten nach Abs. 1 Ziff. 2 erfordert zusätzlich eine Interessenabwägung, wie dies Art. 9 Abs. 2 Bst. g DSGVO vorsieht, indem die Verarbeitung in einem angemessenen Verhältnis zum verfolgten Zweck stehen und den Wesensgehalt des Rechts auf Datenschutz wahren muss.

Abs. 2 Satz 1 und 2 führt das Erfordernis aus Art. 9 Abs. 2 Bst. b, g und i DSGVO aus, „geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person“ bzw. „angemessene und spezifische Massnahmen zur Wahrung der

Grundrechte und Interessen der betroffenen Person“ vorzusehen. Die in Abs. 2 Satz 2 aufgeführten Massnahmen treffen jeden Verantwortlichen und damit auch jeden, der besondere Kategorien personenbezogener Daten verarbeitet.

Die in Art. 9 Abs. 2 Bst. h DSGVO (unter Bezugnahme auf den Art. 9 Abs. 3 DSGVO) geforderten besonderen Garantien sind unmittelbar durch Abs. 1 Ziff. 1 Bst. b umgesetzt und werden daher mit Abs. 2 Satz 3 von Abs. 2 ausgenommen.

Art. 20 entspricht § 22 der Rezeptionsvorlage.

**Zu Art. 21**

Die Vorschrift schafft für öffentliche Stellen im Rahmen der jeweiligen Aufgabenerfüllung eine nationale Rechtsgrundlage für die Verarbeitung personenbezogener Daten zu einem anderen Zweck als demjenigen, zu dem sie ursprünglich erhoben worden sind (Weiterverarbeitung). Soweit eine der tatbestandlichen Voraussetzungen nach Abs. 1 erfüllt ist, kann die Weiterverarbeitung personenbezogener Daten durch öffentliche Stellen auf diese Vorschrift gestützt werden. Dies gilt unabhängig davon, ob die Zwecke der Weiterverarbeitung mit den Zwecken, für welche die Daten ursprünglich erhoben wurden, nach Art. 6 Abs. 4 DSGVO vereinbar sind.

Abs. 2 stellt für die Weiterverarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 DSGVO klar, dass neben dem Vorliegen einer der tatbestandlichen Voraussetzungen des Abs. 1 auch ein Ausnahmetatbestand nach Art. 9 Abs. 2 DSGVO oder nach Art. 22 der Gesetzesvorlage vorliegen muss.

Mit der Vorschrift wird von dem durch die DSGVO eröffneten Regelungsspielraum Gebrauch gemacht, wonach die Mitgliedstaaten nationale Regelungen in Fällen, in denen der Zweck der Weiterverarbeitung nicht mit dem ursprünglichen Zweck vereinbar ist, erlassen dürfen, soweit die nationale Regelung eine „in einer

demokratischen Gesellschaft notwendige und verhältnismässige Massnahme zum Schutz der in Art. 21 Abs. 1 genannten Ziele darstellt“.

Art. 21 entspricht § 23 der Rezeptionsvorlage.

**Zu Art. 22**

Die Vorschrift schafft eine nationale Rechtsgrundlage für die Weiterverarbeitung personenbezogener Daten durch nicht-öffentliche Stellen. Soweit eine der tatbestandlichen Voraussetzungen nach Abs. 1 erfüllt ist, kann die Weiterverarbeitung personenbezogener Daten durch die nicht-öffentliche Stelle auf diese Vorschrift gestützt werden, unabhängig davon, ob die Zwecke der Weiterverarbeitung mit den ursprünglichen Zwecken, für die die Daten ursprünglich erhoben wurden, nach Art. 6 Abs. 4 DSGVO vereinbar sind.

Abs. 2 stellt für die Weiterverarbeitung besonderer Kategorien personenbezogener Daten klar, dass neben dem Vorliegen einer der tatbestandlichen Voraussetzungen des Abs. 1 auch ein Ausnahmetatbestand nach Art. 9 Abs. 2 DSGVO oder nach Art. 20 der Gesetzesvorlage vorliegen muss.

Mit der Vorschrift wird von dem durch die DSGVO eröffneten Regelungsspielraum Gebrauch gemacht, wonach die Mitgliedstaaten nationale Regelungen in Fällen, in denen der Zweck der Weiterverarbeitung nicht mit dem ursprünglichen Zweck vereinbar ist, erlassen dürfen, soweit die nationale Regelung eine „in einer demokratischen Gesellschaft notwendige und verhältnismässige Massnahme zum Schutz der in Art. 23 Abs. 1 DSGVO genannten Ziele darstellt“.

Art. 22 entspricht § 24 der Rezeptionsvorlage.

**Zu Art. 23**

Die Vorschrift schafft materiell eine nationale Rechtsgrundlage für die Übermittlung personenbezogener Daten durch öffentliche Stellen, soweit diese zu einem

anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, erfolgt. Die Norm findet auch auf den Fall Anwendung, in dem eine öffentliche Stelle Daten, die sie ursprünglich zu Zwecken nach Art. 40 der Gesetzesvorlage erhoben hat, an einen Dritten übermittelt, der die Daten zu Zwecken der DSGVO verarbeiten möchte.

Abs. 1 regelt die tatbestandlichen Voraussetzungen der Datenübermittlung an öffentliche Stellen. Die Regelung erfasst Datenübermittlungen, soweit diese zur Aufgabenerfüllung erforderlich sind. Eine Übermittlung ist gemäss dieser Vorschrift zulässig, wenn die Voraussetzungen für eine „Verarbeitung zu einem anderen Zweck“ nach Art. 21 der Gesetzesvorlage vorliegen.

Abs. 2 regelt die tatbestandlichen Voraussetzungen der Datenübermittlung an nicht-öffentliche Stellen. Die normierten Informationspflichten ergeben sich unmittelbar aus Art. 13 Abs. 3 bzw. Art. 14 Abs. 4 DSGVO.

Abs. 3 stellt für die Übermittlung besonderer Kategorien personenbezogener Daten klar, dass neben dem Vorliegen einer der tatbestandlichen Voraussetzungen der Abs. 1 oder 2 auch ein Ausnahmetatbestand nach Art. 9 Abs. 2 DSGVO oder nach Art. 20 der Gesetzesvorlage vorliegen muss.

Art. 23 entspricht § 25 der Rezeptionsvorlage.

**Zu Art. 24**

Die Öffnungsklausel des Art. 88 DSGVO lässt nationale Regelungen zur Datenverarbeitung im Beschäftigungskontext zu. Mit Art. 24 der Gesetzesvorlage erfährt diese Bestimmung eine Ausführung auf nationaler Ebene. Damit ist nicht ausgeschlossen, dass in Spezialgesetzen weitere Regelungen getroffen werden können, so beispielsweise für das Fragerecht bei der Begründung eines Beschäftigungsverhältnisses, den expliziten Ausschluss von heimlichen Kontrollen im Beschäftigungsverhältnis, die Begrenzung der Lokalisierung von Beschäftigten sowie den

Ausschluss von umfassenden Bewegungsprofilen, den Ausschluss von Dauerüberwachungen und die Verwendung biometrischer Daten zu Authentifizierungs- und Autorisierungszwecken.

Abs. 1 bestimmt, zu welchen Zwecken und unter welchen Voraussetzungen personenbezogene Daten vor, im und nach dem Beschäftigungsverhältnis verarbeitet werden dürfen, wenn dies zum Zweck des Beschäftigungsverhältnisses erforderlich ist.

Im Rahmen der Erforderlichkeitsprüfung sind die widerstreitenden Grundrechtspositionen abzuwägen. Dabei sind die Interessen des Arbeitgebers an der Datenverarbeitung und das Persönlichkeitsrecht des Beschäftigten in einen schonenden Ausgleich zu bringen, der beide Interessen möglichst weitgehend berücksichtigt.

Abs. 1 Satz 1 in Verbindung mit Abs. 5 stellt auch eine Umsetzung von Art. 10 DSGVO dar, der es den Staaten ermöglicht, die Verarbeitung personenbezogener Daten über strafrechtliche Verurteilungen und Straftaten oder damit zusammenhängende Massnahmen im Beschäftigungskontext (z.B. Tätigkeitsverbot) zuzulassen. Der Arbeitgeber kann auf diese Weise beispielsweise sicherstellen, dass die Beschäftigten keinem gesetzlichen oder gerichtlichen Verbot unterliegen und damit von bestimmten Beschäftigungen ausgenommen sind.

Ebenfalls von Satz 1 umfasst ist die Verarbeitung personenbezogener Daten zum Zweck des Beschäftigungsverhältnisses, wenn dies zur Ausübung oder Erfüllung der sich aus Gesetz oder Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Unter Kollektivvereinbarungen sind gemäss Erwägungsgrund 155 DSGVO auch Tarifverträge, Betriebsvereinbarungen und Dienstvereinbarungen zu verstehen.

Satz 2 benennt die Voraussetzungen für die Verarbeitung personenbezogener Daten von Beschäftigten zur Aufdeckung von Straftaten, die im Beschäftigungsverhältnis begangen worden sind.

Abs. 2 trägt der Besonderheit des Beschäftigungsverhältnisses als Abhängigkeitsverhältnis und der daraus resultierenden Situation der Beschäftigten Rechnung. Es handelt sich um eine spezifischere Vorschrift im Sinne von Art. 88 Abs. 1 DSGVO. Nach Erwägungsgrund 155 DSGVO können insbesondere Vorschriften über die Bedingungen erlassen werden, unter denen personenbezogene Daten im Beschäftigungskontext auf der Grundlage einer Einwilligung der Beschäftigten verarbeitet werden dürfen.

Bei der Beurteilung, ob eine Einwilligung freiwillig erteilt wurde, sind insbesondere die im Beschäftigungsverhältnis grundsätzlich bestehende Abhängigkeit des Beschäftigten vom Arbeitgeber und die Umstände des Einzelfalls zu berücksichtigen. Neben der Art der verarbeiteten Daten und der Eingriffstiefe ist beispielsweise auch der Zeitpunkt der Einwilligungserteilung massgebend. Vor Abschluss eines (Arbeits-)Vertrages werden Beschäftigte regelmässig einer grösseren Drucksituation ausgesetzt sein, eine Einwilligung in eine Datenverarbeitung zu erteilen. Satz 2 legt fest, dass eine freiwillige Einwilligung insbesondere vorliegen kann, wenn der Beschäftigte in Folge der Datenverarbeitung einen rechtlichen oder wirtschaftlichen Vorteil erlangt oder Arbeitgeber und Beschäftigter gleichgerichtete Interessen verfolgen. Die Gewährung eines Vorteils liegt beispielsweise in der Einführung eines betrieblichen Gesundheitsmanagements zur Gesundheitsförderung oder der Erlaubnis zur Privatnutzung von betrieblichen IT-Systemen. Auch die Verfolgung gleichgerichteter Interessen spricht für die Freiwilligkeit einer Einwilligung. Hierzu kann etwa die Aufnahme von Name und Geburtsdatum in eine Geburtstagsliste oder die Nutzung von Fotos für das Intranet

zählen, bei der Arbeitgeber und Beschäftigter im Sinne eines betrieblichen Miteinanders zusammenwirken.

Als formelle Voraussetzung einer Einwilligung ist grundsätzlich die Schriftform angeordnet, um die informationelle Selbstbestimmung der betroffenen Beschäftigten abzusichern. Damit wird die Nachweispflicht des Arbeitgebers im Sinne von Art. 7 Abs. 1 DSGVO konkretisiert. Hinzu kommt die Pflicht des Arbeitgebers zur Aufklärung in Textform über den Zweck der Datenverarbeitung und den jederzeit möglichen Widerruf durch den Beschäftigten sowie dessen Folgen nach Art. 7 Abs. 3 DSGVO.

Abs. 3 dient (neben Art. 20 Abs. 1 Ziff. 1 Bst. a der Gesetzesvorlage) der Ausführung von Art. 9 Abs. 2 Bst. b DSGVO. Im Einklang mit der Verordnung ist eine Verarbeitung besonderer Kategorien personenbezogener Daten zu Beschäftigungszwecken zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person am Ausschluss der Verarbeitung überwiegt. Die Verarbeitung besonderer Kategorien personenbezogener Daten für Zwecke des Beschäftigungsverhältnisses kann auch die Verarbeitung von Daten zur Beurteilung der Arbeitsfähigkeit einschliessen. Die Zulässigkeit der Verarbeitung besonderer Kategorien personenbezogener Daten für andere Zwecke bleibt unberührt; beispielsweise richtet sich diese im Fall der Verarbeitung zu Zwecken der Gesundheitsvorsorge nach Art. 20 Abs. 1 Ziff. 1 Bst. b der Gesetzesvorlage. Sollte eine Verarbeitung zugleich mehreren Zwecken dienen, gilt für den jeweiligen Zweck die jeweils einschlägige Verarbeitungsgrundlage. Neben der Verhältnismässigkeitsprüfung im Rahmen der Erforderlichkeit darf kein Grund zu der Annahme bestehen, dass die schutzwürdigen Interessen der Betroffenen die Interessen der Verantwortlichen an der Verarbeitung überwie-

gen. Die Vorschriften des Abs. 2 gelten auch für die Einwilligung in die Verarbeitung besonderer Kategorien personenbezogener Daten, wie beispielsweise von Gesundheitsdaten. Die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. An die Freiwilligkeit einer Einwilligung in die Datenverarbeitung besonderer Kategorien personenbezogener Daten sind strenge Anforderungen gestellt. Nach Art. 9 Abs. 2 Bst. b DSGVO muss die nationale Regelung geeignete Garantien für die Grundrechte und die Interessen der betroffenen Person vorsehen. Dem trägt der Verweis auf Art. 20 Abs. 2 der Gesetzesvorlage Rechnung.

Abs. 4 bestimmt, dass die Verarbeitung personenbezogener Beschäftigtendaten aufgrund von Kollektivvereinbarungen zulässig ist. Art. 88 Abs. 1 DSGVO ermöglicht es, spezifischere Regelungen zum Datenschutz im Beschäftigungskontext in Kollektivvereinbarungen zu treffen. Hinsichtlich besonderer Kategorien personenbezogener Daten beruht Abs. 4 auf Art. 9 Abs. 2 Bst. b DSGVO. Abs. 4 stellt in Umsetzung des Art. 88 Abs. 1 DSGVO klar, dass Kollektivvereinbarungen die Rechtsgrundlage für Regelungen zum Beschäftigtendatenschutz bilden können. Sie sollen den Verhandlungsparteien der Kollektivvereinbarungen die Ausgestaltung eines auf die betrieblichen Bedürfnisse zugeschnittenen Beschäftigtendatenschutzes ermöglichen. Dabei steht ihnen ein Ermessensspielraum im Rahmen des geltenden Rechts einschliesslich der DSGOV zu; Art. 88 Abs. 2 DSGVO ist zu beachten. Damit wird auch den Anforderungen des Art. 9 Abs. 2 Bst. b DSGVO bei der Verarbeitung besonderer Kategorien personenbezogener Daten Rechnung getragen.

Nach Abs. 5 muss der Verantwortliche geeignete Massnahmen zur Wahrung der Grundrechte und Interessen des Beschäftigten vorsehen. Beispielsweise muss bei der Datenverarbeitung sichergestellt sein, dass sie auf rechtmässige Weise, nach Treu und Glauben und in einer für den Beschäftigten nachvollziehbaren Weise erfolgt. Die Daten werden in einer Form gespeichert, welche die Identifizierung

des Beschäftigten nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, erforderlich ist. Der Verantwortliche stellt sicher, dass die Verarbeitung in einer Weise erfolgt, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet, einschliesslich des Schutzes vor unbefugter oder unrechtmässiger Verarbeitung. Er trifft sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der eigentlichen Verarbeitung geeignete technische und organisatorische Massnahmen, die darauf ausgelegt sind, die Datenschutzgrundsätze wie etwa die Datenminimierung wirksam umzusetzen. Der Verantwortliche unternimmt Schritte um sicherzustellen, dass ihm unterstellte natürliche Personen, die Zugang zu personenbezogenen Daten haben, diese nur aufgrund seiner Anweisung verarbeiten, es sei denn, diese sind rechtlich zur Verarbeitung verpflichtet. Damit wird insbesondere auch das Erfordernis aus Art. 10 DSGVO umgesetzt, geeignete Garantien für die Rechte und Freiheiten der Beschäftigten vorzusehen.

Abs. 6 stellt klar, dass die Rechte der Interessenvertretungen der Beschäftigten (z.B. des LANV oder interner Arbeitnehmervertretungen) unberührt bleiben.

Abs. 7 legt fest, dass die Abs. 1 bis 6 im Beschäftigungsverhältnis auch gelten, wenn personenbezogene Daten, einschliesslich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen. Er geht dabei von der Beschreibung des Anwendungsbereichs in Art. 2 Abs. 1 DSGVO aus.

Abs. 8 bestimmt, wer als Beschäftigter im Sinne dieser Vorlage gilt. In Ziff. 1 wird klargestellt, dass Leiharbeitnehmer nicht nur im Verhältnis zum Verleiher, sondern auch im Verhältnis zum Entleiher als Beschäftigte gelten.

Art. 24 entspricht § 26 der Rezeptionsvorlage.

**Zu Art. 25**

Mit Abs. 1, der für die öffentliche und private Forschung durch öffentliche und nicht-öffentliche Stellen gilt, wird von der Ermächtigung aus Art. 9 Abs. 2 Bst. j DSGVO Gebrauch gemacht, wonach die Verarbeitung besondere Kategorien personenbezogener Daten auch ohne Einwilligung der Betroffenen für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig ist.

Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt. Art. 9 Abs. 2 DSGVO sieht Ausnahmen von diesem Verbot vor. Die Ausnahmen gelten teilweise unmittelbar aufgrund der DSGVO (z.B. die ausdrückliche Einwilligung nach Art. 9 Abs. 2 Bst. a DSGVO). Mit Abs. 1 wird darüber hinaus auf Basis von Art. 9 Abs. 2 Bst. j eine zusätzliche Regelung im nationalen Recht für die Verarbeitung besonderer Kategorien personenbezogener Daten zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken geschaffen. Die Verarbeitung nach Abs. 1 setzt dabei das Vorliegen einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO voraus (z.B. gemäss Art. 6 Abs. 1 Bst. f eines berechtigten Interesses des Verantwortlichen).

Art. 9 Abs. 2 Bst. j DSGVO erfordert, dass eine Forschungsklausel in angemessenem Verhältnis zu dem verfolgten Ziel steht, den Wesensgehalt des Rechts auf Datenschutz wahrt und angemessene und spezifische Massnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsieht. Dem trägt der Verweis auf Art. 20 Abs. 2 Satz 2 der Gesetzesvorlage Rechnung.

Abs. 1 gilt nur für die Verarbeitung von Daten im Sinne von Art. 9 Abs. 1 DSGVO. Die Verarbeitung von nicht unter Art. 9 fallenden Daten richtet sich entweder unmittelbar nach der DSGVO (insbesondere Art. 6 Abs. 1) oder nach im Einklang mit der DSGVO erlassenen Rechtsgrundlagen des EWR- oder nationalen Gesetz-

gebers. Nationale Vorschriften finden sich in der gegenständlichen Gesetzesvorlage oder in Spezialgesetzen.

Für die Weiterverarbeitung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen gilt: Nach Art. 5 Abs. 1 Bst. b DSGVO gilt eine Weiterverarbeitung für wissenschaftliche oder historische Forschungszwecke und für statistische Zwecke nicht als unvereinbar mit den ursprünglichen Zwecken. Da diese Zwecke bei der Weiterverarbeitung kompatibel mit dem Zweck der Erstverarbeitung sind, kann sich der Verantwortliche als Rechtsgrundlage erneut auf die Rechtsgrundlage stützen, die bereits für die Erstverarbeitung galt.

Dies trifft auch auf die Weiterverarbeitung besonderer Kategorien personenbezogener Daten zu, für die Art. 25 Abs. 1 der Gesetzesvorlage als Ausnahmetatbestand vom Verbot des Art. 9 Abs. 1 DSGVO gilt. Art. 21 und 22 der Gesetzesvorlage finden insoweit keine Anwendung. Entsprechendes gilt für die Übermittlung besonderer Kategorien von Daten durch öffentliche Stellen zu wissenschaftlichen oder historischen und statistischen Forschungszwecken; Art. 23 der Gesetzesvorlage findet insoweit keine Anwendung.

Abs. 2 Satz 1 schränkt unter Ausnutzung der Öffnungsklausel des Art. 89 Abs. 2 DSGVO die Rechte nach den Art. 15, 16, 18 und 21 DSGVO ein, indem die Rechte der Betroffenen beschränkt werden, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Diese Einschränkung der Betroffenenrechte in Abs. 2 gilt für alle Kategorien personenbezogener Daten.

Im Sinne des Abs. 2 Satz 1 kann die Verwirklichung des Forschungszwecks in bestimmten Einzelfällen ohne Einschränkungen des Auskunftsrechts aus Art. 15

DSGVO beispielsweise dann unmöglich sein, wenn sie beispielsweise ethisch nicht tragbar wäre.

Darüber hinaus schränkt Abs. 2 Satz 2 das Auskunftsrecht für die Fälle unverhältnismässigen Aufwands unter Ausnutzung der Öffnungsklausel des Art. 23 Abs.1 Bst. i DSGVO ein. Dies kann beispielsweise dann der Fall sein, wenn ein Forschungsvorhaben mit besonders grossen Datenmengen arbeitet.

Soweit spezialgesetzliche Regelungen zur Datenverarbeitung aus den Spezialgesetzen anzuwenden sind, gehen sie Art. 25 der Gesetzesvorlage vor.

Art. 25 entspricht § 27 der Rezeptionsvorlage.

**Zu Art. 26**

Art. 26 regelt die Datenverarbeitung für im öffentlichen Interesse liegende Archivzwecke und gilt für die Verarbeitung personenbezogener Daten durch öffentliche und nicht-öffentliche Stellen. Er bezieht sich sowohl auf öffentliches als auch privates Archivgut.

Mit Abs. 1 wird von der Ermächtigung aus Art. 9 Abs. 2 Bst. j DSGVO Gebrauch gemacht. Nach Art. 9 Abs. 1 DSGVO ist die Verarbeitung besonderer Kategorien personenbezogener Daten grundsätzlich untersagt. Art. 9 Abs. 2 DSGVO sieht Ausnahmen von diesem Verbot vor. Die Ausnahmen gelten teilweise unmittelbar aufgrund der DSGVO (z.B. die ausdrückliche Einwilligung nach Art. 9 Abs. 2 Bst. a DSGVO). Mit 26 Abs. 1 wird darüber hinaus auf Basis von Art. 9 Abs. 2 Bst. j DSGVO im nationalen Recht ein zusätzlicher Ausnahmetatbestand für die Verarbeitung besonderer Kategorien personenbezogener Daten für Archivzwecke geschaffen. Der Verweis in Abs. 1 auf den Beispielskatalog des Art. 20 Abs. 2 Satz 2 der Gesetzesvorlage hat nicht zur Folge, dass die Anwendung mindestens einer genannten Massnahme bei der Verarbeitung besonderer Kategorien von Daten zu im öffentlichen Interesse liegenden Archivzwecken zwingend ist. Vielmehr

können auch andere angemessene und spezifische Massnahmen getroffen werden.

Abs. 1 gilt nur für die Verarbeitung von Daten im Sinne von Art. 9 Abs. 1 DSGVO (besondere Kategorien personenbezogener Daten). Die Verarbeitung von nicht unter Art. 9 DSGVO fallenden Daten richtet sich entweder unmittelbar nach der DSGVO (insbesondere Art. 6 Abs. 1) oder nach im Einklang mit der DSGVO erlassenen Rechtsgrundlagen des EWR- oder nationalen Gesetzgebers. Nationale Vorschriften finden sich in der gegenständlichen Gesetzesvorlage oder in Spezialgesetzen.

Für die Weiterverarbeitung gilt: Nach Art. 5 Abs. 1 Bst. b DSGVO gilt eine Weiterverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken nicht als unvereinbar mit den ursprünglichen Zwecken. Daher kann sich der Verantwortliche hinsichtlich der Rechtsgrundlage für die Weiterverarbeitung erneut auf die Rechtsgrundlage stützen, die bereits für die Erstverarbeitung galt. Art. 21, 22 und 23 der Gesetzesvorlage finden keine Anwendung. Will der Verantwortliche aber besondere Kategorien von Daten weiterverarbeiten, benötigt er nicht nur eine Rechtsgrundlage, sondern auch einen Ausnahmetatbestand vom Verbot nach Art. 9 Abs. 1 DSGVO. Er muss mithin auch bei der Weiterverarbeitung Art. Abs. 1 beachten.

In den Abs. 2 bis 4 werden unter Ausnutzung der Öffnungsklausel des Art. 89 Abs. 3 DSGVO die Rechte gemäss der Art. 15, 16, 18, 20 und 21 DSGVO eingeschränkt. Die Ausnahme gemäss Abs. 2 bezieht sich auf sämtliche durch Art. 15 DSGVO gewährten Rechte, insbesondere auch auf das Recht auf Erhalt einer Kopie. Die Abs. 2 bis 4 gelten für die Verarbeitung sämtlicher personenbezogener Daten, einschliesslich besonderer Kategorien personenbezogener Daten.

**Zu Art. 27**

Auf der Grundlage der Öffnungsklausel des Art. 23 Abs. 1 Bst. i DSGVO beschränkt Abs. 1 gegenüber Geheimnisträgern das Recht auf Information und Auskunft. Satz 2 beschränkt die Betroffenenrechte auch für die Fälle, in denen Informationen „nach einer Rechtsvorschrift“ geheim gehalten werden müssen; Satz 1 bezieht sich nicht auf diese nach Rechtsvorschriften bestehenden Geheimhaltungspflichten, da die Informationspflicht hier bereits unmittelbar durch Art. 14 Abs. 5 Bst. d DSGVO beschränkt wird. Sätze 3 und 4 beziehen sich auf eine Beschränkung der Benachrichtigungspflicht nach Art. 34 DSGVO.

Abs. 2 dient dem Schutz der ungehinderten Kommunikation zwischen Mandant und Berufsgeheimnisträger. Wirtschaftsprüfer und Rechtsanwälte werden oftmals nicht (nur) mit der Verfolgung von Rechtsansprüchen (vgl. hierzu Art. 29 Abs. 1 Ziff. 4 der Gesetzesvorlage), sondern mit vielfältigen Beratungsdienstleistungen (Steuerberatung, Begleitung von Unternehmenstransaktionen, Gutachter- und Sachverständigentätigkeit etc.) beauftragt. Es widerspräche dem besonderen Schutz des Mandatsverhältnisses, wenn der Mandant in jedem Fall sämtliche durch die Datenübermittlung an den Berufsgeheimnisträger betroffenen Personen über die Zwecke der Datenübermittlung, die Identität der beauftragten Berufsgeheimnisträger etc. informieren müsste. Durch die in Abs. 2 letzter Halbsatz eingefügte Abwägungsklausel wird den Rechten der Betroffenen angemessen Rechnung getragen. Die Einschränkung der Informationspflicht beruht auf der Öffnungsklausel des Art. 23 Abs. 1 Bst. i DSGVO.

Abs. 3 Satz 1 macht von der Öffnungsklausel des Art. 90 DSGVO Gebrauch, ihr entspricht Erwägungsgrund 164 DSGVO. Nach Art. 58 Abs. 1 Bst. e und f DSGVO haben die Aufsichtsbehörden die Befugnis, vom Verantwortlichen und vom Auftragsverarbeiter zu allen für die Erfüllung ihrer Aufgaben notwendigen personenbezogenen Daten und Informationen sowie zu den Geschäftsräumen, ein-

schliesslich aller Datenverarbeitungsanlagen und -geräte, Zugang zu erhalten. Art. 90 Abs. 1 DSGVO eröffnet den Mitgliedstaaten die Möglichkeit, die Befugnisse der Aufsichtsbehörden im Sinne des Art. 58 Abs. 1 Bst. e und f DSGVO gegenüber Geheimnisträgern zu regeln. Mit Abs. 3 Satz 1 wird diese Möglichkeit insbesondere dergestalt umgesetzt, dass eine Aufsichtsbehörde entgegen Art. 58 Abs. 1 Bst. e DSGVO dann keinen Zugang zu Daten und Informationen hat, soweit dadurch die Geheimhaltungspflicht verletzt würde. Ohne eine Einschränkung der Befugnisse der Aufsichtsbehörden käme es zu einer Kollision mit Pflichten des Geheimnisträgers. Gerade bei den freien Berufen schützt die berufsrechtliche Schweigepflicht das Vertrauen des Mandanten und der Öffentlichkeit in den Berufsstand. Das Mandatsverhältnis soll nicht mit Unsicherheiten hinsichtlich seiner Vertraulichkeit belastet sein. Abs. 3 Satz 2 verlängert die Geheimhaltungspflicht auf die Aufsichtsbehörde. Berufsgeheimnisträger bedienen sich vermehrt externer IT-Dienstleister und verpflichten diese als Auftragsverarbeiter vertraglich zur Verschwiegenheit. Um zu vermeiden, dass die Auftragsverarbeiter vertragsbrüchig werden, wenn sie die ihnen anvertrauten Daten gegenüber der Aufsichtsbehörde offenlegen müssten, umfasst Abs. 3 auch den Auftragsverarbeiter.

Art. 27 entsprich § 29 der Rezeptionsvorlage.

**Zu Art. 28**

Die Bestimmung zu Auskunfteien (Unternehmen, die gewerbsmässig Auskünfte über private oder geschäftliche Verhältnisse anderer, besonders über deren Kreditwürdigkeit erteilen) und Scoring (auf dem Scoringmodell basierende Überprüfung der Kreditwürdigkeit eines Unternehmens oder einer Privatperson) dient dem Schutz des Wirtschaftsverkehrs. Ihnen kommt für Betroffene wie auch für die Wirtschaft eine überragende Bedeutung zu. Verbraucher vor Überschuldung zu schützen, liegt sowohl im Interesse der Verbraucher als auch der Wirtschaft. Die Ermittlung der Kreditwürdigkeit und die Erteilung von Bonitätsauskünften

bilden das Fundament des Kreditwesens und damit der Funktionsfähigkeit der Wirtschaft.

Die Regelung legt fest und konkretisiert, welche Voraussetzungen ein von einer Auskunftei ermittelter Score-Wert im Hinblick auf so genannte Negativ-Merkmale erfüllen muss, damit er im Wirtschaftsverkehr verwendet werden darf. Die Kriterien begrenzen die Zulässigkeit der Ermittlung von Score-Werten in bestimmten Fällen und schaffen so einen angemessenen Ausgleich der widerstreitenden Interessen, beispielsweise dadurch, dass Auskunfteien offene Forderungen nur dann gemeldet werden dürfen und dort verarbeitet werden können, wenn sie unbestritten oder tituliert sind. Die Bestimmung lässt die Vorschriften des allgemeinen Datenschutzrechts über die Zulässigkeit der Verarbeitung von personenbezogenen Daten unberührt. Dies betrifft etwa unter anderem auch die Übermittlung und Verwendung für die Ermittlung von Wahrscheinlichkeitswerten von personenbezogenen Daten über die Begründung, ordnungsgemässe Durchführung und Beendigung eines Vertragsverhältnisses eines Geschäfts mit finanziellem Ausfallrisiko (Positivdaten).

Insoweit wird für alle Beteiligten Sicherheit in der Weise geschaffen, dass Scoringverfahren und Kreditinformationssysteme mit der Meldung von Positiv- und Negativdaten, die beispielsweise durch Kreditinstitute, Finanzdienstleistungsunternehmen, Zahlungsinstitute, Telekommunikations-, Handels-, Energieversorgungs- und Versicherungsunternehmen oder Leasinggesellschaften erfolgt, prinzipiell weiter zulässig bleiben.

Art. 28 entsprich § 31 der Rezeptionsvorlage.

**Zu Art. 29 bis 34 – Rechte der betroffenen Person (Kapitel 2)**

Art. 23 DSGVO sieht vor, dass die Rechte und Pflichten gemäss den Art. 12 bis 22 und Art. 34 sowie die in Art. 5 geregelten Grundsätze für die Verarbeitung perso-

nenbezogener Daten, sofern deren Bestimmungen den in den Art. 12 bis 22 vorgesehenen Rechten und Pflichten entsprechen, durch nationale oder EWR-Rechtsvorschriften beschränkt werden können. Die Beschränkung muss allerdings den Wesensgehalt der Grundrechte und Grundfreiheiten achten und eine notwendige und verhältnismässige Massnahme darstellen, um die in Art. 23 Abs. 1 Bst. a bis j DSGVO aufgezählten Ziele sicherzustellen.

Art. 23 DSGVO verlangt deshalb besondere Massnahmen zum Schutz der Grundrechte und Grundfreiheiten der von der Beschränkung betroffenen Person. Vor allem muss gemäss Art. 23 Abs. 2 DSGVO jede Gesetzgebungsmassnahme „gegebenenfalls spezifische Vorschriften" zumindest in Bezug auf die in Art. 23 Abs. 2 Bst. a bis h DSGVO aufgezählten Massnahmen[26] enthalten.

Die in Kapitel 2 vorgenommenen Einschränkungen der Betroffenenrechte und Pflichten des Verantwortlichen und Auftragsverarbeiters ergänzen die in der DSGVO unmittelbar vorgesehenen Ausnahmen.

Die Beschränkungen der Betroffenenrechte in Kapitel 2 finden auch Anwendung auf die in Art. 89 DSGVO geregelte Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken, zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken. Zwar bestimmt Art. 89 Abs. 2 und 3 DSGVO, dass bei einer Verarbeitung zu den dort genannten Forschungs- und statistischen Zwecken Mitgliedstaaten insoweit Ausnahmen von den Rechten gemäss der Art. 15, 16, 18 und 21 DSGVO sowie bei der Verarbeitung zu im öffentlichen Interesse liegenden Archivzwecken zusätzlich Art. 19 und 20 vorsehen können. Dies aber nur insofern, als diese Rechte voraussichtlich die Verwirklichung der spezifischen

[26] Zwecke der Verarbeitung, Kategorien personenbezogener Daten, Umfang der Beschränkungen, Garantien gegen Missbrauch, unrechtmässigen Zugang oder unrechtmässige Übermittlung, Angaben zum Verantwortlichen, Speicherfristen, Risiken für die Rechte und Freiheiten der betroffenen Personen und das Recht der betroffenen Personen auf Unterrichtung über die Beschränkung.

Zwecke unmöglich machen oder ernsthaft beeinträchtigen und solche Ausnahmen für die Erfüllung dieser Zwecke notwendig sind. Eine Beschränkung der Betroffenenrechte muss jedoch nicht nur nach Art. 89 Abs. 2 und 3 DSGVO, sondern auch nach Art. 23 DSGVO möglich sein, da die Verarbeitung zu den in Art. 89 DSGVO genannten Zwecken andernfalls gegenüber sonstigen Verarbeitungen schlechter gestellt wäre. Dies, obwohl die DSGVO die Verarbeitung zu Archiv-, Forschungs- und Statistikzwecken mit der Sonderreglung in Kapitel IX DSGVO privilegieren wollte.

**Zu Art. 29**

Art. 29 regelt die Beschränkung der Informationspflicht bei der Erhebung von personenbezogenen Daten bei der betroffenen Person.

Die in Abs. 1 vorgesehene Beschränkung der Informationspflicht gilt nur für die in Art. 13 Abs. 3 DSGVO vorgesehene Fallgruppe, dass der Verantwortliche beabsichtigt, die personenbezogenen Daten für einen anderen Zweck weiterzuverarbeiten als den, für den die Daten bei der betroffenen Person erhoben wurden. Die Informationspflicht aus Art. 13 Abs. 1 und 2 DSGVO wird demgegenüber nicht beschränkt.

Die mit der DSGVO erstmals eingeführte (Folge-)Informationspflicht des Verantwortlichen bei beabsichtigter Zweckänderung hat bis jetzt keine Entsprechung im geltenden Datenschutzgesetz. In dieser Konstellation besteht im Gegensatz zu der in Art. 13 Abs. 1 und 2 DSGVO vorgesehenen Informationspflicht zum Zeitpunkt der Erhebung der Daten typischerweise kein unmittelbarer Kontakt zwischen dem Verantwortlichen und der betroffenen Person. In diesen Fällen kann sich die Information der betroffenen Person als unverhältnismässig erweisen.

Abs. 1 Ziff. 1 sieht daher eine Ausnahme von der Informationspflicht nach Art. 13 Abs. 3 DSGVO vor, wenn die Weiterverarbeitung analog gespeicherter Daten

betroffen ist, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem ursprünglichen Erhebungszweck vereinbar ist und die Kommunikation nicht in digitaler Form erfolgt. Zudem muss das Interesse der betroffenen Person an der Informationserteilung als gering anzusehen sein.

Die Ziff. 2 und 3 enthalten speziell für öffentliche Stellen geltende Einschränkungen der Informationspflicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung die ordnungsgemässe Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben gefährden (Ziff. 2) oder die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Landes Nachteile bereiten würde (Ziff. 3). Einschränkende Voraussetzung ist in beiden Fällen, dass die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen.

Ziff. 4 sieht eine Einschränkung zur Sicherstellung der Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor (Art. 23 Abs. 1 Bst. j DSGVO).

Ziff. 5 schützt die vertrauliche Übermittlung von Daten an öffentliche Stellen (Art. 23 Abs. 1 Bst. e DSGVO). Erfasst sind beispielsweise Fallgruppen, in denen die Information der betroffenen Person über die Weiterverarbeitung zu einer Vereitelung oder ernsthaften Beeinträchtigung des – legitimen – Verarbeitungszwecks führen würde, etwa wenn die zuständige Strafverfolgungsbehörde über den Verdacht einer Straftat informiert werden soll.

Abs. 2 legt fest, dass der Verantwortliche geeignete Massnahmen zum Schutz der berechtigten Interessen der betroffenen Person zu treffen hat, wenn eine Information der betroffenen Person gemäss Abs. 1 unterbleibt. Hierdurch werden die nach Art. 23 Abs. 2 DSGVO erforderlichen Schutzmassnahmen beachtet. Zu den geeigneten Massnahmen zählt die Bereitstellung dieser Informationen für die

Öffentlichkeit. Eine Veröffentlichung in allgemein zugänglicher Form kann etwa die Bereitstellung der Information auf einer allgemein zugänglichen Webseite des Verantwortlichen sein (Erwägungsgrund 58 Satz 2 DSGVO). Die Information hat in Entsprechung zu Art. 12 Abs. 1 DSGVO in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache zu erfolgen.

Der Verantwortliche hat schriftlich festzuhalten, aus welchen Gründen er von einer Information abgesehen hat. Die Stichhaltigkeit der Gründe unterliegt der Kontrolle durch die Datenschutzstelle, die durch die Dokumentationspflicht ermöglicht wird. Die in Abs. 2 Satz 1 und 2 zum Schutz der berechtigten Interessen der betroffenen Person geforderten Massnahmen des Verantwortlichen finden im Fall des Abs. 1 Ziff. 4 und 5 keine Anwendung. Andernfalls könnten die in Satz 1 und 2 geforderten Massnahmen zu einer Vereitelung oder ernsthaften Beeinträchtigung des – legitimen – Verarbeitungszwecks führen.

Abs. 3 bestimmt, dass der Verantwortliche die Information der betroffenen Person zeitnah nachzuholen hat, wenn die Ausschlussgründe des Abs. 1 nur vorübergehend vorliegen.

Art. 29 entsprich § 32 der Rezeptionsvorlage.

**Zu Art. 30**

Art. 30 regelt die Beschränkung der Informationspflicht, wenn die personenbezogenen Daten nicht bei den betroffenen Personen erhoben wurden.

Abs. 1 Ziff. 1 gilt nur für öffentliche Stellen. Für die Erläuterungen wird auf die Erläuterungen zu Art. 29 Abs. 1 Ziff. 2 und 3 der Gesetzesvorlage verwiesen.

Abs. 1 Ziff. 2 gilt nur für nicht-öffentliche Stellen. Der Ausnahmetatbestand ist gegeben, wenn die Erteilung der Information die Geltendmachung, Ausübung

oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Verarbeitung Daten aus zivilrechtlichen Verträgen beinhaltet und der Verhütung von Schäden durch Straftaten dient. Einen Anwendungsfall können Datenverarbeitungen zur Verfolgung zivilrechtlicher Ansprüche darstellen (Art. 23 Abs. 1 Bst. j DSGVO).

Die vorgesehene Beschränkung der Informationspflicht dient den Zielen der nationalen Sicherheit (Art. 23 Abs. 1 Bst. a DSGVO), der Landesverteidigung (Art. 23 Abs. 1 Bst. b DSGVO), der öffentlichen Sicherheit (Art. 23 Abs. 1 Bst. c DSGVO), der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit (Art. 23 Abs. 1 Bst. d DSGVO) sowie sonstiger wichtiger Ziele des allgemeinen öffentlichen Interesses des Landes (Art. 23 Abs. 1 Bst. e DSGVO).

Abs. 2 entspricht im Wesentlichen Art. 29 Abs. 2 Satz 1 und 2 der Gesetzesvorlage und es wird auf die dortige Begründung verwiesen.

Abs. 3 betrifft den Fall der Informationserteilung an die Landespolizei zu Zwecken der nationalen Sicherheit.

Art. 30 entsprich § 33 der Rezeptionsvorlage.

**Zu Art. 31**

Art. 31 regelt die Beschränkung des Auskunftsrechts der betroffenen Person. Abs. 1 enthält ergänzend zu den in Art. 25 Abs. 2, Art. 26 Abs. 2 und Art. 27 Abs. 1 Satz 2 der Gesetzesvorlage genannten Ausnahmen Einschränkungen des Auskunftsrechts der betroffenen Person. Die Abs. 2 und 3 regeln Massnahmen zum Schutz der Rechte und Freiheiten der betroffenen Person.

Abs. 1 Ziff. 1 verweist für das Auskunftsrecht auf die Beschränkungen des Art. 30 Abs. 1 und 3 der Gesetzesvorlage.

Gemäss Abs. 1 Ziff. 2 hat der Verantwortliche jedoch sicherzustellen, dass durch geeignete technische und organisatorische Massnahmen eine Verwendung der Daten zu anderen Zwecken ausgeschlossen ist. Bei der Ermittlung des Aufwands hat der Verantwortliche die bestehenden technischen Möglichkeiten, gesperrte und archivierte Daten der betroffenen Person im Rahmen der Auskunftserteilung verfügbar zu machen, zu berücksichtigen. Werden die Daten ausschliesslich aufgrund von Aufbewahrungsvorschriften gespeichert, ist die Verarbeitung der Daten einzuschränken (Art. 32 Abs. 3 der Gesetzesvorlage).

Die Dokumentationspflicht und die Begründungspflicht nach Abs. 2 sind Massnahmen zum Schutz der Rechte und Freiheiten der betroffenen Personen im Sinne des Art. 23 Abs. 2 Bst. c, d, g und h DSGVO. Hierdurch wird die betroffene Person in die Lage versetzt, die Ablehnung der Auskunftserteilung nachzuvollziehen und gegebenenfalls durch die Datenschutzstelle prüfen zu lassen. Ergänzend hierzu hat der Verantwortliche nach Art. 12 Abs. 4 DSGVO die betroffene Person auf die Möglichkeit der Beschwerde bei der Datenschutzstelle und des gerichtlichen Rechtsschutzes hinzuweisen. Satz 3 enthält die strenge Zweckbindung der zum Zweck der Auskunftserteilung und zu deren Vorbereitung gespeicherten Daten.

Abs. 3 regelt die Beschränkung zum Schutz der öffentlichen Sicherheit (Art. 23 Abs. 1 Bst. c DSGVO) und der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten (Art. 23 Abs. 1 Bst. d DSGVO).

Abs. 4 regelt die Einschränkung des Auskunftsrechts für personenbezogene Daten, die durch öffentliche Stellen weder automatisiert noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert sind oder werden sollen. Diese

Form der Datenverarbeitung ist zwar nach Art. 2 Abs. 1 DSGVO nicht von dessen sachlichen Anwendungsbereich erfasst, jedoch gilt nach Art. 1 Abs. 5 der Gesetzesvorlage die DSGVO – und mithin auch das Auskunftsrecht nach deren Art. 15 – auch für diese Form der Datenverarbeitung. Unter Abs. 4 fallen insbesondere Akten oder Aktensammlungen sowie ihre Deckblätter, die nicht nach bestimmten Kriterien geordnet sind (vgl. Erwägungsgrund 15 Satz 3 DSGVO). Die Einschränkung liegt daher ausserhalb des Anwendungsbereichs der DSGVO.

Das Auskunftsrecht besteht nur unter der Voraussetzung, dass die betroffene Person Angaben macht, die dem Verantwortlichen das Auffinden der Daten ermöglichen. Ferner darf der für die Erteilung der Auskunft erforderliche Aufwand nicht ausser Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse stehen.

**Zu Art. 32**

Art. 32 schränkt das Recht der betroffenen Person auf Löschung und die damit korrespondierende Pflicht des Verantwortlichen aus Art. 17 Abs. 1 DSGVO ein. Die in Art. 17 Abs. 3 DSGVO genannten Ausnahmen bleiben von der Vorschrift unberührt. Die Regelung gilt sowohl für öffentliche als auch für nicht-öffentliche Stellen. Unter den Voraussetzungen der Abs. 1 bis 3 tritt an die Stelle der Löschung die Einschränkung der Verarbeitung (Art. 18 DSGVO). Hierdurch wird die Beschränkung des Rechts auf bzw. der Pflicht zur Löschung personenbezogener Daten auf das erforderliche Ausmass im Sinne des Art. 23 Abs. 2 Bst. c DSGVO begrenzt. Art 18 Abs. 2 und 3 sowie Art. 19 DSGVO vermitteln effektive Garantien gegen Missbrauch und unrichtige Übermittlung im Sinne des Art. 23 Abs. 2 Bst. d DSGVO.

Der vertretbare Aufwand für den Verantwortlichen bemisst sich nach dem jeweiligen Stand der Technik und erfasst insbesondere nicht oder nur mit unverhältnismässig hohem Aufwand veränderbare oder löschbare Datenspeicher. Ein-

schränkend gilt dies nach Satz 3 nicht für die Fallgruppe der unrechtmässigen Verarbeitung nach Art. 17 Bst. d DSGVO, da der Verantwortliche bei einer unrechtmässigen Datenverarbeitung nicht schutzwürdig ist und sich nicht auf einen unverhältnismässig hohen Aufwand der Löschung wegen der von ihm selbst gewählten Art der Speicherung berufen kann.

Abs. 2 Satz 1 sieht eine Beschränkung zur Wahrung schutzwürdiger Interessen der betroffenen Person vor (Art. 23 Abs. 1 Bst. i DSGVO). Die Ausnahme ergänzt in den Fällen, in denen der Verantwortliche die Daten der betroffenen Person nicht länger benötigt oder unrechtmässig verarbeitet hat (Art. 17 Abs. 1 Bst. a und d DSGVO), die Regelung des Art. 18 Abs. 1 Bst. b und c DSGVO. Nach Art. 18 Abs. 1 Bst. b DSGVO erfolgt die Einschränkung der Verarbeitung unrechtmässig verarbeiteter Daten nur auf entsprechendes Verlangen der betroffenen Person. Art. 18 Abs. 1 Bst. c DSGVO lässt eine Einschränkung der Verarbeitung nicht länger benötigter Daten auf Verlangen der betroffenen Person nur zu, wenn die betroffene Person sie zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen benötigt. Abs. 2 sieht demgegenüber auch ohne entsprechendes Verlangen der betroffenen Person eine generelle Pflicht des Verantwortlichen zur Einschränkung der Verarbeitung vor, wenn er Grund zu der Annahme hat, dass durch die Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Die Regelung ist notwendig, da der Verantwortliche nach Art. 17 DSGVO grundsätzlich verpflichtet ist, nicht mehr erforderliche oder unrechtmässig verarbeitete Daten zu löschen.

Die Einschränkung der Verarbeitung anstelle der Löschung soll die betroffene Person in die Lage versetzen, ihr Verlangen auf Einschränkung der Verarbeitung gegenüber dem Verantwortlichen zu äussern oder sich für eine Löschung der Daten zu entscheiden. Dies wird durch die Unterrichtungspflicht nach Satz 2, welche zugleich eine Massnahme zum Schutz der Rechte und Freiheiten sowie

der berechtigten Interessen der betroffenen Person nach Art. 23 Abs. 2 Bst. h DSGVO darstellt, gewährleistet. In der Regel wird es sich daher nur um eine vorübergehende Beschränkung der Löschungspflicht des Verantwortlichen handeln (Art. 23 Abs. 2 Bst. c DSGVO).

Abs. 3 sieht eine Beschränkung für den Fall vor, dass einer Löschung nicht mehr erforderlicher Daten satzungsmässige oder vertragliche Aufbewahrungsfristen entgegenstehen. Die ergänzende Einschränkung der gesetzlichen Aufbewahrungsfrist ist in Art. 32 der Gesetzesvorlage über die sich unmittelbar aus der DSGVO ergebende Ausnahme des Art. 17 Abs. 3 Bst. b – Erfüllung einer rechtlichen Verpflichtung nach EWR- oder nationalem Recht – erfasst. Die Ausnahme schützt den Verantwortlichen vor einer Pflichtenkollision.

**Zu Art. 33**

Art. 33 schränkt das Recht auf Widerspruch nach Art. 21 Abs. 1 DSGVO gegenüber einer öffentlichen Stelle ein, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift die Verarbeitung vorschreibt. Art. 33 setzt öffentliche Interessen des Verantwortlichen im Sinne des Art. 23 Abs. 1 Bst. e DSGVO voraus, die im konkreten Einzelfall zwingend sein und Vorrang vor den Interessen der betroffenen Person haben müssen.

Art. 25 Abs. 2 und Art. 26 Abs. 4 der Gesetzesvorlage enthalten spezifische Einschränkungen des Widerspruchsrechts für die Datenverarbeitung zu Forschungszwecken, statistischen Zwecken und im öffentlichen Interesse liegenden Archivzwecken.

**Zu Art. 34**

Art. 34 trägt den spezifischen Belangen der Finanz- und Versicherungswirtschaft Rechnung. Die Regelung beruht auf Art. 22 Abs. 2 Bst. b DSGVO, welcher den

Mitgliedstaaten die Möglichkeit einräumt, über Art. 22 Abs. 2 Bst. a und c DSGVO hinausgehende Zulässigkeitstatbestände für automatisierte Entscheidungen im Einzelfall zu schaffen.

Abs. 1 Bst. a regelt die zulässigen Fälle der Versicherungswirtschaft.

Im Gegensatz zu Art. 22 Abs. 2 Bst. a DSGVO ist das Bestehen eines Vertragsverhältnisses zwischen der von der automatisierten Entscheidung betroffenen Person und dem Verantwortlichen keine zwingende Voraussetzung des Abs. 1 Bst. a. Es genügt vielmehr, dass die automatisierte Entscheidung im Rahmen der Leistungserbringung nach einem Versicherungsvertrag ergeht.

Durch Abs. 1 Bst. a Ziff. 2 sind automatisierten Einzelentscheidungen im Rahmen ausservertraglicher Rechtsverhältnisse möglich. Abs. 1 Bst. a Ziff. 2 ermöglicht insbesondere die automatisierte Schadensregulierung. Voraussetzung ist, dass dem Begehren des Antragstellers, der gleichzeitig datenschutzrechtlich die betroffene Person ist, entsprochen wird. In diesen Fällen ist eine Rechtsbeeinträchtigung der betroffenen Person nicht ersichtlich.

Abs. 1 Bst. a Ziff. 3 ermöglicht die automatisierte Entscheidung über Versicherungsleistungen der Krankenversicherung bei der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen. Auch wenn dem Begehren des Antragstellers als von der Entscheidung betroffener Person nicht oder nicht vollständig stattgegeben wird, ist die automatisierte Rechnungsprüfung durch die Krankenversicherung zulässig, wenn der Verantwortliche angemessene Massnahmen zur Wahrung der berechtigten Interessen der betroffenen Person trifft. Diese sind in Abs. 1 letzter Satz geregelt und gelten auch für die anderen zulässigen Ausnahmen. Hierzu zählt zumindest das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunkts und auf Anfechtung der Entscheidung. Über diese Rechte ist die betroffene Person zu

informieren. Die aufgeführten Massnahmen entsprechen den Schutzmechanismen des Art. 22 Abs. 3 DSGVO, so dass zwischen Art. 37 Abs. 1 Bst. a Ziff. 3 der Gesetzesvorlage und den Zulässigkeitstatbeständen des Art. 22 Abs. 2 Bst. a und c DSGVO ein harmonisiertes Konzept der Schutzmechanismen besteht.

Beantragt hingegen ein Versicherungsnehmer mit personenbezogenen Daten eines Dritten, namentlich eines im Rahmen der Krankenversicherung mitversicherten Angehörigen, eine Leistung, liegt keine Entscheidung im Sinne des Art. 22 Abs. 1 DSGVO gegenüber der datenschutzrechtlich betroffenen Person – dem Dritten – vor. Vielmehr entscheidet die Versicherung ausschliesslich automatisiert über Ansprüche aus dem Versicherungsvertrag mit dem Antragsteller als Versicherungsnehmer. Hierbei werden personenbezogene Daten des Dritten automatisiert verarbeitet, wofür es einer Rechtsgrundlage nach Art. 6 Abs. 1 DSGVO, jedoch keiner Ausnahmeregelung vom grundsätzlichen Verbot der automatisierten Entscheidung im Einzelfall bedarf.

Abs. 1 Bst. b regelt die Zulässigkeit automatisierter Entscheidungen für Risikobewertungen nach Art. 9a des Sorgfaltspflichtgesetzes.

Abs. 1 Bst. c sieht die Zulässigkeit automatisierter Entscheidungen für Kreditgeschäfte nach Art. 3 Abs. 3 Bst. b des Bankengesetzes vor. Jene Bestimmung ordnet die Ausleihung von fremden Geldern an einen unbestimmten Kreis von Kreditnehmern dem Geschäftsbereich von Banken zu.

Abs. 1 Bst. d sieht die Zulässigkeit automatisierter Entscheidungen bei Wertpapierdienstleistungen oder Wertpapiernebendienstleistungen nach Art. 3 Abs. 4 des Bankengesetzes bzw. Art. 3 des Vermögensverwaltungsgesetzes vor.

Abs. 2 Satz 1 erlaubt Versicherungsunternehmen im Rahmen automatisierter Entscheidungen nach Abs. 1 Bst. a eine Verarbeitung von Gesundheitsdaten im Sinne des Art. 4 Ziff. 15 DSGVO. Dies ist insbesondere bei der automatisierten

Abrechnung von Leistungsansprüchen durch die private Krankenversicherung notwendig. Abs. 2 beruht auf Art. 22 Abs. 4 i.V.m. mit Art. 9 Abs. 2 Bst. DSGVO. Die Gewährleistung eines bezahlbaren und funktionsfähigen Krankenversicherungsschutzes ist als gewichtiges Interesse des Gemeinwohls anerkannt. Eine wirtschaftliche Leistungsbearbeitung im Massenverfahren setzt den Einsatz von automatisierten Verfahren voraus, insbesondere wenn es um die Anwendung gesetzlicher und somit standardisierter Gebühren oder Tarife geht.

Nach Art. 9 Abs. 2 Bst. g DSGVO muss die nationale Regelung in angemessenem Verhältnis zum verfolgten Ziel stehen, den Wesensgehalt des Rechts auf Datenschutz wahren und angemessene und spezifische Massnahmen zur Wahrung der Grundrechte und Interessen der betroffenen Person vorsehen. Dem trägt der Verweis in Art. 20 Abs. 2 Satz 2 der Gesetzesvorlage Rechnung.

**Zu Art. 35**

Art. 43 Abs. 1 DSGVO verlangt, dass die Zertifizierungsstelle durch die zuständige Aufsichtsbehörde oder die nationale Akkreditierungsstelle oder von beiden akkreditiert wird.

Eine Zertifizierungsstelle ist eine Organisation, welche Zertifizierungen in bestimmten Bereichen (z.B. Industrie-Service, Management-Systeme, Produkt-Zertifizierungen und -prüfungen) durchführt. Bei Bestehen der Prüfung stellt sie ein entsprechendes Zertifikat oder ein anderes Kennzeichen für das Bestehen aus. Als Zertifizierungsstelle kann jede Stelle agieren, welche nach den gesetzlichen Voraussetzungen durch die liechtensteinische Akkreditierungsstelle als Zertifizierungsstelle zugelassen wird.

Eine Akkreditierungsstelle hat zur Aufgabe, in verschiedenen Bereichen den Umstand zu bescheinigen, dass eine Zertifizierungsstelle für das Erfüllen ihrer Aufgaben über die notwendigen Eigenschaften verfügt.

Abs. 1 bestimmt, dass die Befugnis, als Zertifizierungsstelle tätig zu sein, durch die nationale Akkreditierungsstelle erfolgt.

Abs. 2 bestimmt, dass mittels Verordnung die Vorschriften über die Akkreditierung von Zertifizierungsverfahren und die Einführung von Datenschutzsiegeln und -prüfzeichen näher bestimmt werden.

Es ist angedacht, das bisherige System, welches auf der Verordnung vom 10. Dezember 2013 über die Datenschutzzertifizierungen (VDSZ) basiert, weiter anzuwenden.[27]

**Zu Art. 36**

Art. 83 DSGVO sieht für bestimmte Verstösse Geldbussen vor. Die DSGVO regelt aber das anzuwendende Verfahren nicht. Vielmehr fordert Art. 83 Abs. 8 DSGVO ausdrücklich, dass die Mitgliedstaaten für die Anwendung dieser Bestimmung angemessene Verfahrensgarantien vorsehen. Art. 36 der Gesetzesvorlage dient der Umsetzung dieser Forderung. Art. 83 DSGVO sieht in Abs. 9 vor, dass die Verhängung der Bussen auch einem Gericht übertragen werden kann, wovon hier Gebrauch gemacht wird.

Schon im geltenden Datenschutzgesetz obliegt es gemäss Art. 39 bis 41 dem Landgericht, Strafen auszusprechen. Der Datenschutzstelle kam diesbezüglich bisher keine Funktion zu. Dieser Ansatz soll beibehalten werden. Einerseits sieht Art. 83 DSGVO sehr hohe Bussenbeträge vor und ist der Ausspruch von Bussen solcher Höhe durch eine andere Instanz als ein Gericht in Liechtenstein bisher unüblich. Andererseits wird das Bussverfahren durch das Gericht effizienter gehandhabt, als dies bei einer Durchführung durch die Datenschutzstelle der Fall wäre.

---

[27] Vgl. https://www.gesetze.li/konso/2013403000.

In Abs. 1 wird festgelegt, dass das Landgericht die in Art. 83 Abs. 4 bis 6 DSGVO geregelten Bussen ausspricht. Es finden damit die Vorschriften über das Strafverfahren Anwendung.

Für den Fall, dass der Ausspruch von Bussen von der Aufsichtsbehörde an eine andere Instanz verschoben wird, sieht Art. 83 Abs. 9 DSGVO vor, dass es in solchen Fällen die Aufsichtsbehörde dennoch möglich sein muss, das Bussenverfahren anzustossen. Diesbezüglich bedarf es keiner neuen Bestimmung, da § 53 Abs. 1 StPO schon jetzt vorschreibt, dass eine Behörde – und darunter fällt auch die Datenschutzstelle – verpflichtet ist, das Bekanntwerden eines Verdachts einer von Amts wegen zu verfolgenden strafbaren Handlung, die ihren gesetzmässigen Wirkungsbereich betrifft, an die Staatsanwaltschaft oder die Landespolizei zur Anzeige zu bringen.

Abs. 2 nimmt öffentliche Stellen von Bussen aus. Damit wird von der Öffnungsklausel des Art. 83 Abs. 7 DSGVO Gebrauch gemacht, welche nationale Regeln erlaubt, ob und in welchem Umfang gegen Behörden und sonstige öffentliche Stellen Bussen verhängt werden können. Diese Ausnahme rechtfertigt sich dadurch, dass eine dem Staat zufallende Busse vom Staat bezahlt würde. Es fände also lediglich eine interne Umbuchung statt, was nicht sinnvoll ist. Trotzdem entsteht dadurch hier kein sanktionsfreier Raum. Es ist auf das gut ausgebaute Disziplinarrecht, das bestehende Strafrecht des 22. Abschnitts des Strafgesetzbuches über strafbare Verletzungen der Amtspflicht, Korruption und verwandte strafbare Handlungen zu verweisen. Die Ausnahme findet ihre Grenze, wenn öffentliche Stellen im Rahmen ihrer Tätigkeit im Wettbewerb mit anderen Verarbeitern stehen. In solchen Fällen sollen sie bei der Verhängung von Bussen gegenüber ihren Wettbewerbern nicht bessergestellt werden.

Abs. 3 bestimmt, dass die Staatsanwaltschaft nur mit Zustimmung der Datenschutzstelle von der Strafverfolgung zurücktreten kann. Damit wird der Daten-

schutzstelle ein gewisser Einfluss auf das Strafverfahren gegeben. Dies erscheint gerechtfertigt, als die Datenschutzstelle als Aufsichtsbehörde ein gesteigertes Interesse am Ausgang des Verfahrens hat.

**Zu Art. 37**

Art. 84 Abs. 1 DSGVO berechtigt und verpflichtet die EWR-Staaten, „andere Sanktionen“ für Verstösse gegen die Verordnung festzulegen. Art. 84 DSGVO ist damit eine Öffnungsklausel, um neben Geldbussen im Sinne des Art. 83 DSGVO strafrechtliche Sanktionen vorzusehen. Hiervon macht Art. 37 der Gesetzesvorlage Gebrauch.

In Abs. 1 wird die unberechtigte Übermittlung oder Zugänglichmachung von Daten mit Strafe bewehrt.

In Abs. 2 wird die unberechtigte Verarbeitung oder das Erschleichen von personenbezogenen Daten mit Strafe bewehrt.

Abs. 3 bestimmt, dass die Verfolgung nur auf Antrag geschieht. Auch der Datenschutzstelle kommt das Antragsrecht zu.

Abs. 4 dient dem Verbot einer Selbstbezichtigung.

**Zu Art. 38**

In dieser Bestimmung wird die Installation einer Videoüberwachung vor deren Bewilligung mit Busse bewehrt.

Abs. 2 nimmt öffentliche Stellen analog zu Art. 36 Abs. 2 der Gesetzesvorlage von Bussen aus (siehe hierzu die entsprechenden Erläuterungen).

Abs. 3 dient analog zu Art. 37 Abs. 4 der Gesetzesvorlage dem Verbot einer Selbstbezichtigung (siehe hierzu die entsprechenden Erläuterungen).

**Zu Art. 39**

Abs. 1 trifft die näheren Bestimmungen über den Schadenersatz. Es wird im Wesentlichen auf die allgemeinen Schadenersatzbestimmungen gemäss Allgemeinem Bürgerlichem Gesetzbuch (ABGB) verwiesen.

Gemäss Abs. 2 ist ein Verantwortlicher oder Auftragsverarbeiter, der keine Niederlassung im EWR hat, verpflichtet, einen Vertreter im EWR zu benennen. Dieser dient gemäss Art. 27 Abs. 4 DSGVO den betroffenen Personen sowie den Aufsichtsbehörden als Anlaufstelle. Es ist daher sachgerecht, ihn auch als bevollmächtigt anzusehen, Zustellungen in Zivilgerichtsverfahren vor den nationalen Gerichten für den Verantwortlichen oder Auftragsverarbeiter entgegenzunehmen. Hierdurch werden insbesondere die praktischen Schwierigkeiten bei der grenzüberschreitenden Zustellung einer Klage vermieden. Es bleibt dem zuständigen Gericht allerdings unbenommen, einen in einem Drittstaat ansässigen Verantwortlichen oder Auftragsverarbeiter – insbesondere bei unklarer Sach- und Rechtslage – ausdrücklich aufzufordern, einen Zustellungsbevollmächtigten im Inland zu benennen.

**Zu Art. 40**

Der Dritte Teil dient im Wesentlichen der Umsetzung der DSRL-PJ.

Art. 40 regelt den Anwendungsbereich dieses Dritten Teils. Er gilt nur für Verarbeitungen personenbezogener Daten durch öffentliche Stellen und als öffentliche Stellen geltende öffentliche Unternehmen, die für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, zuständig sind und nur soweit sie zu diesen Zwecken Daten verarbeiten. Dies sind beispielsweise die Landespolizei oder die Staatsanwaltschaft, soweit sie die Daten zu den genannten Zwecken verarbeiten.

Für die Anwendung des Dritten Teils und damit auch der DSRL-PJ genügt demnach eine Verarbeitung personenbezogener Daten zu den oben genannten Zwecken allein nicht; daneben muss auch eine grundsätzliche Befugnis- und Aufgabenzuweisung (Zuständigkeit) für die Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder die Strafvollstreckung, einschliesslich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit, vorliegen.

Ebenso sind Verwaltungsstraftaten vom Anwendungsbereich umfasst. Hierdurch wird insbesondere erreicht, dass die polizeiliche Datenverarbeitung einheitlichen Regeln folgt, unabhängig davon, ob eine Straftat oder eine Verwaltungsstraftat in Rede steht. Aus dem Ziel, dem Verwaltungsstrafverfahren einheitliche datenschutzrechtliche Regeln gegenüberzustellen, folgt, dass somit auch in Bezug auf die Datenverarbeitung durch Behörden, die nicht Polizeibehörden sind, aber Verwaltungsstraftaten verfolgen, ahnden und vollstrecken, der Dritte Teil des vorliegenden Gesetzes gilt und die Datenverarbeitung den Regelungen gemäss DSRL-PJ untersteht. Daraus folgt demnach auch, dass die Datenverarbeitung bei Verwaltungsbehörden, deren Aufgabenzuweisung nicht mit den in Art. 40 genannten Zwecken übereinstimmt, grundsätzlich solange und insoweit nicht in den Anwendungsbereich der Richtlinie und damit des Dritten Teils dieser Gesetzesvorlage fällt, wie die von ihnen geführten Verfahren nicht in ein konkretes Verwaltungsstrafverfahren übergehen.

Auftragsverarbeiter – ob öffentliche oder nicht-öffentliche Stellen –, deren Tätigkeit sich grundsätzlich dadurch auszeichnet, dass sie Daten zur Erfüllung einer Auftragsverarbeitungsvereinbarung und nicht aufgrund eigener Aufgabenzuschreibung verarbeiten, sind durch die Regelungen des Dritten Teils nur adressiert, sofern konkret auf sie verwiesen wird. Die von ihnen durchgeführten Verarbeitungen richten sich im Übrigen nach den Regelungen der DSGVO bzw. dem Ersten und Zweiten Teil dieser Vorlage. Das schliesst nicht aus, dass durch den

dritten Teil angesprochene Verantwortliche auch als Auftragsverarbeiter tätig sein können.

Art. 40 entspricht dem § 45 der Rezeptionsvorlage.

**Zu Art. 41**

Die Begriffsbestimmungen in den Ziff. 1 bis 15 werden zum Zweck der Umsetzung der DSRL-PJ aufgenommen. Sie schliessen an die Begriffsbestimmungen in Art. 3 DSRL-PJ an. Zudem wird die Einwilligung unter Übernahme der Definition aus der DSGVO in Ziff. 17 aufgenommen.

Art. 41 entspricht § 46 der Rezeptionsvorlage.

**Zu Art. 42**

Art. 42 dient der Umsetzung von Art. 4 Abs. 1 DSRL-PJ und führt einige allgemeine Verarbeitungsgrundsätze, die in Teilen an späterer Stelle noch einmal aufgenommen werden, an zentraler Stelle zusammen.

Art. 42 entspricht § 47 der Rezeptionsvorlage.

**Zu Art. 43**

Art. 43 dient der Umsetzung von Art. 10 DSRL-PJ.

Abs. 1 legt den Grundsatz fest, dass die Verarbeitung besonderer Kategorien personenbezogener Daten zulässig ist, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist. Abs. 1 schafft damit eine Rechtsgrundlage für diese Verarbeitungen. Dies kann auch die Verarbeitung in den in Art. 10 Bst. b und c DSRL-PJ genannten Zusammenhängen umfassen, d. h. zur Wahrung lebenswichtiger Interessen der Betroffenen oder eines Dritten oder wenn Daten verarbeitet werden sollen, welche die betroffene Person offensichtlich öffentlich gemacht hat.

In Abs. 2 wird in Satz 1 klargestellt, dass bei der Verarbeitung geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen werden müssen. In Satz 2 werden Aussagen zu möglichen Massnahmen zur Umsetzung dieser Vorgabe getroffen. Die Aufzählung gibt unverbindliche Beispiele wieder, wie geeignete Garantien aussehen können. Die konkrete Ausgestaltung der Massnahmen kann also von Einzelfall zu Einzelfall variieren.

Art. 43 entspricht § 48 der Rezeptionsvorlage.

**Zu Art. 44**

Satz 1 setzt Art. 4 Abs. 2 DSRL-PJ um. Es wird klargestellt, dass Verantwortliche Daten so lange und so weit zu anderen Zwecken, als zu denen sie ursprünglich erhoben wurden, verarbeiten dürfen, als es sich bei diesen anderen Zwecken um einen der in Art. 40 der Gesetzesvorlage genannten handelt und diese Verarbeitung erforderlich und verhältnismässig ist. Grundsätzlich eröffnet Art. 4 Abs. 2 DSRL-PJ stets die Möglichkeit, die Daten für einen der in Art. 40 der Gesetzesvorlage genannten Zwecke zu verarbeiten und innerhalb der Palette der genannten Zwecke auch Zweckänderungen vorzunehmen.

Eine Verarbeitung zu anderen als in Art.40 der Gesetzesvorlage genannten Zwecken ist zulässig, sofern es dafür eine Rechtsgrundlage gibt vorgesehen ist. (vgl. dazu beispielsweise Art. 23 der Gesetzesvorlage).

Art. 44 entspricht § 49 der Rezeptionsvorlage.

**Zu Art. 45**

Art. 45 greift Art. 4 Abs. 3 DSRL-PJ auf, wonach Verantwortliche Daten auch zu wissenschaftlichen, statistischen und historischen Zwecken verarbeiten dürfen, solange diese Verarbeitung unter die in Art. 40 der Gesetzesvorlage genannten Zwecke subsumiert werden kann. Als Beispiel kann hier kriminologische oder kriminaltechnische Forschung angeführt werden. Voraussetzung hierfür ist das

Vorliegen geeigneter Vorkehrungen zum Schutz der Rechtsgüter der betroffenen Personen. Es hat eine Interessenabwägung zwischen der beabsichtigten Verarbeitung und dem Schutzinteresse der Betroffenen stattzufinden.

Art. 45 entspricht § 50 der Rezeptionsvorlage.

**Zu Art. 46**

In Art. 46 finden sich die Voraussetzungen für eine wirksame Einwilligung zur Verarbeitung personenbezogener Daten. Abs. 1 bis 3 entsprechen Art. 7 Abs. 1 bis 3 DSGVO. Für die Beurteilung der Frage, ob die Freiwilligkeit der Einwilligung vorliegt, ist wesentlich auf die Umstände der Erteilung abzustellen. Dabei ist insbesondere von Bedeutung, dass die Einwilligung auf der freien Entscheidung der betroffenen Person beruht. Die schriftliche Einwilligung muss von anderen, allenfalls schriftlich geregelten Sachverhalten klar zu unterscheiden sein. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen.

Art. 46 entspricht § 51 der Rezeptionsvorlage, welche sich auch an § 4a Abs. 1 geltendes BDSG orientiert.

**Zu Art. 47**

Art. 47 setzt Art. 23 DSRL-PJ um und regelt, dass jede einem Verantwortlichen oder einem Auftragsverarbeiter unterstellte Person Daten ausschliesslich auf Weisung des Verantwortlichen verarbeiten darf, ausser es gibt eine gesetzliche Verpflichtung zur Verarbeitung.

Art. 47 entspricht § 52 der Rezeptionsvorlage.

**Zu Art. 48**

Gemäss Art. 48 dürfen mit Datenverarbeitung befasste Personen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis).

Art. 48 entspricht § 53 der Rezeptionsvorlage.

**Zu Art. 49**

Art. 49 setzt Art. 11 DSRL-PJ um und regelt das Verbot automatisierter, insbesondere auf Profiling basierender, Einzelentscheidungen. Um eine in Abs. 1 genannte – nur unter bestimmten Umständen zulässige – „Entscheidung, die eine nachteilige Rechtsfolge für die betroffene Person“ hat, zu sein, muss es sich bei einer solchen Entscheidung um einen Rechtsakt mit Aussenwirkung gegenüber der betroffenen Person – regelmässig einen Verwaltungsakt – handeln. Interne Zwischenschritte, die Ausfluss automatisierter Prozesse sind, fallen nicht hierunter.

Art. 49 entspricht § 54 der Rezeptionsvorlage.

**Zu Art. 50**

Art. 50 dient der Umsetzung von Art. 13 Abs. 1 DSRL-PJ. Diese Bestimmung legt aktive Informationspflichten des Verantwortlichen gegenüber betroffenen Personen fest, unabhängig von der Geltendmachung von Betroffenenrechten. Dieser Informationspflicht sollen Verantwortliche in allgemeiner Form nachkommen können. Durch die explizit in Erwägungsgrund 42 DSRL-PJ aufgenommene Möglichkeit der Information über die Internetseite des Verantwortlichen wird der Sinn und Zweck der Regelung klargestellt: Betroffene Personen sollen sich unabhängig von der Datenverarbeitung im konkreten Fall in leicht zugänglicher Form einen Überblick über die Zwecke der beim Verantwortlichen durchgeführten Verarbeitungen verschaffen können und eine Übersicht über die ihnen zustehenden Betroffenenrechte bekommen.

Art. 50 entspricht § 55 der Rezeptionsvorlage.

**Zu Art. 51**

Art. 56 betrifft Fälle, in denen in spezialgesetzlichen Regelungen eine aktive Benachrichtigung betroffener Personen vorgesehen ist. Eine Festlegung dieser in

Art. 13 Abs. 2 DSRL-PJ genannten „besonderen Fälle“ ist nicht verallgemeinernd auf Ebene des Datenschutzgesetzes möglich und muss somit im jeweiligen Spezialgesetz beachtet werden. Leitend für die Entscheidung, ob eine Benachrichtigung unabhängig von der Geltendmachung eines Betroffenenrechts angezeigt ist, wäre beispielsweise, ob die Verarbeitung mit oder ohne Wissen der betroffenen Person, unter Umständen in Verbindung mit einer erhöhten Eingriffstiefe, erfolgt. In letztgenannten Fällen ist eine aktive, gegebenenfalls nachträgliche, Benachrichtigung die einzige Möglichkeit für die betroffene Person, von der Verarbeitung Kenntnis zu erlangen und allenfalls deren Rechtmässigkeit mithilfe der Geltendmachung von Betroffenenrechten zu prüfen.

Abs. 1 stellt klar, welche Informationen betroffenen Personen von dem Verantwortlichen in diesen Fällen aktiv übermittelt werden müssen, und dient dabei der Umsetzung von Art. 13 Abs. 2 DSRL-PJ.

Abs. 2 ermöglicht es in Umsetzung von Art. 13 Abs. 3 DSRL-PJ, zu den in Abs. 2 genannten Zwecken von der Bereitstellung der in Abs. 1 genannten Informationen abzusehen, sie einzuschränken oder sie aufzuschieben. Die Vorschrift geht zum Schutz der betroffenen Person über das durch die DSRL-PJ Gebotene hinaus, indem jeweils eine Gefährdung – gegenüber einer in der DSRL-PJ angesprochenen Beeinträchtigung – der in den Ziff. 1 bis 3 genannten Rechtsgüter oder Zwecke vorausgesetzt wird. Den Ausnahmen ist der Gedanke gemein, dass die Auskunftserteilung nicht zur Gefährdung der ordnungsgemässen Erfüllung der Aufgaben des Verantwortlichen führen soll. Die Nutzung der Möglichkeit, von der Bereitstellung der in Abs. 1 genannten Informationen abzusehen, sie einzuschränken oder aufzuschieben, muss Verhältnismässigkeitsgrundsätzen genügen, mithin in ein angemessenes Verhältnis zur Bedeutung der Betroffeneninformation für die spätere Geltendmachung von Betroffenenrechten gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen, ob die Bereitstellung etwa nur

teil- oder zeitweise eingeschränkt werden kann („soweit und so lange“; Art. 13 Abs. 3 DSRL-PJ).

Abs. 3 statuiert ein Zustimmungserfordernis der Landespolizei. Dieses rechtfertigt sich, da ein der Situation der aktiven Geltendmachung von Betroffenenrechten vergleichbarer Sachverhalt vorliegt.

Art. 51 entspricht § 56 der Rezeptionsvorlage. § 56 Abs. 3 der Rezeptionsvorlage orientiert sich an § 19 Abs. 3 geltendes BDSG.

**Zu Art. 52**

Art. 52 thematisiert das Auskunftsrecht als zentrales Betroffenenrecht und normiert gleichzeitig dessen Einschränkungen. Die Vorschrift dient mithin der Umsetzung der Art. 14 (Bestehen des Auskunftsrechts) und 15 (Ausnahmen) DSRL-PJ. Das Auskunftsrecht setzt – im Gegensatz zu in Art. 51 der Gesetzesvorlage angesprochenen aktiven Benachrichtigungspflichten – einen entsprechenden Antrag der betroffenen Person voraus.

Abs. 1 legt den Umfang des der betroffenen Person zustehenden Auskunftsrechts fest. Der in den Ziff. 1 und 4 genannte Begriff „Kategorie“ ermöglicht dem Verantwortlichen eine angemessene Generalisierung der Angaben zu den verarbeiteten personenbezogenen Daten sowie zu den Übermittlungsempfängern. Die Angaben nach Ziff. 1 zu den verarbeiteten personenbezogenen Daten können in verständlicher Form im Sinne einer zusammenfassenden Übersicht gemacht werden. Die Angaben müssen also nicht in einer Form gemacht werden, welche Aufschluss über die Art und Weise der Speicherung oder Sichtbarkeit der Daten beim Verantwortlichen (im Sinne einer Kopie) zulässt. Ebenso bedeutet die Pflicht zur Angabe der verfügbaren Informationen zur Datenquelle gemäss Ziff. 2 nicht, dass die Identität natürlicher Personen oder gar vertrauliche Informationen preisgegeben werden müssen. Der Verantwortliche muss sich bei der Anga-

be zu den personenbezogenen Daten, die Gegenstand der Verarbeitung sind, letztlich von dem gesetzgeberischen Ziel leiten lassen, bei der betroffenen Person ein Bewusstsein über Umfang und Art der verarbeiteten Daten zu erzeugen und es ihr zu ermöglichen, aufgrund dieser Informationen zu ermessen, ob die Verarbeitung rechtmässig ist und – wenn Zweifel hieran bestehen – gegebenenfalls die Geltendmachung weiterer Betroffenenrechte auf diese Informationen stützen zu können.

Abs. 2 sorgt für einen Gleichlauf mit Art. 31 Abs. 1 Ziff. 2 der Gesetzesvorlage. Demnach besteht kein Recht auf Auskunft durch die betroffene Person, wenn die Daten nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder sonstiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder ausschliesslich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen und die Auskunftserteilung einen unverhältnismässigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Massnahmen ausgeschlossen ist.

Abs. 3 begrenzt die Auskunft im Fall einer Unverhältnismässigkeit.

Abs. 4 normiert, unter welchen Voraussetzungen das Auskunftsrecht durch den Verantwortlichen vollständig oder teilweise eingeschränkt werden darf. D.h., es ist jeweils eine Gefährdung der in Art. 51 Abs. 2 der Gesetzesvorlage genannten Rechtsgüter oder Zwecke vorausgesetzt (vgl. Ausführungen zu Art. 51 Abs. 2 der Gesetzesvorlage). Die Nutzung der Möglichkeit, von der Auskunftserteilung vollständig oder teilweise abzusehen, muss Verhältnismässigkeitsgrundsätzen genügen und ihr muss eine nachvollziehbare Interessenabwägung vorausgehen. Die durch das teilweise oder vollständige Absehen von der Auskunftserteilung geschützten Rechtsgüter müssen mithin in ein angemessenes Verhältnis zur Bedeutung der Auskunftserteilung für die spätere Geltendmachung weiterer Betroffenenrechte gebracht werden. So hat der Verantwortliche im Einzelfall zu prüfen,

ob die Auskunft etwa nur teilweise eingeschränkt oder zu einem späteren Zeitpunkt erteilt werden kann.

Abs. 5 übernimmt für diese Bestimmung das gleiche Zustimmungsprinzip, wie es in Art. 51 Abs. 3 der Gesetzesvorlage vorgesehen ist. Es wird auf die dortigen Erläuterungen verwiesen.

Die Sätze 1 und 2 von Abs. 6 dienen der Umsetzung von Art. 15 Abs. 3 Sätze 1 und 2 DSRL-PJ. Hierdurch wird dem Verantwortlichen die Möglichkeit gegeben, das Auskunftsverlangen unbeantwortet zu lassen („*neither confirm nor deny*“). Die betroffene Person ist in einem solchen Fall grundsätzlich schriftlich zu informieren und die Ablehnung ist zu begründen, ausser diese Schritte würden bereits dazu führen, dass der mit der Ablehnung oder Einschränkung der Information verfolgte Zweck damit gefährdet würde. Die Rezeptionsvorlage orientiert sich bezüglich des Absehens von einer Begründung in Satz 3 an § 19 Abs. 5 Satz 1 geltendes BDSG.

Abs. 7 thematisiert die Möglichkeiten, die der betroffenen Person im Fall des Absehens von einer Begründung für die vollständige oder teilweise Einschränkung des Auskunftsrechts oder im Fall der überhaupt ausbleibenden Beantwortung des Auskunftsverlangens bleiben. Nach Satz 1 kann die betroffene Person ihr Auskunftsrecht nach Auskunftsverweigerung durch den Verantwortlichen über die Datenschutzstelle ausüben. Dies dient der Umsetzung von Art. 17 Abs. 1 DSRL-PJ und kommt einer deklaratorischen Wiederholung des in Art. 55 der Gesetzesvorlage enthaltenen Grundsatzes gleich, wonach betroffene Personen jederzeit die Datenschutzstelle anrufen können. Satz 2 sieht in Umsetzung von Art. 17 Abs. 2 DSRL-PJ eine entsprechende Unterrichtung durch den Verantwortlichen vor, die allerdings nicht auf Fälle Anwendung findet, in denen der Verantwortliche nach Abs. 6 berechtigt ist, von einer Information des Antragstellers ganz abzusehen.

Macht die betroffene Person gemäss Satz 1 von ihrem Auskunftsrecht nach einer Ablehnung oder Einschränkung einer Auskunft Gebrauch, so hat die Datenschutzstelle zunächst abzuklären, ob ihrer Tätigkeit im Sinne des Satz 3 eine Gefährdung der Sicherheit des Landes entgegensteht. Sätze 4 und 5 betreffen den Inhalt der der betroffenen Person seitens der Datenschutzstelle zur Verfügung gestellten Informationen im Ergebnis der dort durchgeführten Prüfung. Damit wird Art. 17 Abs. 3 Satz 1 DSRL-PJ umgesetzt und zur Stärkung der Betroffenenrechte in Satz 5 über das von der DSRL-PJ Geforderte hinausgegangen, indem die Mitteilung die Information enthalten darf, ob datenschutzrechtliche Verstösse festgestellt wurden, mithin die Auskunftsverweigerung oder teilweise Einschränkung der Auskunft rechtmässig war. Satz 8 setzt Art. 17 Abs. 3 Satz 2 DSRL-PJ um. Abs. 8 setzt Art. 15 Abs. 4 DSRL-PJ um.

Art. 52 entspricht § 57 der Rezeptionsvorlage. Abs. 7 Satz 3 der Rezeptionsvorlage orientiert sich an § 19 Abs. 6 Satz 1 geltendes BDSG. Abs. 7 Satz 6 und 7 der Rezeptionsvorlage orientieren sich an § 19 Abs. 6 Satz 2 geltendes BDSG.

**Zu Art. 53**

In Art. 53 werden die Betroffenenrechte auf Berichtigung, Löschung und Einschränkung der Verarbeitung und deren Ausnahmen zusammengeführt. Art. 53 dient der Umsetzung von Art. 16 DSRL-PJ in seiner Ausformung als Betroffenenrecht.

Abs. 1 betrifft das Recht auf Berichtigung unrichtiger bzw. auf Vervollständigung unvollständiger Daten. Hier wird Art. 16 Abs. 1 DSRL-PJ umgesetzt. In Satz 2 wird ein in Erwägungsgrund 47 DSRL-PJ enthaltener Gedanke aufgenommen, wonach zur Vorbeugung massenhafter und nicht erfolgversprechender Anträge klargestellt wird, dass sich die Berichtigung auf die betroffene Person betreffende Tatsachen bezieht und nicht etwa auf den Inhalt von Zeugenaussagen. Gleiches gilt etwa für polizeifachliche Bewertungen. In Satz 3 wird Art. 16 Abs. 3 Satz 1 Bst. a

DSRL-PJ umgesetzt. Zwar sieht der Richtlinientext im beschriebenen Fall die Verarbeitungseinschränkung als Alternative zur Löschung vor. Da die Richtlinie allerdings im Fall der Verarbeitung unrichtiger Daten deren Berichtigung, aber nicht deren Löschung vorsieht, wird in Abs. 1 für Fälle, in denen nach Bestreiten der Richtigkeit der Daten deren Richtigkeit oder Unrichtigkeit nicht festgestellt werden kann, an die Stelle der Berichtigung eine Verarbeitungseinschränkung vorgesehen. Für das Bestreiten der Richtigkeit der beim Verantwortlichen verarbeiteten Daten durch die betroffene Person reicht die reine Behauptung der Unrichtigkeit nicht aus; vielmehr müssen die Zweifel an der Unrichtigkeit durch Beibringung geeigneter Tatsachen substantiiert werden. Dies dient dem Schutz der polizeilichen Arbeit und der Vermeidung unverhältnismässigen Prüfaufwands.

Abs. 2 statuiert das Betroffenenrecht auf Löschung und dient der Umsetzung von Art. 16 Abs. 2 DSRL-PJ. Das Recht auf Löschung des Betroffenen bzw. die Pflicht zur Löschung durch den Verantwortlichen, wenn die Verarbeitung der Daten unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen, besteht unabhängig von einer Geltendmachung durch den Betroffenen.

Abs. 3 betrifft die Voraussetzungen, unter denen an die Stelle einer Löschung nach Abs. 2 eine Verarbeitungseinschränkung treten kann. Die Rezeptionsvorlage orientiert sich bezüglich Abs. 3 Satz 1 Ziff. 1 und 3 an § 20 Abs. 3 geltendes BDSG, welcher um Art. 16 Abs. 3 Satz 1 Bst. b DSRL-PJ ergänzt wird (Abs. 3 Satz 1 Ziff. 2). Abs. 3 Satz 1 Ziff. 1 übernimmt zudem einen in Erwägungsgrund 47 Satz 4 DSRL-PJ enthaltenen Gedanken: Die Möglichkeit, von der Löschung wegen unverhältnismässigen Aufwands abzusehen, ist als restriktiv auszulegende Ausnahmeregelung anzusehen. Im Grundsatz sollte die bei Verantwortlichen zum Einsatz kommende IT-Infrastruktur darauf ausgelegt sein, eine Löschungsverpflichtung auch technisch nachvollziehen zu können.

Abs. 4 fordert, dass die Verarbeitungseinschränkung im Kontext automatisierter Verarbeitung erkennbar sein muss.

Die in Abs. 5 enthaltene Verpflichtung zur Meldung der Berichtigung an Stellen, von denen die unrichtigen Daten stammen, setzt Art. 16 Abs. 5 DSRL-PJ um.

Abs. 6 dient der Umsetzung von Art. 16 Abs. 4 DSRL-PJ und betrifft das zur Anwendung gelangende Verfahren, wenn der Verantwortliche einem Antrag auf Berichtigung oder Löschung nicht oder nur eingeschränkt nachkommt. Die Vorschrift ist Art. 52 Abs. 6 der Gesetzesvorlage nachgebildet. Deshalb wird – so auch in Abs. 7 – weitgehend auf die entsprechenden Vorschriften in Art. 52 der Gesetzesvorlage zur vollständigen oder teilweisen Einschränkung des Auskunftsrechts verwiesen.

Art. 53 entspricht dem § 58 der Rezeptionsvorlage.

**Zu Art. 54**

In Art. 54 werden Elemente des Art. 12 DSRL-PJ umgesetzt[28].

Informationen und Mitteilungen sollen in einer präzisen, verständlichen und leicht zugänglichen Form und in einer klaren und einfachen Sprache erfolgen. Der Verantwortliche hat die Ausübung der zustehenden Rechte zu erleichtern und sich im Zweifelsfall der Identität der betroffenen Person zu versichern. Wenngleich es Abs. 4 dem Verantwortlichen in begründeten Zweifelsfällen ermöglicht, zusätzliche Informationen zur Identitätsklärung anzufordern, ist hierdurch keine Änderung der bisherigen verbreiteten Praxis angezeigt, den Nachweis der Identität auch weiterhin als Grundvoraussetzung für die Antragsstellung anzusehen.

---

[28] Abs. 1 setzt Art. 12 Abs. 1, Abs. 2 setzt Art. 12 Abs. 3, Abs. 3 setzt Art. 12 Abs. 4 und Abs. 4 setzt Art. 12 Abs. 5 DSRL-PJ um.

Art. 54 entspricht § 59 der Rezeptionsvorlage.

**Zu Art. 55**

Art. 55 stellt auch für den Bereich der Verarbeitung durch Verantwortliche zu den in Art. 40 der Gesetzesvorlage genannten Zwecken klar, dass sich Betroffene mit Beschwerden über die bei Verantwortlichen durchgeführte Verarbeitung an die Datenschutzstelle wenden können. Insbesondere mit Abs. 1 dieser Vorschrift wird Art. 52 DSRL-PJ umgesetzt. Abs. 2 setzt Art. 52 Abs. 2 DSRL-PJ um.

Art. 55 entspricht § 60 der Rezeptionsvorlage. Die Rezeptionsvorlage orientiert sich ihrerseits an § 21 geltendes BDSG.

**Zu Art. 56**

Art. 56 setzt Art. 53 Abs. 1 DSRL-PJ um und bestimmt, dass Adressaten von verbindlichen Entscheidungen der Datenschutzstelle Rechtsschutz gegen diese suchen können. In Erwägungsgrund 86 DSRL-PJ wird betont, dass sich der Rechtsschutz insbesondere auf die Ausübung von Untersuchungs-, Abhilfe- und Genehmigungsbefugnissen oder die Ablehnung oder Abweisung von Beschwerden durch die Datenschutzstelle bezieht; für reine Stellungnahmen oder Empfehlungen hingegen soll der Rechtsweg nicht offen stehen. In diesem Zusammenhang wird auf die sich aus seiner systematischen Stellung ergebende Anwendbarkeit von Art. 19 der Gesetzesvorlage in Bezug auf das Rechtsschutzverfahren hingewiesen.

In Abs. 2 wird – in Umsetzung von Art. 53 Abs. 2 DSRL-PJ – der Rechtsschutz auf Fälle der Untätigkeit der Datenschutzstelle ausgedehnt.

Art. 56 entspricht § 61 der Rezeptionsvorlage.

**Zu Art. 57**

Art. 57 dient der Umsetzung von Art. 22 DSRL-PJ und stellt Anforderungen auf, wenn der Verantwortliche Auftragsverarbeitungsverhältnisse eingehen will.

Abs. 1 regelt die grundsätzliche Zuständigkeit des Verantwortlichen.

Abs. 2 setzt Art. 22 Abs. 1 DSRL-PJ um und beschreibt an den Auftragsverarbeiter zu stellende Anforderungen.

In Abs. 3 werden Voraussetzungen für die Eingehung von Unterauftragsverarbeitungsverhältnissen normiert. Damit wird Art. 22 Abs. 2 DSRL-PJ umgesetzt.

In Abs. 4 wird in Übernahme von Elementen aus Art. 28 Abs. 4 DSGVO die Überführung von den Auftragsverarbeiter treffenden Pflichten auf einen Unterauftragnehmer thematisiert.

In Abs. 5 werden die erforderlichen Inhalte einer der Auftragsverarbeitung zugrundeliegenden Vereinbarung festgelegt. Es sind dies insbesondere das Erfordernis einer dokumentierten Weisung, die Verpflichtung zur Vertraulichkeit, die Unterstützung des Verantwortlichen, die Löschung oder Rückgabe der Daten, die Zurverfügungstellung von Informationen und die erforderlichen Überprüfungen. Diese Inhalte sind sowohl Art. 22 Abs. 3 DSRL-PJ als auch Art. 28 Abs. 3 DSGVO entnommen. In Satz 2 Ziff. 1 werden Elemente aus Art. 28 Abs. 3 Bst. a DSGVO und § 11 Abs. 3 Satz 2 geltendes BDSG, in Ziff. 5 Elemente aus Art. 28 Abs. 3 Bst. h, in Ziff. 7 Elemente aus Art. 28 Abs. 3 Bst. c und in Ziff. 8 Elemente aus Art. 28 Abs. 3 Bst. f DSGVO aufgenommen.

Abs. 6 trifft in Umsetzung von Art. 22 Abs. 4 DSRL-PJ Aussagen zur Form der Vereinbarung. Diese muss handschriftlich oder elektronisch abgefasst sein.

Abs. 7 dient der Umsetzung von Art. 22 Abs. 5 DSRL-PJ und bestimmt, dass ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoss gegen diese Vorschrift bestimmt, als Verantwortlicher gilt.

Art. 57 entspricht § 62 der Rezeptionsvorlage. Die Rezeptionsvorlage orientiert sich an § 11 geltendes BDSG. Bezüglich Abs. 1 orientiert sich die Rezeptionsvorlage an § 11 Abs. 1 geltendes BDSG. Bezüglich Abs. 5 orientiert sich die Rezeptionsvorlage an § 11 Abs. 2 und 3 geltendes BDSG.

**Zu Art. 58**

Art. 58 dient der Umsetzung von Art. 21 DSRL-PJ hinsichtlich der gemeinsam Verantwortlichen, wenn zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung festlegen.

Art. 58 entspricht § 63 der deutschen Rezeptionsvorlage. Zur beispielhaften Konkretisierung der infrage kommenden Fälle orientiert sich die Rezeptionsvorlage an einer Formulierung aus § 6 Abs. 2 geltendes BDSG, welche übernommen wird.

**Zu Art. 59**

Art. 59 dient der Umsetzung von Art. 29 DSRL-PJ. Er verpflichtet den Verantwortlichen, erforderliche technisch-organisatorische Massnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten. Gleichzeitig wird klargestellt, dass die Ausgestaltung der Massnahmen Ergebnis eines Abwägungsprozesses sein soll, in den insbesondere der Stand der verfügbaren Technik, die entstehenden Kosten, die näheren Umstände der Verarbeitung und die in Aussicht zu nehmende Gefährdung für die Rechtsgüter der betroffenen Person einzubeziehen sind. Die Erforderlichkeit der Massnahmen ist daran zu bemessen, ob ihr Aufwand in einem angemessenen Verhältnis zum angestrebten Schutzzweck steht. Zudem wird klarstellend geregelt, dass bei der Festlegung der technisch-organisatorischen Massnahmen

die einschlägigen Standards und Empfehlungen, insbesondere allgemein anerkannte technische Richtlinien (z.B. von spezialisierten Instituten, Ämtern, Think Tanks), zu berücksichtigen sind.

In Abs. 2 werden Inhalte aus Art. 32 Abs. 1 Bst. a bis c DSGVO übernommen. Anstatt der in Abs. 1 genannten Massnahmen kann daher auch die Pseudonymisierung und Verschlüsselung personenbezogener Daten erfolgen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Dabei muss die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme sowie die Verfügbarkeit der personenbezogenen Daten sichergestellt bleiben.

Abs. 3 benennt die Ziele, die im Hinblick auf automatisierte Verarbeitungen durch die Etablierung geeigneter technisch-organisatorischer Massnahmen verfolgt und erreicht werden sollen. Der Verantwortliche oder Auftragsverarbeiter hat diesen Katalog den von ihm zu ergreifenden Massnahmen zu Grunde zu legen.

Art. 59 entspricht § 64 der Rezeptionsvorlage. Bezüglich Abs. 1 orientiert sich die Rezeptionsvorlage an § 9 Satz 2 geltendes BDSG. Bezüglich Abs. 3 orientiert sich die Rezeptionsvorlage an § 9 geltendes BDSG und dem Anhang zu § 9 Satz 1 geltendes BDSG.

**Zu Art. 60**

Art. 60 dient der Umsetzung von Art. 30 DSRL-PJ und legt den Umfang und die Modalitäten der Meldung von Verletzungen des Schutzes personenbezogener Daten nach Art. 41 Ziff. 10 der Gesetzesvorlage an die Datenschutzstelle fest. Ansatzpunkt der Meldung sind, wie sich auch aus der systematischen Stellung der Vorschrift im Bereich Sicherheit der Verarbeitung ergibt, Vorfälle wie etwa Datenabflüsse.

Eine Verletzung des Schutzes personenbezogener Daten ist grundsätzlich unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie bekannt geworden ist, der Datenschutzstelle zu melden (Abs. 1).

Die in Abs. 5 geforderte Dokumentation muss in Qualität und Quantität so beschaffen sein, dass sie der Datenschutzstelle die Überprüfung der Einhaltung der gesetzlichen Vorgaben ermöglicht.

Abs. 7 folgt durch einen Verweis auf Art. 37 Abs. 2 der Gesetzesvorlage der Überlegung, wonach die Motivation zur Meldung einer Verletzung des Schutzes personenbezogener Daten nicht dadurch verringert werden soll, dass die durch die Meldung verfügbar werdenden Informationen zur Verarbeitung zur Einleitung eines Strafverfahrens führen können.

Abs. 8 stellt klar, dass die in Art. 56 der Gesetzesvorlage enthaltene Meldepflicht an die Datenschutzstelle andere Meldepflichten nicht ausschliesst bzw. diesen nicht vorgeht.

Art. 60 entspricht § 65 der Rezeptionsvorlage.

**Zu Art. 61**

Art. 61 setzt Art. 31 DSRL-PJ um und bestimmt, dass eine Verletzung des Schutzes personenbezogener Daten der betroffenen Person unverzüglich zu melden ist, wenn voraussichtlich eine erhebliche Gefahr für Rechtsgüter des Betroffenen drohen könnte (Abs. 1).

Nach Abs. 2 hat die Benachrichtigung in klarer und einfacher Sprache die Art der Verletzung zu beschreiben und zumindest die in Art. 60 Abs. 3 Ziff. 2 bis 4 der Gesetzesvorlage genannten Informationen und Massnahmen zu enthalten.

Abs. 3 benennt die Ausnahmen dieser grundsätzlichen Informationspflicht.

Nach Abs. 4 kann die Datenschutzstelle eine ungenügende Benachrichtigung – bzw. das Fehlen einer Ausnahme nach Abs. 3 – förmlich feststellen.

Abs. 5 legt fest, unter welchen Voraussetzungen die Benachrichtigung der betroffenen Personen aufgeschoben, eingeschränkt oder unterlassen werden kann.

In Abs. 6 wird durch einen Verweis auf Art. 37 Abs. 4 der Gesetzesvorlage der Gedanke überführt, wonach auch bei einer Benachrichtigung der betroffenen Person die Motivation zu dieser Benachrichtigung über eine Verletzung des Schutzes personenbezogener Daten nicht dadurch verringert werden soll, dass die durch die Meldung verfügbar werdenden Informationen zur Einleitung eines Strafverfahrens führen können.

Art. 61 entspricht § 65 der Rezeptionsvorlage. Bezüglich Abs. 6 orientiert sich die Rezeptionsvorlage an § 42a Satz 6 geltendes BDSG.

**Zu Art. 62**

Art. 62 dient der Umsetzung von Art. 27 DSRL-PJ und bestimmt, dass der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen hat, wenn die Form der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge hat. Diese Datenschutz-Folgenabschätzung ist ein zentrales Element der strukturellen Stärkung des Datenschutzes.

Die Voraussetzungen zur Durchführung einer Datenschutz-Folgenabschätzung können nur unvollkommen gesetzlich konkret ausgestaltet werden. So lässt sich dennoch feststellen, dass mithilfe einer Datenschutz-Folgenabschätzung vorab hinsichtlich des Umfangs der Verarbeitung nicht eine Einzelverarbeitung, sondern lediglich die Verwendung massgeblicher Systeme und Verfahren zur Verarbeitung personenbezogener Daten in den Blick genommen werden müssen. Insoweit lässt sich – abseits der prozeduralen Verbindung – eine Vergleichbarkeit

mit den Voraussetzungen der Durchführung einer Anhörung der Datenschutzstelle begründen. Kriterien für die Entscheidung, ob die vorgesehene Verarbeitung qualitativ erhöhte Gefahren für die Rechtsgüter der betroffenen Person in sich birgt, können beispielsweise der Kreis der betroffenen Personen, die Art der zur Datenerhebung eingesetzten Mittel oder der Kreis der zugriffsberechtigten Personen, mithin die Eingriffsintensität der mit der Verarbeitung verbundenen Massnahmen im Sinne einer Gesamtwürdigung sein.

Die Konkretisierung der in Abs. 1 genannten Voraussetzungen für eine Datenschutz-Folgenabschätzung obliegt letztlich der Praxis. Dabei wird allerdings zu beachten sein, dass die entstehenden Aufwände angemessen und „beherrschbar“ bleiben müssen, also die Verhältnismässigkeit gewahrt bleiben muss. Ferner ist festzuhalten, dass das Erfordernis einer Datenschutz-Folgenabschätzung nur für neue Verarbeitungssysteme oder wesentliche Veränderungen an bestehenden gilt.

Abs. 2 nimmt Art. 35 Abs. 1 Ziff. 2, Abs. 3 Art. 35 Abs. 2 DSGVO auf und legt fest, dass für die Untersuchung mehrerer ähnlicher Datenverarbeitungen mit ähnlich hohem Gefahrenpotential eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden kann.

Der Verantwortliche hat die Datenschutzstelle gemäss Abs. 3 an der Durchführung der Folgenabschätzung zu beteiligen.

Abs. 4 legt den Inhalt der Datenschutz-Folgenabschätzung fest und konkretisiert die in Art. 27 Abs. 2 der Rezeptionsvorlage enthaltenen allgemeinen Angaben unter Übernahme der Angaben aus Art. 35 Abs. 7 DSGVO enthaltenen Punkte. Eine Datenschutz-Folgenabschätzung ist die systematische Vorabbewertung von Risiken für die Rechte der von den einzelnen Schritten einer Datenbearbeitung betroffenen Personen. Sie dient als Grundlage, um die Datenbearbeitung so aus-

zugestalten, dass die Risiken einer Verletzung der Rechte von Beginn an minimiert werden.

Abs. 5 nimmt Art. 35 Abs. 11 DSGVO auf und bestimmt, dass die Datenschutzstelle erforderlichenfalls prüft, ob eine Datenverarbeitung gemäss der Datenschutz-Folgenabschätzung durchgeführt wird.

Art. 62 entspricht § 67 der Rezeptionsvorlage.

**Zu Art. 63**

Art. 63 setzt Art. 26 DSRL-PJ um. Die hier angesprochene Pflicht des Verantwortlichen zur Zusammenarbeit mit der Datenschutzstelle fasst die ohnehin sich aus anderen Vorschriften ergebenden Kooperationsverpflichtungen und Kooperationsbeziehungen zwischen Verantwortlichem und der Datenschutzstelle zusammen.

Art. 63 entspricht § 68 der Rezeptionsvorlage.

**Zu Art. 64**

Art. 64 dient der Umsetzung von Art. 28 DSRL-PJ. Die Anhörung der Datenschutzstelle dient der datenschutzrechtlichen Absicherung in Bezug auf beabsichtigte Verarbeitungen in neu anzulegenden Dateisystemen, die ein erhöhtes Gefährdungspotential für Rechtsgüter der betroffenen Personen in sich bergen. Insofern besteht eine enge inhaltliche Verbindung zum Instrument der Datenschutz-Folgenabschätzung (Art. 62 der Gesetzesvorlage).

Prozedural wird diese Verbindung dadurch hergestellt, dass nach Abs. 1 Ziff. 1 eine Anhörung der Datenschutzstelle durchzuführen ist, wenn im Ergebnis einer Datenschutz-Folgenabschätzung eine erhöhte Gefährdung angenommen wird und der Verantwortliche hierauf nicht mit Massnahme zur Gefährdungsminimierung reagiert.

Der Umfang der der Datenschutzstelle vorzulegenden Unterlagen wird in Abs. 2 durch Zusammenführung der Vorgaben aus Art. 28 Abs. 4 DSRL-PJ und Art. 36 Abs. 3 DSGVO angeglichen.

Nach Abs. 3 kann die Datenschutzstelle – wenn sie der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstossen würde – dem Verantwortlichen Empfehlungen unterbreiten, welche Massnahmen noch ergriffen werden sollten.

Gemäss Abs. 4 kann mit der Verarbeitung personenbezogener Daten nach der Anhörung begonnen werden, wenn die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung hat. Zwar wird man im Regelfall den Abschluss der Konsultation im Interesse der Betroffenen abwarten. Im Ausnahmefall können jedoch Abweichungen geboten sein. Die in Abs. 4 vorgesehene Eilfallregelung trägt solchen operativen und fachlichen Erfordernissen in Abweichung von Abs. 3 Satz 1 Rechnung. Die Nutzung der Eilfallregelung entbindet den Verantwortlichen gleichwohl nicht davon, die Empfehlungen der Datenschutzstelle nach pflichtgemässem Ermessen zu prüfen und die Verarbeitung gegebenenfalls daraufhin anzupassen. Zudem schmälert die Eilfallregelung nicht die der Datenschutzstelle zur Verfügung stehenden Befugnisse.

Art. 64 entspricht § 69 der Rezeptionsvorlage.

**Zu Art. 65**

Art. 65 dient der Umsetzung von Art. 24 DSRL-PJ und verpflichtet den Verantwortlichen zur Führung eines Verzeichnisses über bei ihm durchgeführte Kategorien von Datenverarbeitungstätigkeiten. Dieses Verzeichnis dient vor allem der Datenschutzstelle dazu, einen Überblick über die beim Verantwortlichen durchgeführten Datenverarbeitungen zu erhalten. Das Zusammenspiel von Anhörung der Datenschutzaufsicht (Art. 64 der Gesetzesvorlage), Einsicht in das Verzeichnis

(Art. 65 Abs. 3 der Gesetzesvorlage) und Zurverfügungstellung von Protokolldaten (Art. 71 Abs. 5 der Gesetzesvorlage) gewährt der Datenschutzstelle ein umfassendes Bild über die beim Verantwortlichen durchgeführten Datenverarbeitungen. Dies ermöglicht es ihr, ihre Aufgaben und Befugnisse im Hinblick auf den jeweiligen Verantwortlichen zielgerichtet, effizient und verhältnismässig auszurichten und zu nutzen. Die Beteiligung der Datenschutzstelle wird arrondiert und ergänzt durch die interne Beratungs- und Kontrolltätigkeit der Datenschutzstelle gemäss Art. 7 der Gesetzesvorlage und die in Art. 16 Abs. 4 der Gesetzesvorlage enthaltene Regelung zum umfassenden Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen.

In Abs. 1 werden die in das Verzeichnis aufzunehmenden Angaben benannt. Die Begrifflichkeit „Kategorien von Datenverarbeitungstätigkeiten“ stellt hierbei klar, dass sich das Verzeichnis nicht auf einzelne Datenverarbeitungsvorgänge, sondern auf sinnvoll abgrenz- und kategorisierbare Teile der beim Verantwortlichen durchgeführten Datenverarbeitungen bezieht.

Abs. 2 verpflichtet den Verantwortlichen, ein Verzeichnis, wenngleich in geringerem Umfang, auch für Verarbeitungen zu führen, wenn er personenbezogene Daten im Auftrag verarbeitet.

In Abs. 3 werden Aussagen zur Form des Verzeichnisses (schriftlich oder elektronisch) getroffen. Dies bedeutet, dass Verzeichnisse entweder rein elektronisch geführt oder auch durch Ausdrucke oder in sonstiger schriftlicher Form geführt werden können.

Nach Abs. 4 werden das Verzeichnis und seine Aktualisierungen der Datenschutzstelle auf Anfrage zur Verfügung gestellt.

Art. 65 entspricht § 70 der Rezeptionsvorlage.

**Zu Art. 66**

Durch Art. 66 wird Art. 20 DSRL-PJ umgesetzt, welcher generische Anforderungen an die datenschutzfreundliche Gestaltung von Datenverarbeitungssystemen (*Privacy by Design*), d.h. ein Systemaufbau, welcher die Privatsphäre bereits im Kern berücksichtigt, und die Implementierung datenschutzfreundlicher Grundeinstellungen (*Privacy by Default*), d.h. ein Systemaufbau, bei dem die Verarbeitungsoptionen am Anfang grundsätzlich auf den privatsphärenfreundlichsten Optionen eingestellt sind und weitere Optionen zur Einschränkungen der Privatsphäre erst nachträglich gewählt werden können, formuliert. Der Norm liegt der Gedanke zugrunde, dass der Aufwand zur Verfolgung der hier formulierten Ziele und Anforderungen im Sinne effizienten Mitteleinsatzes in einem angemessenen Verhältnis zum angestrebten Schutzzweck stehen sollte.

Die in Abs. 2 angesprochene Anforderung, die automatisierte umfassende Zugänglichmachung personenbezogener Daten zu verhindern, mündet letztlich in die Anforderung, eine solche Zugänglichmachung stets durch menschliches Zutun einer Prüfung zu unterziehen.

Art. 66 entspricht § 71 der Rezeptionsvorlage. Die Rezeptionsvorlage orientiert sich weiterhin an § 3a geltendes BDSG.

**Zu Art. 67**

Art. 67 dient der Umsetzung von Art. 6 DSRL-PJ. Die Bestimmung regelt die Unterscheidung zwischen verschiedenen Kategorien betroffener Personen. Der Verantwortliche soll bei der Verarbeitung von personenbezogenen Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen unterscheiden. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa der Unterscheidung entsprechende Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Massnahmen der Datensicherheit, werden Spezialgesetzen überlassen.

Art. 67 entspricht § 72 der Rezeptionsvorlage.

**Zu Art. 68**

Art. 68 dient der Umsetzung von Art. 7 Abs. 1 DSRL-PJ. Die Bestimmung legt fest, dass der Verantwortliche bei der Verarbeitung danach unterscheiden muss, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Beurteilungen, die auf persönlichen Einschätzungen beruhen, sollen möglichst als solche kenntlich gemacht werden. Die konkreten Rechtsfolgen der vorgesehenen Unterscheidung bei der Verarbeitung, etwa der Unterscheidung entsprechende Aussonderungsprüffristen, Rechte- und Rollenkonzepte oder besondere Massnahmen der Datensicherheit, werden Spezialgesetzen überlassen.

Art. 68 entspricht § 73 der Rezeptionsvorlage.

**Zu Art. 69**

Gemäss Abs. 1 hat der Verantwortliche angemessene Massnahmen zu ergreifen, um zu gewährleisten, dass unrichtige oder nicht mehr aktuelle personenbezogene Daten nicht übermittelt oder sonst zur Verfügung gestellt werden. Abs. 1 dient damit der Umsetzung von Art. 7 Abs. 2 DSRL-PJ.

Bei der Anwendung und Auslegung der Anforderungen des Art. 69 der Gesetzesvorlage ist zu beachten, dass die Frage nach der „Aktualität“ von Daten und der damit verbundenen Vorgabe, keine „nicht mehr aktuellen“ Daten zu übermitteln bzw. bereitzustellen, stets nur im konkreten Ermittlungszusammenhang und unter Beachtung des konkreten Verarbeitungszwecks beantworten lässt. In bestimmten Ermittlungszusammenhängen kann auch die Übermittlung nicht (mehr) aktueller Daten, wie alte Meldeadressen, alte (Geburts-)namen etc., bedeutsam und für die Aufgabenerfüllung erforderlich sein.

Abs. 2 wiederum setzt Art. 9 Abs. 3 DSRL-PJ um. Beispiele für die in Spezialgesetzen vorgesehene Mitgabe besonderer Bedingungen können Zweckbindungsrege-

lungen bei der Weiterverarbeitung durch den Empfänger, das Verbot der Weiterübermittlung ohne Genehmigung oder Konsultationserfordernisse vor der Beauskunftung betroffener Personen durch den Empfänger sein.

Abs. 3 Setzt Art. 9 Abs. 4 DSRL-PJ um. Er stellt sicher, dass unter den EWR/Schengen-Staaten und den zugehörigen Institutionen eine einheitliche Anwendung sichergestellt ist.

Art. 69 entspricht § 74 der Rezeptionsvorlage.

**Zu Art. 70**

Art. 70 dient der Umsetzung von Art. 16 DSRL-PJ in seiner Ausformung als Pflicht des Verantwortlichen. Systematisch werden in Art. 70 Pflichten des Verantwortlichen zur Berichtigung und Löschung personenbezogener Daten sowie zur Einschränkung ihrer Verarbeitung thematisiert, die unabhängig davon bestehen, ob eine betroffene Person darum ersucht. Die spiegelbildlich bestehenden Rechte der betroffenen Person auf Berichtigung, Löschung personenbezogener Daten sowie auf Einschränkung der Verarbeitung durch den Verantwortlichen finden sich in Art. 53 der Gesetzesvorlage.

In Abs. 1 wird die Pflicht des Verantwortlichen zur Berichtigung nach Art. 16 Abs. 5 DSRL-PJ umgesetzt.

Abs. 2 dient der Umsetzung von Art. 16 Abs. 2 DSRL-PJ, in dem gleichzeitig sowohl das Betroffenenrecht auf Löschung als auch die unabhängig davon bestehende Pflicht des Verantwortlichen zur Löschung erwähnt wird. Im Übrigen wird auf die Ausführungen zu Art. 53 Abs. 3 der Gesetzesvorlage verwiesen.

Abs. 3 dient der Umsetzung von Art. 5 DSRL-PJ und übernimmt den Katalog der Voraussetzungen für eine Einschränkung der Datenbearbeitung. Zudem dient Abs. 3 der Umsetzung von Art. 16 Abs. 6 und Art. 7 Abs. 3 DSRL-PJ und legt fest,

dass dem Empfänger mitzuteilen ist, wenn unrichtige personenbezogene Daten übermittelt wurden oder personenbezogenen Daten unrechtmässig übermittelt worden sind.

Abs. 4 hält fest, dass der Verantwortliche generell für die Löschung oder eine Überprüfung der Notwendigkeit der Speicherung angemessene Fristen vorsehen muss. Abs. 4 dient damit der Umsetzung von Art. 16 Abs. 6 und Art. 7 Abs. 3 DSRL-PJ.

Art. 70 entspricht § 75 der Rezeptionsvorlage.

**Zu Art. 71**

Art. 71 dient der Umsetzung von Art. 25 DSRL-PJ und statuiert in Abs. 1 eine umfassende Pflicht des Verantwortlichen zur Protokollierung der unter seiner Verantwortung durchgeführten Datenverarbeitungen.

Abs. 2 enthält konkrete Vorgaben an den Inhalt der Protokolle.

Abs. 3 führt Verwendungsbeschränkungen an, wobei von der durch die DSRL-PJ eröffneten Möglichkeit, die Protokolldaten über die Datenschutzkontrolle, Eigenüberwachung und Aufrechterhaltung der Datensicherheit hinaus auch im Zusammenhang mit der Verhütung oder Verfolgung von Straftaten zu verwenden, Gebrauch gemacht wird.

In Abs. 4 wird eine Löschfrist für die Protokolldaten bestimmt (am Ende des auf deren Generierung folgenden Jahres).

In Abs. 5 wird festgelegt, dass die Protokolle der Datenschutzstelle zum Zweck der Datenschutzkontrolle zur Verfügung stehen müssen.

Art. 71 entspricht § 76 der Rezeptionsvorlage.

**Zu Art. 72**

Art. 72 dient der Umsetzung von Art. 48 DSRL-PJ. Der Verantwortliche hat im Zusammenhang mit der Meldung von Verstössen sowohl verantwortlicheninterne Meldungen als auch Hinweise von betroffenen Personen oder sonstigen Dritten in den Blick zu nehmen. Für beide Stränge bietet sich als Kontakt- und Beratungsstelle der Datenschutzbeauftragte an.

Art. 72 entspricht § 77 der Rezeptionsvorlage.

**Zu Art. 73**

Art. 73 dient der Umsetzung von Art. 35 DSRL-PJ und statuiert Voraussetzungen und Anforderungen, die bei jeder Datenübermittlung an Stellen in Drittstaaten oder an internationale Organisationen vorliegen müssen. Dies auch bezüglich der insbesondere nach Art. 74 bis 76 der Gesetzesvorlage erforderlichen Abwägungsentscheidung.

In besonderer Ausprägung dessen fordert Abs. 2 ein Unterbleiben der Übermittlung, wenn im Einzelfall Anlass zur Besorgnis besteht und diese Besorgnis auch nach einer Prüfung durch den Verantwortlichen weiter besteht, dass ein elementaren rechtsstaatlichen Grundsätzen genügender Umgang mit den übermittelten Daten nicht gesichert ist. Hierbei ist besonders zu berücksichtigen, wenn der Empfänger einen angemessenen Schutz der Daten garantiert.

Abs. 3 regelt die Notwendigkeit einer Bewilligung, wenn personenbezogene Daten, die aus einem anderen EU/Schengen-Staat übermittelt oder zur Verfügung gestellt wurden, nach Abs. 1 übermittelt werden sollen.

Abs. 4 regelt die Verpflichtung des Übermittelnden, durch geeignete Massnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale Organisationen weiterübermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat.

Art. 73 entspricht § 78 der Rezeptionsvorlage.

**Zu Art. 74**

Art. 74 dient der Umsetzung von Art. 37 DSRL-PJ. Es werden zu Art. 73 der Gesetzesvorlage ergänzende Voraussetzungen für Datenübermittlungen an Stellen in Drittstaaten, zu denen die Europäische Kommission keinen in den EWR übernommenen Angemessenheitsbeschluss gemäss Art. 36 DSRL-PJ gefasst hat, formuliert. Bei solchen Konstellationen kommt dem Verantwortlichen – insbesondere nach Art. 74 Abs. 1 Ziff. 2 der Gesetzesvorlage – die Aufgabe zu, das Vorliegen geeigneter Garantien für den Schutz personenbezogener Daten beim Empfänger zu beurteilen. In der Praxis kann nach einer solchen Beurteilung die Datenübermittlung mit der Mitgabe von Verarbeitungsbedingungen – etwa Löschverpflichtungen nach Zweckerreichung, Weiterübermittlungsverbote, Zweckbindungen – verbunden werden. Ein solches Vorgehen ist dazu geeignet, diese Beurteilung zu dokumentieren und ihr Ergebnis zu sichern. Im Zusammenhang mit dem auch hier anwendbaren Art. 73 Abs. 2 der Gesetzesvorlage entfaltet der dort erwähnte Gesichtspunkt der Einzelfallgarantie des Empfängerstaats bei der Prüfung des Vorhandenseins geeigneter Garantien besondere Bedeutung.

Abs. 2 dient der Umsetzung von Art. 37 Abs. 3 DSRL-PJ zur Dokumentation der Übermittlungen nach Art. 74 der Gesetzesvorlage.

Abs. 3 dient der Umsetzung von Art. 37 Abs. 2 DSRL-PJ, der die Unterrichtung der Datenschutzstelle über Kategorien von Übermittlungen vorsieht, die ohne Vorliegen eines Angemessenheitsbeschlusses der EU, aber wegen Bestehens geeigneter Garantien für den Schutz personenbezogener Daten im Drittstaat nach entsprechender Beurteilung durch den übermittelnden Verantwortlichen erfolgen.

Art. 74 entspricht § 79 der Rezeptionsvorlage.

**Zu Art. 75**

Art. 75 dient der Umsetzung von Art. 38 DSRL-PJ und beleuchtet Konstellationen, in denen weder ein in den EWR übernommener Angemessenheitsbeschluss der Europäischen Kommission vorliegt noch die in Art. 74 der Gesetzesvorlage erwähnten Garantien in Form eines rechtsverbindlichen Instruments oder nach Beurteilung durch den übermittelnden Verantwortlichen bestehen.

Abs. 2 verbietet die Übermittlung, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

Abs. 3 erklärt die Bestimmungen des Art. 74 Abs. 2 der Gesetzesvorlage über die Dokumentation der Übermittlungen auch in diesen Fällen für anwendbar.

Art. 75 entspricht § 80 der Rezeptionsvorlage.

**Zu Art. 76**

Art. 76 dient der Umsetzung von Art. 39 DSRL-PJ. Die hier geregelte Konstellation zeichnet sich dadurch aus, dass der Kreis der möglichen Empfänger über öffentliche Stellen, die im Rahmen der Strafverfolgung tätig sind, hinaus auf sonstige öffentliche Stellen und Private ausgeweitet wird. Abgebildet werden etwa Ersuchen an Finanzinstitutionen oder Telekommunikationsdienstleister, die notwendigerweise mit der Übermittlung personenbezogener Daten verbunden sind.

Für solche Übermittlungen „im besonderen Einzelfall“ gelten die in Abs. 1 genannten strengen Voraussetzungen.

Gemäss Abs. 2 hat der Verantwortliche im Fall des Abs. 1 bestimmte in Art. 73 Abs. 1 Ziff. 1. genannte Stellen über die Übermittlung zu unterrichten.

Abs. 3 erklärt die Bestimmungen des Art. 74 Abs. 2 (Dokumentation) und Abs. 3 der Gesetzesvorlage (jährliche Berichterstattung an die Datenschutzstelle) auch in diesen Fällen für anwendbar.

In Abs. 4 ist eine verstärkte Zweckbindung der gemäss Art. 76 der Gesetzesvorlage übermittelten Daten vorgesehen.

Abs. 5 stellt klar, dass Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit unberührt bleiben.

Art. 76 entspricht § 81 der Rezeptionsvorlage.

**Zu Art. 77**

Art. 77 dient der Umsetzung des Art. 50 DSRL-PJ und regelt die Zusammenarbeit der Aufsichtsbehörden. Die Datenschutzstelle hat den EU/Schengen-Aufsichtsbehörden Informationen zu übermitteln und Amtshilfe zu leisten. Die Amtshilfe betrifft insbesondere Auskunftsersuchen und aufsichtsbezogene Massnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

Abs. 1 bestimmt die grundsätzliche Verpflichtung zur Leistung der Amtshilfe.

Abs. 2 schreibt vor, dass ein Amtshilfeersuchen spätestens innerhalb eines Monats nach deren Eingang zu erledigen ist.

Abs. 3 legt fest, unter welchen Voraussetzungen die Datenschutzstelle die Erledigung eines Amtshilfeersuchens ablehnen kann. Als Kriterien kommen nur die Unzuständigkeit und die Gesetzeswidrigkeit in Frage.

Mit Abs. 4 wird die Datenschutzstelle zur Information über das laufende Amtshilfeersuchen gegenüber der ersuchenden Stelle verpflichtet.

Abs. 5 bestimmt, dass die Kommunikation in Amtshilfesachen vorzugsweise in elektronischer Form und in standardisierten Formaten erfolgt. Als standardisiertes Format kann gelten, was üblich ist (so z.B. PDF oder andere gängige Formate).

Gemäss Abs. 6 werden Amtshilfeersuchen grundsätzlich kostenfrei erledigt. Allerdings sind andere Vereinbarungen zu Kosten unter den Aufsichtsbehörden möglich.

In Abs. 7 wird der notwendige Inhalt eines Amtshilfeersuchens näher definiert.

Art. 77 entspricht § 82 der Rezeptionsvorlage.

**Zu Art. 78**

Die Vorschrift setzt Art. 56 DSRL-PJ um. Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten einen Schaden zugefügt, ist er gegenüber der betroffenen Person zu Schadensersatz verpflichtet.

Nach Abs. 1 ist ein Verantwortlicher, welcher einer betroffenen Person durch eine rechtswidrige Verarbeitung personenbezogener Daten einen Schaden zufügt, zu Schadenersatz verpflichtet. Bei nicht automatisierten Datenverarbeitungen ist zusätzlich ein Verschulden Voraussetzung.

Abs. 2 enthält eine besondere Bestimmung betreffend die Art des Schadenersatzes.

In Abs. 3 wird bei automatisierten Verarbeitungen eine Regelung bezüglich der gemeinsamen Haftung festgelegt, wenn der Verantwortliche, dem der Schaden zuzuordnen ist, nicht eindeutig festgestellt werden kann.

Der Abs. 4 verweist im Fall eines Mitverschuldens der betroffenen Person auf die entsprechenden Bestimmungen des ABGB (§§ 1301 bis 1304).

Abs. 5 regelt schliesslich die Verjährung unter Verweis auf das ABGB.

Art. 78 entspricht § 83 der Rezeptionsvorlage.

**Zu Art. 79**

Die Vorschrift setzt Art. 57 DSRL-PJ um, welcher es den Staaten überlässt, Sanktionen bei Verstössen gegen die nach dieser Richtlinie erlassenen Vorschriften zu verhängen. Durch den in Art. 79 der Gesetzesvorlage enthaltenen Verweis auf Art. 37 der Gesetzesvorlage werden im Bereich der Richtlinie dieselben Sanktionen angewendet. Es wird auf die Erläuterungen zu Art. 42 der Gesetzesvorlage verwiesen.

Art. 79 entspricht § 84 der Rezeptionsvorlage.

**Zu Art. 80**

Die Vorschrift enthält spezifische Regelungen für Verarbeitungen personenbezogener Daten im Rahmen von nicht in die Anwendungsbereiche der DSGVO und der DSRL-PJ fallenden Tätigkeiten.

Abs. 1 enthält eine Übermittlungsvorschrift an Drittstaaten und supra- oder internationale Organisationen ausschliesslich zur Erfüllung der in der Vorschrift genannten Zwecke.

Abs. 2 normiert eine Ausnahme der Betretungsbefugnis nach Art. 16 Abs. 4 der Gesetzesvorlage, soweit eine Gefährdung der Sicherheit des Landes gegeben ist. Wenn eine solche Betretung bei der Landespolizei eine Gefährdung der Sicherheit des Landes darstellen könnte, kann die Regierung diese Gefährdung durch Beschluss feststellen und hat eine Betretung in diesen Fällen zu unterbleiben. Eine Gefährdung des Landes kann beispielsweise im Bereich des Staatsschutzes gegeben sein. Zum Staatsschutz nach Art. 2 Abs. 2 PolG gehören die Erkennung, Verhinderung und Bekämpfung von Gefährdungen des Bestandes des Staates und seiner Einrichtungen. Als solche Gefährdungen gelten: Aktivitäten, die auf eine gewaltsame Änderung der staatlichen Ordnung abzielen; Terrorismus; Angriffe gegen den Staat, Störung der Beziehung zum Ausland, Landesverrat und

wirtschaftlicher Nachrichtendienst; gewalttätiger Extremismus; organisierte Kriminalität; Vorbereitungen zu verbotenem Handel mit Waffen und radioaktiven Materialien sowie zu verbotenem Technologietransfer.

Abs. 3 Satz 1 enthält einen speziellen Ausschluss von den Informationspflichten gemäss Art. 13 Abs. 1 und 2 DSGVO, der nur für öffentliche Stellen gilt, die nicht in den Anwendungsbereich der DSGVO und der DSRL-PJ fallen, und soweit keine spezialgesetzliche Regelung besteht. Der Ausschluss ist notwendig, um bei Verarbeitungen personenbezogener Daten im Bereich der nationalen Sicherheit und der Erfüllung staatsvertraglicher Verpflichtungen auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung, die nicht spezialgesetzlich geregelt sind, zu regeln. Nach Satz 2 ist das Recht auf Auskunft ausgeschlossen, wenn eine Informationspflicht nicht besteht. Satz 3 bestimmt, dass die Regelungen nach Art. 29 Abs. 2 und Art. 30 Abs. 2 der Gesetzesvorlage bei Unterbleiben der Informierung bzw. Auskunft bei Verarbeitungen nach Satz 1 keine Anwendung finden.

**Zu den Übergangsbestimmungen**

**Zu Art. 81**

Art. 81 bestimmt, dass die Regierung die zur Durchführung dieser Gesetzesvorlage notwendigen Verordnungen erlässt.

**Zu Art. 82**

Art. 82 hebt das geltende Datenschutzgesetz zum Zeitpunkt des Inkrafttretens dieser Gesetzesvorlage auf.

**Zu Art. 83**

Abs. 1 und 2 knüpfen an Art. 8 der Gesetzesvorlage an und legen fest, dass der vom Landtag gemäss dem geltenden DSG gewählte Datenschutzbeauftragte und das übrige Personal auf den Zeitpunkt des Inkrafttretens dieser Gesetzesvorlage

in die neu beim für den Geschäftsbereich Justiz zuständigen Ministerium eingerichtete Datenschutzstelle überführt werden.

Zudem wird festgelegt, dass die Amtszeit des Datenschutzbeauftragten durch das Inkrafttreten dieser Gesetzesvorlage nicht unterbrochen wird und somit nach Ablauf von acht Jahren nach seiner Wahl durch den Landtag endet.

**Zu Art. 84**

Art. 84 hält fest, dass die Amtszeit der Datenschutzkommission mit dem Inkrafttreten dieser Gesetzesvorlage endet und deren Aufgaben ab diesem Zeitpunkt durch die Beschwerdekommission für Verwaltungsangelegenheiten ausgeübt werden.

Mit der Schaffung des Datenschutzgesetzes im Jahr 2002 wurde auch die Datenschutzkommission als Entscheidungs- und Beschwerdeinstanz ins Leben gerufen. Der Geschäftsanfall der Datenschutzkommission war in all den Jahren sehr gering, so dass sich die Aufrechterhaltung einer eigenständigen Kommission nicht weiter rechtfertigen lässt.

**Zu Art. 85**

Art. 85 bestimmt, dass zum Zeitpunkt des Inkrafttretens dieser Gesetzesvorlage bereits erteilte Bewilligungen für eine Videoüberwachung ihre Gültigkeit behalten. Eine Verlängerung einer zum Zeitpunkt des Inkrafttretens dieser Gesetzesvorlage bereits bewilligten Videoüberwachung richtet sich aber ab dem Inkrafttreten dieser Gesetzesvorlage nach dieser.

**Zu Art. 86**

Art. 86 ändert in den dort genannten Gesetzen die Bezeichnung "Personendaten" in die Bezeichnung "personenbezogene Daten" ab.

## 1. ABÄNDERUNG DES GESETZES ÜBER DIE BETRIEBLICHE PERSONALVORSORGE DES STAATES

**Zu Art. 1 Bst. d**

Da die Datenschutzstelle neu beim für den Geschäftsbereich Justiz zuständigen Ministerium eingerichtet wird, erübrigt sich eine gesonderte Nennung der Datenschutzstelle in Art. 1 Bst. d, zumal die Datenschutzstelle als beim für den Geschäftsbereich Justiz zuständigen Ministerium eingerichtete Stelle neu unter Art. 1 Bst. c (Personal der Landesverwaltung) subsummiert werden kann.

## 2. ABÄNDERUNG DES FINANZKONTROLLGESETZES

**Zu Art. 14 Abs. 4**

Nachdem die Datenschutzstelle neu beim für den Geschäftsbereich Justiz zuständigen Ministerium eingerichtet wird und damit die bisher geltenden Zuständigkeiten des Landtagspräsidiums im Zusammenhang mit der Datenschutzstelle entfallen, erübrigt sich die Nennung der Datenschutzstelle in Art. 14 Abs. 4, wonach in Bezug auf die Datenschutzstelle das Landtagspräsidium zu benachrichtigen wäre.

**Zu Art. 15**

Zumal die Datenschutzstelle neu beim für den Geschäftsbereich Justiz zuständigen Ministerium eingerichtet wird und damit die bisher geltenden Zuständigkeiten des Landtagspräsidiums im Zusammenhang mit der Datenschutzstelle entfallen, erübrigt sich die Nennung der Datenschutzstelle in Art. 15, wonach die Finanzkontrolle in Bezug auf die Datenschutzstelle allfällige Anträge an das Landtagspräsidium zu richten hätte.

Der Vollständigkeit halber wird an dieser Stelle darauf hingewiesen, dass die Datenschutzstelle aufgrund der bisher geltenden Zuordnung zum Landtag in Art. 10

Abs. 2 Bst. e der Geschäftsordnung für den Landtag des Fürstentums Liechtenstein erwähnt ist. Wenn die Datenschutzstelle neu beim für den Geschäftsbereich Justiz zuständigen Ministerium eingerichtet ist, wäre Art. 10 Abs. 2 Bst. e der Geschäftsordnung für den Landtag des Fürstentums Liechtenstein entsprechend anzupassen.

## 3. ABÄNDERUNG DES BESCHWERDEKOMMISSIONSGESETZES

**Zu Art. Art. 4 Abs. 1 Bst. s**

Abs. 1 Bst. s legt die Zuständigkeit der Beschwerdekommission für Verwaltungsangelegenheiten neu auch für Beschwerden gegen Verfügungen und Entscheidungen im Bereich Datenschutz fest.

## 4. ABÄNDERUNG DES POLIZEIGESETZES

**Zu Art. 24d**

Auf der Grundlage der Terminologie des neuen DSG wird in Abs. 5 der Begriff „Personendaten“ durch den Begriff „personenbezogene Daten“ ersetzt.

**Zu Art. 30a**

Auf der Grundlage der Terminologie des neuen DSG wird in Abs. 1 Bst. d der Begriff „besonders schützenswerte Personendaten“ wird durch den Begriff „besonderen Kategorien personenbezogener Daten“ ersetzt.

**Zu Art. 30c**

Aufgrund der Totalrevision des DSG wird in Abs. 2 der Verweis auf dieses entsprechend korrigiert.

**Zu Art. 30f**

In der Sachüberschrift unter Bst. c wird der Begriff „Datenbekanntgabe“ entsprechend der neuen Terminologie des neuen DSG auf „Datenoffenlegung“ korrigiert.

In Bst. a dieser Bestimmung werden erneut begriffliche Abänderungen im Hinblick auf die im DSG neu verwendeten Ausdrücke durchgeführt. Der Verweis auf das DSG wird gestrichen, da diese Ausnahme unter dem neuen Rechtsrahmen nicht mehr erforderlich ist.

**Zu Art. 31**

In der Überschrift vor Art. 31 wird die Kapitelüberschrift von „Bearbeiten“ auf „Verarbeitung von polizeilichen Daten“ angepasst. Ebenso wird die Sachüberschrift in Art. 31 von „Datenbearbeitung“ auf „Datenverarbeitung“ angepasst. Dies entspricht den im neuen DSG verwendeten Begrifflichkeiten.

Abs. 1 erfolgen wiederum begriffliche Anpassungen im Hinblick auf die im neuen DSG verwendeten Ausdrücke. Zudem wird ausgeführt, was beispielsweise unter „besonderen Kategorien personenbezogener Daten“ zu verstehen ist.

In Abs. 2 werden die Begriffe „Bearbeitung“ und „Weiterbearbeitung“ durch die Begriffe „Verarbeitung“ und „Weiterverarbeitung“ ersetzt.

In Abs. 3 wir präzisiert, dass es sich um „personenbezogene“ Daten gemäss Abs. 1 handelt.

Abs. 4 regelt die nachträgliche Information der betroffenen Person gemäss Abs. 1 und setzt Art. 13 Abs. 3 DSRL-PJ um.

**Zu Art. 34a**

Die Abänderungen in Abs. 8 Bst. b und c betreffen begriffliche Anpassungen. Das Wort „Datenbearbeitung“ wird durch „Datenverarbeitung“ ersetzt und das Wort „personenbezogene“ wird an zwei Stellen ergänzt.

**Zu Art. 34 b**

Neben begrifflichen Anpassungen im Hinblick auf die im neuen DSG verwendeten Ausdrücke (Datenverarbeitung, Datenverarbeitungsregeln, personenbezogene

Daten) wird ausgeführt, was beispielsweise unter „besonderen Kategorien personenbezogener Daten“ zu verstehen ist. In Abs. 2 wird Bst. d um den Begriff Profiling ergänzt. Dabei handelt es sich um die Erstellung von Persönlichkeitsprofilen und damit um einen der Recherche vorgelagerten Schritt, der gesondert erwähnt werden soll.

**Zu. Art. 34c**

In den Abs. 1 und 2 werden begriffliche Anpassungen im Hinblick auf die im DSG neu verwendeten Ausdrücke gemacht. Das Wort „Personendaten“ wir durch „personenbezogene Daten“ und das Wort „bearbeitete“ durch den präzisierten Ausdruck „verarbeitete personenbezogene“ ersetzt.

**Zu Art. 34d**

In Abs. 1 erfolgen begriffliche Anpassungen. Wie schon bei anderen Bestimmungen dieser Vorlage wird hier der Ausdruck „besonderer Kategorien personenbezogener Daten“ anstelle von „besonders schützenswerter Personendaten“ eingefügt. Zudem wird der Begriff „Persönlichkeitsprofile“ durch „Daten aus dem Profiling“ ersetzt und anstelle des Wortes „bekanntgeben“ wird unter dem Begriff „Datenbekanntgabe“ neu von „offenlegen oder übermitteln“ gesprochen. Der bisherige Bst. a wird in Abs. 1 integriert und Bst. b gestrichen.

In den Abs. 2 und 3 finden sich ebenfalls begriffliche Anpassungen (siehe „personenbezogene Daten“).

In Abs. 4 erfolgt eine begriffliche Präzisierung („diese“ Daten).

**Zu Art. 34e**

In den Abs. 2 und 3 wird der Begriff „Personendaten“ durch den Begriff „personenbezogene Daten“ ersetzt.

**Zu Art. 34f**

Da es sich bei dieser Bestimmung um eine reine Verweisnorm handelt, wird diese aufgehoben. Inhaltlich erfolgt eine Neuregelung in Art. 64 und 76 neues DSG.

**Zu Art. 34g**

In Abs. 1 erfolgt eine Korrektur des Verweises auf das neue DSG.

In Abs. 2 wird der Begriff „bearbeitet“ durch den Begriff „verarbeitet“ ersetzt und präzisiert, dass es sich um „personenbezogene“ Daten handelt.

**Zu Art. 34h**

In den Abs. 1, 3, 4, 6 und 7 werden begriffliche Änderungen vorgenommen („personenbezogene“ Daten und „Datenverarbeitung“ anstelle von „Datenbearbeitung“).

Zudem wird in den Abs. 1 und 7 der Satzteil „oder zur vorbeugenden Bekämpfung von Straftaten (Art. 2 Abs.1 Bst. d)“ gestrichen, da aufgrund der DSRL-PJ nur noch Ausnahmen hinsichtlich des Staatsschutzes vorgesehen sind.

**Zu Art. 34i**

Dieser Art. wird aufgehoben, da der Inhalt von Abs. 1 neu in Art. 75 DSG und jener von Abs. 2 in Art. 16 DSG geregelt wird. Der Rechtsmittelweg vom bisherigen Abs. 3 kann entfallen, da neu Rechtsmittel an die Beschwerdekommission für Verwaltungsangelegenheiten zu richten sind.

**Zu Art. 35**

In den Abs. 1, 4 und 6 wird der Begriff „Personendaten“ durch den Begriff „personenbezogenen Daten“ ersetzt. In Abs. 3 Bst. c, bei welchem es um die Leistung von Amtshilfe geht, erfolgen Ergänzungen hinsichtlich geeigneter Garantien nach Art. 79 DSG und ein Vorbehalt betreffend Art. 80 DSG.

**Zu Art. 35a**

Abs. 1 Bst. a wird an die neuen Begrifflichkeiten des DSG angepasst. Es wird zudem ausgeführt, was beispielsweise unter „besonderen Kategorien personenbezogener Daten“ zu verstehen ist. Zudem wird der Begriff „Persönlichkeitsprofile“ durch „Daten aus dem Profiling“ ersetzt. In Abs. 2 erfolgt wiederum eine Anpassung des Begriffs „Personendaten“ auf neu „personenbezogene Daten“ und des Begriffs “bearbeitet“ auf neu „verarbeitet“.

**Zu Art. 35p**

Die Sachüberschrift wird gemäss neuer Terminologie des DSG von „Datenübermittlung“ auf den Begriff „Bekanntgabe“ angepasst. Art. 8 Abs. 1 DSRL-PJ verlangt für die Verarbeitung von Personendaten eine entsprechende Rechtsgrundlage. Somit muss die Kompetenz zur Datenübermittlung unter Verweis auf das DSG in diesem Gesetz festgehalten werden wird.

**Zu Art. 35q**

Art. 8 Abs. 1 DSRL-PJ verlangt für die Verarbeitung von Personendaten eine entsprechende Rechtsgrundlage. Somit muss die Kompetenz zur Datenübermittlung unter Anpassung des bisherigen Texts und Verweis auf das DSG in diesem Gesetz festgehalten werden.

## 5. VERFASSUNGSMÄSSIGKEIT / RECHTLICHES

Dieser Vorlage stehen keine verfassungsrechtlichen Bestimmungen entgegen.

# V. REGIERUNGSVORLAGEN

## 1. DATENSCHUTZGESETZ

# Datenschutzgesetz (DSG)

vom…

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich meine Zustimmung:

### Teil 1

### Gemeinsame Bestimmungen

#### Kapitel 1

Anwendungsbereich und Begriffsbestimmungen

Art. 1

*Anwendungsbereich*

1) Dieses Gesetz gilt für die Verarbeitung personenbezogener Daten durch öffentliche Stellen. Für nicht-öffentliche Stellen gilt dieses Gesetz für die ganz oder teilweise automatisierte Verarbeitung personenbezogener Daten sowie die nichtautomatisierte Verarbeitung personenbezogener Daten, die in einem Datei-

system gespeichert sind oder gespeichert werden sollen, es sei denn, die Verarbeitung durch natürliche Personen erfolgt zur Ausübung ausschliesslich persönlicher oder familiärer Tätigkeiten.

2) Spezifische Bestimmungen über den Datenschutz gehen den Vorschriften dieses Gesetzes vor. Regeln sie einen Sachverhalt, für den dieses Gesetz gilt, nicht oder nicht abschliessend, finden die Vorschriften dieses Gesetzes Anwendung. Die Verpflichtung zur Wahrung gesetzlicher Geheimhaltungspflichten oder von Berufs- oder besonderen Amtsgeheimnissen, die nicht auf gesetzlichen Vorschriften beruhen, bleibt unberührt.

3) In Verwaltungsverfahren vor öffentlichen Stellen gehen die Vorschriften dieses Gesetzes denen des Gesetzes über die allgemeine Landesverwaltungspflege vor, soweit bei der Ermittlung des Sachverhalts personenbezogene Daten verarbeitet werden.

4) Dieses Gesetz findet Anwendung auf öffentliche Stellen. Auf nichtöffentliche Stellen findet es Anwendung, sofern

1. der Verantwortliche oder Auftragsverarbeiter personenbezogen Daten im Inland verarbeitet,
2. die Verarbeitung personenbezogener Daten im Rahmen der Tätigkeiten einer inländischen Niederlassung des Verantwortlichen oder Auftragsverarbeiters erfolgt oder
3. der Verantwortliche oder Auftragsverarbeiter zwar keine Niederlassung in einem EWR-Mitgliedstaat hat, er aber in den Anwendungsbereich der Verordnung (EU) 2016/679 fällt.

Sofern dieses Gesetz nicht gemäss Satz 2 Anwendung findet, gelten für den Verantwortlichen oder Auftragsverarbeiter nur Art. 8 bis 19, 35 bis 39.

5) Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten, finden die Verordnung (EU) 2016/679 und die Teile 1 und 2 dieses Gesetzes entsprechend Anwendung, soweit nicht in diesem Gesetz oder einem anderen Gesetz Abweichendes geregelt ist.

Art. 2

*Begriffsbestimmungen*

1) Öffentliche Stellen sind die Organe des Staates, der Rechtspflege, der Gemeinden und von Körperschaften, Stiftungen und Anstalten des öffentlichen Rechts sowie deren Vereinigungen ungeachtet ihrer Rechtsform sowie auch Private, soweit sie in Erfüllung der ihnen übertragenen öffentlichen Aufgaben tätig sind.

2) Nicht-öffentliche Stellen sind natürliche und juristische Personen, Gesellschaften und andere Personenvereinigungen des privaten Rechts, soweit sie nicht unter Abs. 1 fallen.

3) Öffentliche Stellen gelten als nicht-öffentliche Stellen im Sinne dieses Gesetzes, soweit sie als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen.

4) Wo in diesem Gesetz die männliche Form einer Personenbezeichnung verwendet wird, ist darunter auch die weibliche Form zu verstehen.

## Kapitel 2

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

### Art. 3

*Verarbeitung personenbezogener Daten durch öffentliche Stellen*

Die Verarbeitung personenbezogener Daten durch eine öffentliche Stelle ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgabe oder in Ausübung öffentlicher Gewalt, die dem Verantwortlichen übertragen wurde, erforderlich ist.

### Art. 4

*Videoüberwachung öffentlich zugänglicher Räume*

1) Die Beobachtung öffentlich zugänglicher Räume mit optisch-elektronischen Einrichtungen (Videoüberwachung) ist nur zulässig, soweit sie

1. zur Aufgabenerfüllung öffentlicher Stellen,
2. zur Wahrnehmung des Hausrechts oder
3. zur Wahrnehmung berechtigter Interessen für konkret festgelegte Zwecke erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen.

Bei der Videoüberwachung von

1. öffentlich zugänglichen grossflächigen Anlagen, wie insbesondere Sport-, Versammlungs- und Vergnügungsstätten, Einkaufszentren oder Parkplätzen, oder

2. Fahrzeugen und öffentlich zugänglichen grossflächigen Einrichtungen des öffentlichen Verkehrs

gilt der Schutz von Leben, Gesundheit oder Freiheit von dort aufhältigen Personen als ein besonders wichtiges Interesse.

2) Der Umstand der Beobachtung und der Name und die Kontaktdaten des Verantwortlichen sind durch geeignete Massnahmen zum frühestmöglichen Zeitpunkt erkennbar zu machen.

3) Die Speicherung oder Verwendung von nach Abs. 1 erhobenen Daten ist zulässig, wenn sie zum Erreichen des verfolgten Zwecks erforderlich ist und keine Anhaltspunkte bestehen, dass schutzwürdige Interessen der Betroffenen überwiegen. Abs. 1 Satz 2 gilt entsprechend. Für einen anderen Zweck dürfen sie nur weiterverarbeitet werden, soweit dies zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit, zur Abwehr einer schweren Gefahr für Leib, Leben, Freiheit oder Eigentum sowie zur Verfolgung von Straftaten oder zur Beweissicherung erforderlich ist. In den letztgenannten Fällen kann die Landespolizei die Übermittlung der erhobenen Daten verlangen.

4) Werden durch Videoüberwachung erhobene Daten einer bestimmten Person zugeordnet, so besteht die Pflicht zur Information der betroffenen Person über die Verarbeitung gemäss Art. 13 und 14 der Verordnung (EU) 2016/679. Art. 29 gilt entsprechend.

5) Die Daten sind unverzüglich zu löschen, wenn sie zur Erreichung des Zwecks nicht mehr erforderlich sind oder schutzwürdige Interessen der Betroffenen einer weiteren Speicherung entgegenstehen.

6) Der Einsatz einer Videoüberwachung muss vor der Installation durch die Datenschutzstelle bewilligt werden. Von einer Bewilligung ausgenommen sind Bildübermittlungen in Echtzeit ohne Aufzeichnungs- oder sonstige weitere Bearbeitungsmöglichkeit. Gegen die Entscheidung über die Bewilligung kann innerhalb von 14 Tagen Beschwerde bei der Beschwerdekommission für Verwaltungsangelegenheiten erhoben werden. Die Datenschutzstelle ist berechtigt, gegen den Entscheid der Beschwerdekommission Beschwerde zu erheben. Die Regierung regelt das Nähere mit Verordnung.

## Kapitel 3

### Datenschutzbeauftragte öffentlicher Stellen

#### Art. 5

*Benennung*

1) Öffentliche Stellen benennen einen Datenschutzbeauftragten. Dies gilt auch für öffentliche Stellen nach Art. 2 Abs. 3, die am Wettbewerb teilnehmen.

2) Für mehrere öffentliche Stellen kann unter Berücksichtigung ihrer Organisationsstruktur und ihrer Grösse ein gemeinsamer Datenschutzbeauftragter benannt werden.

3) Der Datenschutzbeauftragte wird auf der Grundlage seiner beruflichen Eignung benannt.

4) Der Datenschutzbeauftragte kann Beschäftigter der öffentlichen Stelle sein oder seine Aufgaben auf der Grundlage eines Dienstleistungsvertrags erfüllen.

5) Die öffentliche Stelle veröffentlicht die Kontaktdaten des Datenschutzbeauftragten und teilt diese Daten der Datenschutzstelle mit.

Art. 6

*Stellung*

1) Die öffentliche Stelle stellt sicher, dass der Datenschutzbeauftragte ordnungsgemäss und frühzeitig in alle mit dem Schutz personenbezogener Daten zusammenhängenden Fragen eingebunden wird.

2) Die öffentliche Stelle unterstützt den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben gemäss Art. 7, indem sie die für die Erfüllung dieser Aufgaben erforderlichen Ressourcen und den Zugang zu personenbezogenen Daten und Verarbeitungsvorgängen sowie die zur Erhaltung seines Fachwissens erforderlichen Ressourcen zur Verfügung stellt.

3) Die öffentliche Stelle stellt sicher, dass der Datenschutzbeauftragte bei der Erfüllung seiner Aufgaben keine Anweisungen bezüglich der Ausübung dieser Aufgaben erhält. Der Datenschutzbeauftragte berichtet unmittelbar der Leitung der öffentlichen Stelle. Der Datenschutzbeauftragte darf von der öffentlichen Stelle wegen der Erfüllung seiner Aufgaben nicht abberufen oder benachteiligt werden.

4) Die Abberufung des Datenschutzbeauftragten ist nur in entsprechender Anwendung des Art. 24 StPG zulässig.

5) Betroffene Personen können den Datenschutzbeauftragten zu allen mit der Verarbeitung ihrer personenbezogenen Daten und mit der Wahrnehmung ihrer Rechte gemäss der Verordnung (EU) 2016/679, diesem Gesetz sowie anderen Rechtsvorschriften über den Datenschutz im Zusammenhang stehenden Fragen zu Rate ziehen. Der Datenschutzbeauftragte ist zur Verschwiegenheit über die Identität der betroffenen Person sowie über Umstände, die Rückschlüsse auf die betroffene Person zulassen, verpflichtet, soweit sie oder er nicht davon durch die betroffene Person befreit wird.

6) Wenn der Datenschutzbeauftragte bei seiner Tätigkeit Kenntnis von Daten erhält, für die der Leitung oder einer bei der öffentlichen Stelle beschäftigten Person aus beruflichen Gründen ein Zeugnisverweigerungsrecht zusteht, steht dieses Recht auch dem Datenschutzbeauftragten und den ihm unterstellten Beschäftigten zu. Über die Ausübung dieses Rechts entscheidet die Person, der das Zeugnisverweigerungsrecht aus beruflichen Gründen zusteht, es sei denn, dass diese Entscheidung in absehbarer Zeit nicht herbeigeführt werden kann. Soweit das Zeugnisverweigerungsrecht des Datenschutzbeauftragten reicht, unterliegen seine Akten und andere Dokumente einem Beschlagnahmeverbot.

Art. 7

*Aufgaben*

1) Dem Datenschutzbeauftragten obliegen neben den in der Verordnung (EU) 2016/679 genannten Aufgaben zumindest folgende Aufgaben:

1. Unterrichtung und Beratung der öffentlichen Stelle und der Beschäftigten, die Verarbeitungen durchführen, hinsichtlich ihrer Pflichten nach diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschliesslich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften;

2. Überwachung der Einhaltung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschliesslich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, sowie der Strategien der öffentlichen Stelle für den Schutz personenbezogener Daten, einschliesslich der Zuweisung von Zuständigkeiten, der Sensibilisierung und der Schulung der an den Verarbeitungsvorgängen beteiligten Beschäftigten und der diesbezüglichen Überprüfungen;
3. Beratung im Zusammenhang mit der Datenschutz-Folgenabschätzung und Überwachung ihrer Durchführung gemäss Art. 62;
4. Zusammenarbeit mit der Aufsichtsbehörde;
5. Tätigkeit als Anlaufstelle für die Aufsichtsbehörde in mit der Verarbeitung zusammenhängenden Fragen, einschliesslich der vorherigen Konsultation gemäss Art. 64, und gegebenenfalls Beratung zu allen sonstigen Fragen.

   Im Fall einer oder eines bei einem Gericht bestellten Datenschutzbeauftragten beziehen sich diese Aufgaben nicht auf das Handeln des Gerichts im Rahmen seiner justiziellen Tätigkeit.

2) Der Datenschutzbeauftragte kann andere Aufgaben und Pflichten wahrnehmen. Die öffentliche Stelle stellt sicher, dass derartige Aufgaben und Pflichten nicht zu einem Interessenkonflikt führen.

3) Der Datenschutzbeauftragte trägt bei der Erfüllung seiner Aufgaben dem mit den Verarbeitungsvorgängen verbundenen Risiko gebührend Rechnung, wobei er die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung berücksichtigt.

## Kapitel 4

## Die Datenschutzstelle

### Art. 8
*Errichtung*

1) Bei dem für den Geschäftsbereich Justiz zuständigen Ministerium wird als Aufsichtsbehörde nach Art. 51 der Verordnung (EU) 2016/679 eine Datenschutzstelle eingerichtet.

2) Die Datenschutzstelle besteht aus dem Leiter der Datenschutzstelle und dem übrigen Personal.

### Art. 9
*Zuständigkeit*

1) Die Datenschutzstelle ist zuständig für die Aufsicht über die nicht-öffentlichen Stellen und die öffentlichen Stellen, auch soweit letztere als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen. Die Vorschriften dieses Kapitels gelten auch für Auftragsverarbeiter, soweit sie nicht-öffentliche Stellen sind, bei denen dem Land die Mehrheit der Anteile gehört oder die Mehrheit der Stimmen zusteht und der Auftraggeber eine öffentliche Stelle ist.

2) Die Datenschutzstelle ist nicht zuständig für die Aufsicht über die von den Gerichten im Rahmen ihrer justiziellen Tätigkeit vorgenommenen Verarbeitungen.

Art. 10

*Unabhängigkeit*

1) Die Datenschutzstelle handelt bei der Erfüllung ihrer Aufgaben und bei der Ausübung ihrer Befugnisse völlig unabhängig. Sie unterliegt weder direkter noch indirekter Beeinflussung von aussen und ersucht weder um Weisung noch nimmt sie Weisungen entgegen.

2) Die Datenschutzstelle unterliegt der Prüfung durch die Finanzkontrolle nach Finanzkontrollgesetz, wobei die Prüfung der gesetzlichen Aufgaben der Datenschutzstelle ausgenommen ist.

Art. 11

*Wahl und Amtszeit des Leiters der Datenschutzstelle*

1) Die Regierung wählt den Leiter der Datenschutzstelle für eine Amtszeit von acht Jahren. Die Wiederwahl ist möglich.

2) Der Leiter der Datenschutzstelle muss über die für die Erfüllung seiner Aufgaben und Ausübung seiner Befugnisse erforderliche persönliche und fachliche Eignung verfügen.

Art. 12

*Dienstverhältnis*

1) Der Leiter der Datenschutzstelle und das übrige Personal der Datenschutzstelle sind Staatspersonal. Soweit sich aus der Verordnung (EU) 2016/679 oder diesem Gesetz nicht etwas anderes ergibt, findet das Staatspersonalgesetz sinngemäss Anwendung.

2) Der Leiter der Datenschutzstelle kann nur seines Amtes enthoben werden, wenn er eine schwere Verfehlung begangen hat oder die Voraussetzungen für die Wahrnehmung seiner Aufgaben nicht mehr erfüllt sind.

3) Endet das Dienstverhältnis mit Ablauf der Amtszeit, so kann die Regierung in begründeten Fällen das Dienstverhältnis bis zur Wahl eines Nachfolgers um bis zu sechs Monate erstrecken.

4) Das übrige Personal der Datenschutzstelle wird auf Vorschlag des Leiters der Datenschutzstelle von der Regierung angestellt.

Art. 13

*Rechte und Pflichten*

1) Der Leiter der Datenschutzstelle sieht von allen mit den Aufgaben seines Amtes nicht zu vereinbarenden Handlungen ab und übt während seiner Amtszeit keine andere mit seinem Amt nicht zu vereinbarende entgeltliche oder unentgeltliche Tätigkeit aus. Insbesondere darf der Leiter der Datenschutzstelle neben seinem Amt kein anderes besoldetes Amt, kein Gewerbe und keinen Beruf ausüben und weder der Leitung oder dem Aufsichtsrat oder Verwaltungsrat eines auf Erwerb gerichteten Unternehmens, noch einem Gericht, der Regierung, einem Gemeinderat oder dem Landtag angehören. Er darf nicht gegen Entgelt aussergerichtliche Gutachten abgeben.

2) Der Leiter der Datenschutzstelle hat dem für den Geschäftsbereich Justiz zuständigen Minister Mitteilung über Geschenke zu machen, die er in Bezug auf das Amt erhält.

3) Der Leiter der Datenschutzstelle ist berechtigt, über Personen, die ihm in seiner Eigenschaft als Leiter der Datenschutzstelle Tatsachen anvertraut haben,

sowie über diese Tatsachen selbst das Zeugnis zu verweigern. Dies gilt auch für das übrige Personal der Datenschutzstelle mit der Massgabe, dass über die Ausübung dieses Rechts der Leiter der Datenschutzstelle entscheidet. Soweit das Zeugnisverweigerungsrecht des Leiters der Datenschutzstelle reicht, darf die Vorlegung oder Auslieferung von Akten oder anderen Dokumenten von ihm nicht gefordert werden.

4) Der Leiter der Datenschutzstelle ist, auch nach Beendigung seines Dienstverhältnisses, verpflichtet, über die ihm dienstlich bekanntgewordenen Angelegenheiten Verschwiegenheit zu bewahren. Dies gilt nicht für Mitteilungen im dienstlichen Verkehr oder über Tatsachen, die offenkundig sind oder ihrer Bedeutung nach keiner Geheimhaltung bedürfen. Der Leiter der Datenschutzstelle entscheidet nach pflichtgemässem Ermessen, ob und inwieweit er über solche Angelegenheiten vor Gericht oder aussergerichtlich aussagt oder Erklärungen abgibt; wenn er nicht mehr im Amt ist, ist die Genehmigung des amtierenden Leiters der Datenschutzstelle erforderlich. Unberührt bleibt die gesetzlich begründete Pflicht Straftaten anzuzeigen.

5) Für den Leiter der Datenschutzstelle und das übrige Personal der Datenschutzstelle gelten die Art. 84 und 85 des Steuergesetzes nicht. Dies gilt nicht, soweit die Steuerbehörden die Kenntnis für die Durchführung eines Verfahrens wegen einer Steuerstraftat sowie eines damit zusammenhängenden Steuerverfahrens benötigen, an deren Verfolgung ein zwingendes öffentliches Interesse besteht, oder soweit es sich um vorsätzlich falsche Angaben des Auskunftspflichtigen oder der für ihn tätigen Personen handelt. Stellt die Datenschutzstelle einen Datenschutzverstoss fest, ist sie befugt, diesen anzuzeigen und die betroffene Person hierüber zu informieren.

6) Der Leiter der Datenschutzstelle darf als Zeuge aussagen, es sei denn, die Aussage würde

1. dem Wohl des Landes Nachteile bereiten, insbesondere Nachteile für die Sicherheit oder der Beziehungen zu anderen Staaten, oder
2. Grundrechte verletzen.

Betrifft die Aussage laufende oder abgeschlossene Vorgänge, die dem Kernbereich exekutiver Eigenverantwortung der Regierung zuzurechnen sind oder sein könnten, darf der Leiter der Datenschutzstelle nur in Abstimmung mit der Regierung aussagen. Diese darf die Genehmigung nur verweigern, wenn es das Wohl des Landes erfordert.

7) Der Leiter der Datenschutzstelle erlässt ein Organisationsreglement, das von der Regierung zu genehmigen ist.

Art. 14

*Aufgaben*

1) Die Datenschutzstelle hat neben den in der Verordnung (EU) 2016/679 genannten Aufgaben zusätzlich die folgenden Aufgaben:

1. die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschliesslich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu überwachen und durchzusetzen;
2. die Öffentlichkeit für die Risiken, Vorschriften, Garantien und Rechte im Zusammenhang mit der Verarbeitung personenbezogener Daten zu sensibilisieren und sie darüber aufzuklären, wobei spezifische Massnahmen für Kinder besondere Beachtung finden;

3. den Landtag, die Regierung und andere Einrichtungen und Gremien über legislative und administrative Massnahmen zum Schutz der Rechte und Freiheiten natürlicher Personen in Bezug auf die Verarbeitung personenbezogener Daten zu beraten;

4. die Verantwortlichen und die Auftragsverarbeiter für die ihnen aus diesem Gesetz und sonstigen Vorschriften über den Datenschutz, einschliesslich den zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, entstehenden Pflichten zu sensibilisieren;

5. auf Anfrage jeder betroffenen Person Informationen über die Ausübung ihrer Rechte aufgrund dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschliesslich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zur Verfügung zu stellen und gegebenenfalls zu diesem Zweck mit den Aufsichtsbehörden in anderen Mitgliedstaaten zusammenzuarbeiten;

6. sich mit Beschwerden einer betroffenen Person oder Beschwerden einer Stelle, einer Organisation oder eines Verbandes gemäss Art. 55 der Richtlinie (EU) 2016/680 zu befassen, den Gegenstand der Beschwerde in angemessenem Umfang zu untersuchen und den Beschwerdeführer innerhalb einer angemessenen Frist über den Fortgang und das Ergebnis der Untersuchung zu unterrichten, insbesondere, wenn eine weitere Untersuchung oder Koordinierung mit einer anderen Aufsichtsbehörde notwendig ist;

7. mit anderen Aufsichtsbehörden zusammenzuarbeiten, auch durch Informationsaustausch, und ihnen Amtshilfe zu leisten, um die einheitliche Anwendung und Durchsetzung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschliesslich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, zu gewährleisten;

8. Untersuchungen über die Anwendung dieses Gesetzes und sonstiger Vorschriften über den Datenschutz, einschliesslich der zur Umsetzung der Richtlinie (EU) 2016/680 erlassenen Rechtsvorschriften, durchzuführen, auch auf der Grundlage von Informationen einer anderen Aufsichtsbehörde oder einer anderen Behörde;

9. massgebliche Entwicklungen zu verfolgen, soweit sie sich auf den Schutz personenbezogener Daten auswirken, insbesondere die Entwicklung der Informations- und Kommunikationstechnologie und der Geschäftspraktiken;

10. Beratung in Bezug auf die in Art. 64 genannten Verarbeitungsvorgänge zu leisten und

11. Beiträge zur Tätigkeit des Europäischen Datenschutzausschusses zu leisten.

Im Anwendungsbereich der Richtlinie (EU) 2016/680 nimmt die Datenschutzstelle zudem die Aufgabe nach Art. 55 wahr.

2) Zur Erfüllung der in Abs. 1 Ziff. 3 genannten Aufgabe kann die Datenschutzstelle zu allen Fragen, die im Zusammenhang mit dem Schutz personenbezogener Daten stehen, von sich aus oder auf Anfrage Stellungnahmen an den Landtag oder einer seiner Kommissionen, die Regierung, sonstige Einrichtungen und Stellen richten. Auf Ersuchen des Landtags, einer seiner Kommissionen oder der Regierung geht die Datenschutzstelle ferner Hinweisen auf Angelegenheiten und Vorgänge des Datenschutzes bei den öffentlichen Stellen nach.

3) Die Datenschutzstelle erleichtert das Einreichen der in Abs. 1 Satz 1 Ziff. 6 genannten Beschwerden durch Massnahmen wie etwa die Bereitstellung eines Beschwerdeformulars, das auch elektronisch ausgefüllt werden kann, ohne dass andere Kommunikationsmittel ausgeschlossen werden.

4) Die Erfüllung der Aufgaben der Datenschutzstelle ist für die betroffene Person unentgeltlich. Bei offenkundig unbegründeten oder, insbesondere im Fall von häufiger Wiederholung, exzessiven Anfragen kann die Datenschutzstelle eine angemessene Gebühr auf der Grundlage des Aufwands verlangen oder sich weigern, aufgrund der Anfrage tätig zu werden. In diesem Fall trägt die Datenschutzstelle die Beweislast für den offenkundig unbegründeten oder exzessiven Charakter der Anfrage.

Art. 15

*Tätigkeitsbericht*

Die Datenschutzstelle erstellt einen Jahresbericht über ihre Tätigkeit, der eine Liste der Arten der gemeldeten Verstösse und der Arten der getroffenen Massnahmen, einschliesslich der verhängten Sanktionen und der Massnahmen nach Art. 58 Abs. 2 der Verordnung (EU) 2016/679, enthalten kann. Sie übermittelt den Bericht dem Landtag und der Regierung und macht ihn der Öffentlichkeit zugänglich.

Art. 16

*Befugnisse*

1) Die Datenschutzstelle nimmt im Anwendungsbereich der Verordnung (EU) 2016/679 die Befugnisse gemäss Art. 58 der Verordnung (EU) 2016/679 wahr. Kommt die Datenschutzstelle zu dem Ergebnis, dass Verstösse gegen die Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung personenbezogener Daten vorliegen, teilt sie dies der zuständigen Rechts- oder Fachaufsichtsbehörde mit und gibt dieser vor der Ausübung der Befugnisse des Art. 58 Abs. 2 Bst. b bis g, i und j Verordnung (EU) 2016/679 gegenüber der verantwortlichen nicht-öffentlichen oder öffentlichen Stelle Gelegenheit zur Stel-

lungnahme innerhalb einer angemessenen Frist. Von der Einräumung der Gelegenheit zur Stellungnahme kann abgesehen werden, wenn eine sofortige Entscheidung wegen Gefahr im Verzug oder im öffentlichen Interesse notwendig erscheint oder ihr ein zwingendes öffentliches Interesse entgegensteht. Die Stellungnahme soll auch eine Darstellung der Massnahmen enthalten, die aufgrund der Mitteilung der Datenschutzstelle getroffen worden sind.

2) Stellt die Datenschutzstelle bei Datenverarbeitungen durch nicht-öffentliche oder öffentliche Stellen zu Zwecken ausserhalb des Anwendungsbereichs der Verordnung (EU) 2016/679 Verstösse gegen die Vorschriften dieses Gesetzes oder gegen andere Vorschriften über den Datenschutz oder sonstige Mängel bei der Verarbeitung oder Nutzung personenbezogener Daten fest, so beanstandet sie dies gegenüber der verantwortlichen nicht-öffentlichen oder öffentlichen Stelle. Im Fall einer öffentlichen Stelle informiert sie zusätzlich die Regierung über die Beanstandung. Sie gibt der zuständigen nicht-öffentlichen oder öffentlichen Stelle Gelegenheit zu einer Stellungnahme innerhalb einer von ihr zu bestimmenden angemessenen Frist. Im Fall einer öffentlichen Stelle gibt sie ebenso der Regierung Gelegenheit zu einer Stellungnahme. Die Datenschutzstelle kann von einer Beanstandung absehen oder auf eine Stellungnahme verzichten, insbesondere wenn es sich um unerhebliche oder inzwischen beseitigte Mängel handelt. Die Stellungnahme soll auch eine Darstellung der Massnahmen enthalten, die aufgrund der Beanstandung der Datenschutzstelle getroffen worden sind. Die Datenschutzstelle kann den Verantwortlichen auch davor warnen, dass beabsichtigte Verarbeitungsvorgänge voraussichtlich gegen in diesem Gesetz enthaltene und andere auf die jeweilige Datenverarbeitung anzuwendende Vorschriften über den Datenschutz verstossen.

3) Die Befugnisse der Datenschutzstelle erstrecken sich auch auf

1. von nicht-öffentlichen oder öffentlichen Stellen erlangte personenbezogene Daten über den Inhalt und die näheren Umstände des Brief-, Post- und Fernmeldeverkehrs und
2. personenbezogene Daten, die einem besonderen Amtsgeheimnis, insbesondere dem Steuergeheimnis nach Art. 83 des Steuergesetzes, unterliegen.

4) Die nicht-öffentliche oder öffentlichen Stellen sind verpflichtet, der Datenschutzstelle und den von ihr mit der Überwachung der Einhaltung der Vorschriften über den Datenschutz beauftragten Personen

1. jederzeit Zugang zu den Grundstücken und Räumen, einschliesslich aller Datenverarbeitungsanlagen und -geräte, sowie zu allen personenbezogenen Daten und Informationen, die zur Erfüllung ihrer Aufgaben notwendig sind, zu gewähren und
2. alle Informationen, die für die Erfüllung ihrer Aufgaben erforderlich sind, bereitzustellen. Im Fall nicht-öffentlicher Stellen kann der Informationspflichtige die Information verweigern, wenn deren Bereitstellung ihn selbst oder einen der in § 321 Abs. 1 Ziff. 1 der Zivilprozessordnung bezeichneten Angehörigen der Gefahr strafgerichtlicher Verfolgung aussetzen würde. Der Informationspflichtige ist darauf hinzuweisen.

5) Die Datenschutzstelle berät und unterstützt die Datenschutzbeauftragten mit Rücksicht auf deren typische Bedürfnisse. Sie kann die Abberufung des Datenschutzbeauftragten verlangen, wenn er die zur Erfüllung seiner Aufgaben erforderliche Fachkunde nicht besitzt oder im Fall des Art. 38 Abs. 6 der Verordnung (EU) 2016/679 ein schwerwiegender Interessenkonflikt vorliegt.

6) Die Datenschutzstelle darf die von ihr gespeicherten Daten nur für Zwecke der Aufsicht verarbeiten; hierbei darf sie Daten an andere Aufsichtsbehörden übermitteln. Eine Verarbeitung zu einem anderen Zweck ist über Art. 6 Abs. 4 der Verordnung (EU) 2016/679 hinaus zulässig, wenn

1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde,

2. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit oder zur Wahrung erheblicher Belange des Gemeinwohls erforderlich ist oder

3. sie zur Verfolgung von Straftaten oder Verwaltungsstraftaten, zur Vollstreckung oder zum Vollzug von Strafen oder Massnahmen des Strafgesetzbuchs oder von Erziehungsmassnahmen oder weitere Massnahmen im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbussen erforderlich ist.

   Stellt die Datenschutzstelle einen Verstoss gegen die Vorschriften über den Datenschutz fest, so ist sie befugt, die betroffenen Personen hierüber zu unterrichten und den Verstoss anderen für die Verfolgung oder Ahndung zuständigen Stellen anzuzeigen. Art. 13 Abs. 4 letzter Satz und Abs. 5 gilt entsprechend.

## Kapitel 5

### Vertretung im Europäischen Datenschutzausschuss, Zusammenarbeit mit anderen Aufsichtsbehörden

#### Art. 17

*Vertretung im Europäischen Datenschutzausschuss*

Die Datenschutzstelle vertritt das Land im Europäischen Datenschutzausschuss.

#### Art. 18

*Zusammenarbeit mit anderen Aufsichtsbehörden*

Zur Ermittlung eines Standpunktes an die Aufsichtsbehörden anderer EWR-Staaten, die EFTA-Überwachungsbehörde oder den Europäischen Datenschutzausschuss beteiligt die Datenschutzstelle andere nationale Aufsichtsbehörden, sofern diese von der Angelegenheit betroffen sind.

## Kapitel 6

## Rechtsbehelfe

### Art. 19
*Rechtsschutz*

1) Für Streitigkeiten zwischen einer natürlichen oder einer juristischen Person und der Datenschutzstelle über Rechte gemäss Art. 78 Abs. 1 und 2 der Verordnung (EU) 2016/679 sowie Art. 56 ist der Verwaltungsrechtsweg gegeben.

2) Gegen Entscheidungen und Verfügungen der Datenschutzstelle kann binnen 14 Tagen ab Zustellung Beschwerde bei der Verwaltungsbeschwerdekommission erhoben werden.

3) Gegen Entscheidungen und Verfügungen der Verwaltungsbeschwerdekommission kann binnen 14 Tagen ab Zustellung Beschwerde beim Verwaltungsgerichtshof erhoben werden.

4) Die Datenschutzstelle kann gegen ergangene Entscheidungen und Verfügungen der Verwaltungsbeschwerdekommission oder des Verwaltungsgerichtshofs die zulässigen ordentlichen oder ausserordentlichen Rechtsmittel ergreifen.

5) Die Datenschutzstelle darf Entscheidungen und Verfügungen gegenüber einer Behörde oder deren Rechtsträger die aufschiebende Wirkung nicht entziehen.

## Teil 2

## Durchführungsbestimmungen für Verarbeitungen zu Zwecken gemäss Art. 2 der Verordnung (EU) 2016/679

### Kapitel 1

Rechtsgrundlagen der Verarbeitung personenbezogener Daten

### Abschnitt 1

Verarbeitung besonderer Kategorien personenbezogener Daten und Verarbeitung zu anderen Zwecken

Art. 20

*Verarbeitung besonderer Kategorien personenbezogener Daten*

1) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 zulässig

1. durch öffentliche und nicht-öffentliche Stellen, wenn sie

   a) erforderlich ist, um die aus dem Recht der sozialen Sicherheit und des Sozialschutzes erwachsenden Rechte auszuüben und den diesbezüglichen Pflichten nachzukommen;

   b) zum Zweck der Gesundheitsvorsorge, für die Beurteilung der Arbeitsfähigkeit des Beschäftigten, für die medizinische Diagnostik, die Ver-

sorgung oder Behandlung im Gesundheits- oder Sozialbereich oder für die Verwaltung von Systemen und Diensten im Gesundheits- und Sozialbereich oder aufgrund eines Vertrags der betroffenen Person mit einem Angehörigen eines Gesundheitsberufs erforderlich ist und diese Daten von ärztlichem Personal oder durch sonstige Personen, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder unter deren Verantwortung verarbeitet werden; oder

c) aus Gründen des öffentlichen Interesses im Bereich der öffentlichen Gesundheit, wie des Schutzes vor schwerwiegenden grenzüberschreitenden Gesundheitsgefahren oder zur Gewährleistung hoher Qualitäts- und Sicherheitsstandards bei der Gesundheitsversorgung und bei Arzneimitteln und Medizinprodukten erforderlich ist; ergänzend zu den in Abs. 2 genannten Massnahmen sind insbesondere die berufsrechtlichen und strafrechtlichen Vorgaben zur Wahrung des Berufsgeheimnisses einzuhalten;,

2. durch öffentliche Stellen, wenn sie

a) aus Gründen eines erheblichen öffentlichen Interesses zwingend erforderlich ist;

b) zur Abwehr einer erheblichen Gefahr für die öffentliche Sicherheit erforderlich ist;

c) zur Abwehr erheblicher Nachteile für das Gemeinwohl oder zur Wahrung erheblicher Belange des Gemeinwohls zwingend erforderlich ist oder

d) aus zwingenden Gründen der Verteidigung oder der Erfüllung über- oder zwischenstaatlicher Verpflichtungen einer öffentlichen Stelle des Landes auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Massnahmen erforderlich ist

und soweit die Interessen des Verantwortlichen an der Datenverarbeitung in den Fällen der Ziff. 2 die Interessen der betroffenen Person überwiegen.

2) In den Fällen des Abs. 1 sind angemessene und spezifische Massnahmen zur Wahrung der Interessen der betroffenen Person vorzusehen. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen können dazu insbesondere gehören:

1. technisch organisatorische Massnahmen, um sicherzustellen, dass die Verarbeitung gemäss der Verordnung (EU) 2016/679 erfolgt;
2. Massnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten eingegeben, verändert oder entfernt worden sind;
3. Sensibilisierung der an Verarbeitungsvorgängen Beteiligten;
4. Benennung einer oder eines Datenschutzbeauftragten;
5. Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle und von Auftragsverarbeitern;
6. Pseudonymisierung personenbezogener Daten;
7. Verschlüsselung personenbezogener Daten;
8. Sicherstellung der Fähigkeit, Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung personenbezogener Daten, einschliesslich der Fähigkeit, die Verfügbarkeit und den Zugang bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen;

9. zur Gewährleistung der Sicherheit der Verarbeitung die Einrichtung eines Verfahrens zur regelmässigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Massnahmen oder

10. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Einhaltung der Vorgaben dieses Gesetzes sowie der Verordnung (EU) 2016/679 sicherstellen.

Art. 21

*Verarbeitung zu anderen Zwecken durch öffentliche Stellen*

1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch öffentliche Stellen im Rahmen ihrer Aufgabenerfüllung ist zulässig, wenn

1. offensichtlich ist, dass sie im Interesse der betroffenen Person liegt und kein Grund zu der Annahme besteht, dass sie in Kenntnis des anderen Zwecks ihre Einwilligung verweigern würde;

2. Angaben der betroffenen Person überprüft werden müssen, weil tatsächliche Anhaltspunkte für deren Unrichtigkeit bestehen;

3. sie zur Abwehr erheblicher Nachteile für das Gemeinwohl oder einer Gefahr für die öffentliche Sicherheit, die Verteidigung oder die nationale Sicherheit, zur Wahrung erheblicher Belange des Gemeinwohls oder zur Sicherung des Steuer- und Zollaufkommens erforderlich ist;

4. sie zur Verfolgung von Straftaten oder Verwaltungsstraftaten, zur Vollstreckung oder zum Vollzug von Strafen oder Massnahmen des Strafgesetzbuchs oder von Erziehungsmassnahmen oder weiteren Massnahmen im Sinne des Jugendgerichtsgesetzes oder zur Vollstreckung von Geldbussen erforderlich ist;

5. sie zur Abwehr einer schwerwiegenden Beeinträchtigung der Rechte einer anderen Person erforderlich ist oder

6. sie der Wahrnehmung von Aufsichts- und Kontrollbefugnissen, der Rechnungsprüfung oder der Durchführung von Organisationsuntersuchungen des Verantwortlichen dient; dies gilt auch für die Verarbeitung zu Ausbildungs- und Prüfungszwecken durch den Verantwortlichen, soweit schutzwürdige Interessen der betroffenen Person dem nicht entgegenstehen.

2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Abs. 1 und ein Ausnahmetatbestand nach Art. 9 Abs. 2 der Verordnung (EU) 2016/679 oder nach Art. 20 vorliegen.

Art. 22

*Verarbeitung zu anderen Zwecken durch nicht-öffentliche Stellen*

1) Die Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, durch nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Abwehr von Gefahren für die staatliche oder öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist oder

2. sie zur Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche erforderlich ist,

sofern nicht die Interessen der betroffenen Person an dem Ausschluss der Verarbeitung überwiegen.

2) Die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 zu einem anderen Zweck als zu demjenigen, zu dem die Daten erhoben wurden, ist zulässig, wenn die Voraussetzungen des Abs. 1 und ein Ausnahmetatbestand nach Art. 9 Abs. 2 der Verordnung (EU) 2016/679 oder nach Art. 20 vorliegen.

Art. 23

*Datenübermittlungen durch öffentliche Stellen*

1) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an öffentliche Stellen ist zulässig, wenn sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle oder des Dritten, an den die Daten übermittelt werden, liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach Art. 21 zulassen würden. Der Dritte, an den die Daten übermittelt werden, darf diese nur für den Zweck verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist unter den Voraussetzungen des Art. 21 zulässig.

2) Die Übermittlung personenbezogener Daten durch öffentliche Stellen an nicht-öffentliche Stellen ist zulässig, wenn

1. sie zur Erfüllung der in der Zuständigkeit der übermittelnden Stelle liegenden Aufgaben erforderlich ist und die Voraussetzungen vorliegen, die eine Verarbeitung nach Art. 21 zulassen würden,
2. der Dritte, an den die Daten übermittelt werden, ein berechtigtes Interesse an der Kenntnis der zu übermittelnden Daten glaubhaft darlegt und die betroffene Person kein schutzwürdiges Interesse an dem Ausschluss der Übermittlung hat oder

3. es zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche erforderlich ist

und der Dritte sich gegenüber der übermittelnden öffentlichen Stelle verpflichtet hat, die Daten nur für den Zweck zu verarbeiten, zu dessen Erfüllung sie ihm übermittelt werden. Eine Verarbeitung für andere Zwecke ist zulässig, wenn eine Übermittlung nach Satz 1 zulässig wäre und die übermittelnde Stelle zugestimmt hat.

3) Die Übermittlung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 ist zulässig, wenn die Voraussetzungen des Abs. 1 oder 2 und ein Ausnahmetatbestand nach Art. 9 Abs. 2 der Verordnung (EU) 2016/679 oder nach Art. 20 vorliegen.

## Abschnitt 2

### Besondere Verarbeitungssituationen

### Art. 24
### *Datenverarbeitung für Zwecke des Beschäftigungsverhältnisses*

1) Personenbezogene Daten von Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses verarbeitet werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung oder zur Ausübung oder Erfüllung der sich aus einem Gesetz oder einem Vertrag oder einer Kollektivvereinbarung ergebenden Rechte und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist. Zur Aufdeckung von Straftaten dürfen

personenbezogene Daten von Beschäftigten nur dann verarbeitet werden, wenn zu dokumentierende tatsächliche Anhaltspunkte den Verdacht begründen, dass die betroffene Person im Beschäftigungsverhältnis eine Straftat begangen hat, die Verarbeitung zur Aufdeckung erforderlich ist und das schutzwürdige Interesse des Beschäftigten an dem Ausschluss der Verarbeitung nicht überwiegt, insbesondere Art und Ausmass im Hinblick auf den Anlass nicht unverhältnismässig sind.

2) Erfolgt die Verarbeitung personenbezogener Daten von Beschäftigten auf der Grundlage einer Einwilligung, so sind für die Beurteilung der Freiwilligkeit der Einwilligung insbesondere die im Beschäftigungsverhältnis bestehende Abhängigkeit der beschäftigten Person sowie die Umstände, unter denen die Einwilligung erteilt worden ist, zu berücksichtigen. Freiwilligkeit kann insbesondere vorliegen, wenn für die beschäftigte Person ein rechtlicher oder wirtschaftlicher Vorteil erreicht wird oder Arbeitgeber und beschäftigte Person gleichgelagerte Interessen verfolgen. Die Einwilligung bedarf der Schriftform, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Der Arbeitgeber hat die beschäftigte Person über den Zweck der Datenverarbeitung und über ihr Widerrufsrecht nach Art. 7 Abs. 3 der Verordnung (EU) 2016/679 in Textform aufzuklären.

3) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 für Zwecke des Beschäftigungsverhältnisses zulässig, wenn sie zur Ausübung von Rechten oder zur Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht, dem Recht der sozialen Sicherheit und des Sozialschutzes erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Verarbeitung überwiegt. Abs. 2 gilt auch für die Einwilligung in die Verarbeitung be-

sonderer Kategorien personenbezogener Daten; die Einwilligung muss sich dabei ausdrücklich auf diese Daten beziehen. Art. 20 Abs. 2 gilt entsprechend.

4) Die Verarbeitung personenbezogener Daten, einschliesslich besonderer Kategorien personenbezogener Daten von Beschäftigten für Zwecke des Beschäftigungsverhältnisses, ist auf der Grundlage von Kollektivvereinbarungen zulässig. Dabei haben die Verhandlungspartner Art. 88 Abs. 2 der Verordnung (EU) 2016/679 zu beachten.

5) Der Verantwortliche muss geeignete Massnahmen ergreifen, um sicherzustellen, dass insbesondere die in Art. 5 der Verordnung (EU) 2016/679 dargelegten Grundsätze für die Verarbeitung personenbezogener Daten eingehalten werden.

6) Die Rechte der Interessenvertretungen der Beschäftigten bleiben unberührt.

7) Die Abs. 1 bis 6 sind auch anzuwenden, wenn personenbezogene Daten, einschliesslich besonderer Kategorien personenbezogener Daten, von Beschäftigten verarbeitet werden, ohne dass sie in einem Dateisystem gespeichert sind oder gespeichert werden sollen.

8) Beschäftigte im Sinne dieses Gesetzes sind:

1. Arbeitnehmer, einschliesslich der Leiharbeitnehmer im Verhältnis zum Entleiher,
2. zu ihrer Berufsbildung Beschäftigte,
3. Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben sowie an Abklärungen der beruflichen Eignung oder Arbeitserprobung (Rehabilitanden),

4. in anerkannten Werkstätten für behinderte Menschen Beschäftigte,

5. Personen, die wegen ihrer wirtschaftlichen Unselbständigkeit als arbeitnehmerähnliche Personen anzusehen sind; zu diesen gehören auch die in Heimarbeit Beschäftigten und die ihnen Gleichgestellten,

6. Staatspersonal, Gemeindepersonal, Personal von Körperschaften, Stiftungen und Anstalten des öffentlichen Rechts und Richter.

Bewerber für ein Beschäftigungsverhältnis sowie Personen, deren Beschäftigungsverhältnis beendet ist, gelten als Beschäftigte.

Art. 25

*Datenverarbeitung zu wissenschaftlichen oder historischen Forschungszwecken und zu statistischen Zwecken*

1) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 auch ohne Einwilligung für wissenschaftliche oder historische Forschungszwecke oder für statistische Zwecke zulässig, wenn die Verarbeitung zu diesen Zwecken erforderlich ist und die Interessen des Verantwortlichen an der Verarbeitung die Interessen der betroffenen Person an einem Ausschluss der Verarbeitung erheblich überwiegen. Der Verantwortliche sieht angemessene und spezifische Massnahmen zur Wahrung der Interessen der betroffenen Person gemäss Art. 20 Abs. 2 Satz 2 vor.

2) Die in den Art. 15, 16, 18 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte der betroffenen Person sind insoweit beschränkt, als diese Rechte voraussichtlich die Verwirklichung der Forschungs- oder Statistikzwecke unmöglich machen oder ernsthaft beinträchtigen und die Beschränkung für die Erfüllung der Forschungs- oder Statistikzwecke notwendig ist. Das Recht auf Aus-

kunft gemäss Art. 15 der Verordnung (EU) 2016/679 besteht darüber hinaus nicht, wenn die Daten für Zwecke der wissenschaftlichen Forschung erforderlich sind und die Auskunftserteilung einen unverhältnismässigen Aufwand erfordern würde.

3) Ergänzend zu den in Art. 20 Abs. 2 genannten Massnahmen sind zu wissenschaftlichen oder historischen Forschungszwecken oder zu statistischen Zwecken verarbeitete besondere Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 zu anonymisieren, sobald dies nach dem Forschungs- oder Statistikzweck möglich ist, es sei denn, berechtigte Interessen der betroffenen Person stehen dem entgegen. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungs- oder Statistikzweck dies erfordert.

4) Der Verantwortliche darf personenbezogene Daten nur veröffentlichen, wenn die betroffene Person eingewilligt hat oder dies für die Darstellung von Forschungsergebnissen über Ereignisse der Zeitgeschichte unerlässlich ist.

Art. 26

*Datenverarbeitung zu im öffentlichen Interesse liegenden Archivzwecken*

1) Abweichend von Art. 9 Abs. 1 der Verordnung (EU) 2016/679 ist die Verarbeitung besonderer Kategorien personenbezogener Daten im Sinne des Art. 9 Abs. 1 der Verordnung (EU) 2016/679 zulässig, wenn sie für im öffentlichen Interesse liegende Archivzwecke erforderlich ist. Der Verantwortliche sieht angemessene und spezifische Massnahmen zur Wahrung der Interessen der betroffenen Person gemäss Art. 20 Abs. 2 Satz 2 vor.

2) Das Recht auf Auskunft der betroffenen Person gemäss Art. 15 der Verordnung (EU) 2016/679 besteht nicht, wenn das Archivgut nicht durch den Namen der Person erschlossen ist oder keine Angaben gemacht werden, die das Auffinden des betreffenden Archivguts mit vertretbarem Verwaltungsaufwand ermöglichen.

3) Das Recht auf Berichtigung der betroffenen Person gemäss Art. 16 der Verordnung (EU) 2016/679 besteht nicht, wenn die personenbezogenen Daten zu Archivzwecken im öffentlichen Interesse verarbeitet werden. Bestreitet die betroffene Person die Richtigkeit der personenbezogenen Daten, ist ihr die Möglichkeit einer Gegendarstellung einzuräumen. Das zuständige Archiv ist verpflichtet, die Gegendarstellung den Unterlagen hinzuzufügen.

4) Die in Art. 18 Abs. 1 Bst. a, b und d, den Art. 20 und 21 der Verordnung (EU) 2016/679 vorgesehenen Rechte bestehen nicht, soweit diese Rechte voraussichtlich die Verwirklichung der im öffentlichen Interesse liegenden Archivzwecke unmöglich machen oder ernsthaft beeinträchtigen und die Ausnahmen für die Erfüllung dieser Zwecke erforderlich sind.

Art. 27

*Rechte der betroffenen Person und aufsichtsbehördliche Befugnisse im Fall von Geheimhaltungspflichten*

1) Die Pflicht zur Information der betroffenen Person gemäss Art. 14 Abs. 1 bis 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Art. 14 Abs. 5 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht, soweit durch ihre Erfüllung Informationen offenbart würden, die ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Das Recht auf Auskunft der betroffenen Person gemäss

Art. 15 der Verordnung (EU) 2016/679 besteht nicht, soweit durch die Auskunft Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Die Pflicht zur Benachrichtigung gemäss Art. 34 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Art. 34 Abs. 3 der Verordnung (EU) 2016/679 genannten Ausnahme nicht, soweit durch die Benachrichtigung Informationen offenbart würden, die nach einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen. Abweichend von der Ausnahme nach Satz 3 ist die betroffene Person nach Art. 34 der Verordnung (EU) 2016/679 zu benachrichtigen, wenn die Interessen der betroffenen Person, insbesondere unter Berücksichtigung drohender Schäden, gegenüber dem Geheimhaltungsinteresse überwiegen.

2) Werden Daten Dritter im Zuge der Aufnahme oder im Rahmen eines Mandatsverhältnisses an einen Berufsgeheimnisträger übermittelt, so besteht die Pflicht der übermittelnden Stelle zur Information der betroffenen Person gemäss Art. 13 Abs. 3 der Verordnung (EU) 2016/679 nicht, sofern nicht das Interesse der betroffenen Person an der Informationserteilung überwiegt.

3) Gegenüber den in § 121 Abs. 1, 3 und 4 des Strafgesetzbuchs genannten Personen oder deren Auftragsverarbeitern bestehen die Untersuchungsbefugnisse der Datenschutzstelle gemäss Art. 58 Abs. 1 Bst. e und f der Verordnung (EU) 2016/679 nicht, soweit die Inanspruchnahme der Befugnisse zu einem Verstoss gegen die Geheimhaltungspflichten dieser Personen führen würde. Erlangt die Datenschutzstelle im Rahmen einer Untersuchung Kenntnis von Daten, die einer Geheimhaltungspflicht im Sinne des Satzes 1 unterliegen, gilt die Geheimhaltungspflicht auch für die Aufsichtsbehörde.

Art. 28

*Schutz des Wirtschaftsverkehrs bei Scoring und Bonitätsauskünften*

1) Die Verwendung eines Wahrscheinlichkeitswerts über ein bestimmtes zukünftiges Verhalten einer natürlichen Person zum Zweck der Entscheidung über die Begründung, Durchführung oder Beendigung eines Vertragsverhältnisses mit dieser Person (Scoring) ist nur zulässig, wenn

1. die Vorschriften des Datenschutzrechts eingehalten wurden;
2. die zur Berechnung des Wahrscheinlichkeitswerts genutzten Daten unter Zugrundelegung eines wissenschaftlich anerkannten mathematisch-statistischen Verfahrens nachweisbar für die Berechnung der Wahrscheinlichkeit des bestimmten Verhaltens erheblich sind;
3. für die Berechnung des Wahrscheinlichkeitswerts nicht ausschliesslich Anschriftendaten genutzt wurden und
4. im Fall der Nutzung von Anschriftendaten die betroffene Person vor Berechnung des Wahrscheinlichkeitswerts über die vorgesehene Nutzung dieser Daten unterrichtet worden ist; die Unterrichtung ist zu dokumentieren.

2) Die Verwendung eines von Auskunfteien ermittelten Wahrscheinlichkeitswerts über die Zahlungsfähig- und Zahlungswilligkeit einer natürlichen Person ist im Fall der Einbeziehung von Informationen über Forderungen nur zulässig, soweit die Voraussetzungen nach Abs. 1 vorliegen und nur solche Forderungen über eine geschuldete Leistung, die trotz Fälligkeit nicht erbracht worden ist, berücksichtigt werden,

1. die durch einen Exekutionstitel nach Art. 1 der Exekutionsordnung festgestellt worden sind;

2. die nach Art. 66 der Konkursordnung festgestellt und nicht vom Gemeinschuldner an der Prüfungsverhandlung bestritten worden sind;

3. die der Schuldner ausdrücklich anerkannt hat;

4. bei denen

   a) der Schuldner nach Eintritt der Fälligkeit der Forderung mindestens zweimal schriftlich gemahnt worden ist;

   b) die erste Mahnung mindestens vier Wochen zurückliegt;

   c) der Schuldner zuvor, jedoch frühestens bei der ersten Mahnung, über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist und

   d) der Schuldner die Forderung nicht bestritten hat oder

5. deren zugrunde liegendes Vertragsverhältnis aufgrund von Zahlungsrückständen fristlos gekündigt werden kann und bei denen der Schuldner zuvor über eine mögliche Berücksichtigung durch eine Auskunftei unterrichtet worden ist.

Die Zulässigkeit der Verarbeitung, einschliesslich der Ermittlung von Wahrscheinlichkeitswerten, von anderen bonitätsrelevanten Daten nach allgemeinem Datenschutzrecht bleibt unberührt.

## Kapitel 2

Rechte der betroffenen Person

### Art. 29

*Informationspflicht bei Erhebung von personenbezogenen Daten bei der betroffenen Person*

1) Die Pflicht zur Information der betroffenen Person gemäss Art. 13 Abs. 3 der Verordnung (EU) 2016/679 besteht ergänzend zu der in Art. 13 Abs. 4 der Verordnung (EU) 2016/679 genannten Ausnahme dann nicht, wenn die Erteilung der Information über die beabsichtigte Weiterverarbeitung

1. eine Weiterverarbeitung analog gespeicherter Daten betrifft, bei der sich der Verantwortliche durch die Weiterverarbeitung unmittelbar an die betroffene Person wendet, der Zweck mit dem ursprünglichen Erhebungszweck gemäss der Verordnung (EU) 2016/679 vereinbar ist, die Kommunikation mit der betroffenen Person nicht in digitaler Form erfolgt und das Interesse der betroffenen Person an der Informationserteilung nach den Umständen des Einzelfalls, insbesondere mit Blick auf den Zusammenhang, in dem die Daten erhoben wurden, als gering anzusehen ist;

2. im Fall einer öffentlichen Stelle die ordnungsgemässe Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 Bst. a bis e der Verordnung (EU) 2016/679 gefährden würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen;

3. die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Landes Nachteile bereiten würde und die Interessen des Verantwortli-

chen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen;

4. die Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche beeinträchtigen würde und die Interessen des Verantwortlichen an der Nichterteilung der Information die Interessen der betroffenen Person überwiegen oder

5. eine vertrauliche Übermittlung von Daten an öffentliche Stellen gefährden würde.

2) Unterbleibt eine Information der betroffenen Person nach Massgabe des Abs. 1, ergreift der Verantwortliche geeignete Massnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschliesslich der Bereitstellung der in Art. 13 Abs. 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat. Die Sätze 1 und 2 finden in den Fällen des Abs. 1 Ziff. 4 und 5 keine Anwendung.

3) Unterbleibt die Benachrichtigung in den Fällen des Abs. 1 wegen eines vorübergehenden Hinderungsgrundes, kommt der Verantwortliche der Informationspflicht unter Berücksichtigung der spezifischen Umstände der Verarbeitung innerhalb einer angemessenen Frist nach Fortfall des Hinderungsgrundes, spätestens jedoch innerhalb von zwei Wochen, nach.

Art. 30

*Informationspflicht, wenn die personenbezogenen Daten nicht bei der betroffenen Person erhoben wurden*

1) Die Pflicht zur Information der betroffenen Person gemäss Art. 14 Abs. 1, 2 und 4 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Art. 14 Abs. 5 der Verordnung (EU) 2016/679 und der in Art. 27 Abs. 1 Satz 1 genannten Ausnahme nicht, wenn die Erteilung der Information

1. im Fall einer öffentlichen Stelle

   a) die ordnungsgemässe Erfüllung der in der Zuständigkeit des Verantwortlichen liegenden Aufgaben im Sinne des Art. 23 Abs. 1 Bst. a bis e der Verordnung (EU) 2016/679 gefährden würde oder

   b) die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Landes Nachteile bereiten würde

   und deswegen das Interesse der betroffenen Person an der Informationserteilung zurücktreten muss,

2. im Fall einer nicht-öffentlichen Stelle

   a) die Geltendmachung, Ausübung oder Verteidigung zivilrechtlicher Ansprüche beeinträchtigen würde oder die Verarbeitung Daten aus zivilrechtlichen Verträgen beinhaltet und der Verhütung von Schäden durch Straftaten dient, sofern nicht das berechtigte Interesse der betroffenen Person an der Informationserteilung überwiegt, oder

   b) die zuständige öffentliche Stelle gegenüber dem Verantwortlichen festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohl des Landes Nachteile bereiten würde; im Fall der Datenverarbeitung für Zwecke

der Strafverfolgung bedarf es keiner Feststellung nach dem ersten Halbsatz.

2) Unterbleibt eine Information der betroffenen Person nach Massgabe des Abs. 1, ergreift der Verantwortliche geeignete Massnahmen zum Schutz der berechtigten Interessen der betroffenen Person, einschliesslich der Bereitstellung der in Art. 14 Abs. 1 und 2 der Verordnung (EU) 2016/679 genannten Informationen für die Öffentlichkeit in präziser, transparenter, verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache. Der Verantwortliche hält schriftlich fest, aus welchen Gründen er von einer Information abgesehen hat.

3) Bezieht sich die Informationserteilung auf die Übermittlung personenbezogener Daten durch öffentliche Stellen an die Landespolizei zum Zweck ihrer Tätigkeit im Rahmen des Staatsschutzes (Art. 2 Abs. 2 PolG), ist sie nur mit Zustimmung der Landespolizei zulässig.

Art. 31

*Auskunftsrecht der betroffenen Person*

1) Das Recht auf Auskunft der betroffenen Person gemäss Art. 15 der Verordnung (EU) 2016/679 besteht ergänzend zu den in Art. 25 Abs. 2, Art. 26 Abs. 2 und Art. 27 Abs. 1 Satz 2 genannten Ausnahmen nicht, wenn

1. die betroffene Person nach Art. 30 Abs. 1 Ziff. 1, 2 Bst. b oder Abs. 3 nicht zu informieren ist, oder
2. die Daten

a) nur deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsmässiger Aufbewahrungsvorschriften nicht gelöscht werden dürfen, oder

b) ausschliesslich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen

und die Auskunftserteilung einen unverhältnismässigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Massnahmen ausgeschlossen ist.

2) Die Gründe der Auskunftsverweigerung sind zu dokumentieren. Die Ablehnung der Auskunftserteilung ist gegenüber der betroffenen Person zu begründen, soweit nicht durch die Mitteilung der tatsächlichen und rechtlichen Gründe, auf die die Entscheidung gestützt wird, der mit der Auskunftsverweigerung verfolgte Zweck gefährdet würde. Die zum Zweck der Auskunftserteilung an die betroffene Person und zu deren Vorbereitung gespeicherten Daten dürfen nur für diesen Zweck sowie für Zwecke der Datenschutzkontrolle verarbeitet werden; für andere Zwecke ist die Verarbeitung nach Massgabe des Art. 18 der Verordnung (EU) 2016/679 einzuschränken.

3) Wird der betroffenen Person durch eine öffentliche Stelle des Landes keine Auskunft erteilt, so ist sie auf ihr Verlangen der Datenschutzstelle zu erteilen, soweit nicht die Regierung im Einzelfall feststellt, dass dadurch die Sicherheit des Landes gefährdet würde. Die Mitteilung der Datenschutzstelle an die betroffene Person über das Ergebnis der datenschutzrechtlichen Prüfung darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser nicht einer weitergehenden Auskunft zustimmt.

4) Das Recht der betroffenen Person auf Auskunft über personenbezogene Daten, die durch eine öffentliche Stelle weder automatisiert verarbeitet noch nicht automatisiert verarbeitet und in einem Dateisystem gespeichert werden, besteht nur, soweit die betroffene Person Angaben macht, die das Auffinden der Daten ermöglichen, und der für die Erteilung der Auskunft erforderliche Aufwand nicht ausser Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

Art. 32

*Recht auf Löschung*

1) Ist eine Löschung im Fall nicht automatisierter Datenverarbeitung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismässig hohem Aufwand möglich und ist das Interesse der betroffenen Person an der Löschung als gering anzusehen, besteht das Recht der betroffenen Person auf und die Pflicht des Verantwortlichen zur Löschung personenbezogener Daten gemäss Art. 17 Abs. 1 der Verordnung (EU) 2016/679 ergänzend zu den in Art. 17 Abs. 3 der Verordnung (EU) 2016/679 genannten Ausnahmen nicht. In diesem Fall tritt an die Stelle einer Löschung die Einschränkung der Verarbeitung gemäss Art. 18 der Verordnung (EU) 2016/679. Die Sätze 1 und 2 finden keine Anwendung, wenn die personenbezogenen Daten unrechtmässig verarbeitet wurden.

2) Ergänzend zu Art. 18 Abs. 1 Bst. b und c der Verordnung (EU) 2016/679 gilt Abs. 1 Satz 1 und 2 entsprechend im Fall des Art. 17 Abs. 1 Bst. a und d der Verordnung (EU) 2016/679, solange und soweit der Verantwortliche Grund zu der Annahme hat, dass durch eine Löschung schutzwürdige Interessen der betroffenen Person beeinträchtigt würden. Der Verantwortliche unterrichtet die betroffene Person über die Einschränkung der Verarbeitung, sofern sich die Un-

terrichtung nicht als unmöglich erweist oder einen unverhältnismässigen Aufwand erfordern würde.

3) Ergänzend zu Art. 17 Abs. 3 Bst. b der Verordnung (EU) 2016/679 gilt Abs. 1 entsprechend im Fall des Art. 17 Abs. 1 Bst. a der Verordnung (EU) 2016/679, wenn einer Löschung satzungsgemässe oder vertragliche Aufbewahrungsfristen entgegenstehen.

Art. 33

*Widerspruchsrecht*

Das Recht auf Widerspruch gemäss Art. 21 Abs. 1 der Verordnung (EU) 2016/679 gegenüber einer öffentlichen Stelle besteht nicht, soweit an der Verarbeitung ein zwingendes öffentliches Interesse besteht, das die Interessen der betroffenen Person überwiegt, oder eine Rechtsvorschrift zur Verarbeitung verpflichtet.

Art. 34

*Automatisierte Entscheidungen im Einzelfall einschliesslich Profiling*

1) Das Recht gemäss Art. 22 Abs. 1 der Verordnung (EU) 2016/679, keiner ausschliesslich auf einer automatisierten Verarbeitung beruhenden Entscheidung unterworfen zu werden, besteht über die in Art. 22 Abs. 2 Bst. a und c der Verordnung (EU) 2016/679 genannten Ausnahmen hinaus nicht, wenn die Entscheidung im Rahmen

a) der Leistungserbringung nach einem Versicherungsvertrag ergeht und

   1. die Festsetzung der Versicherungsprämie betrifft;

   2. dem Begehren der betroffenen Person stattgegeben wurde; oder

3. die Entscheidung auf der Anwendung verbindlicher Entgeltregelungen für Heilbehandlungen beruht.

b) von Art. 9a Sorgfaltspflichtgesetz ergeht;

c) des Kreditgeschäfts nach Art. 3 Abs. 3 Bst. b Bankengesetz ergeht; oder

d) einer Wertpapierdienstleistung oder Wertpapiernebendienstleistung nach Art. 3 Abs. 4 Bankengesetz bzw. Art. 3 Vermögensverwaltungsgesetz ergeht.

Mit Ausnahme von Bst. a Ziff. 2 hat Verantwortliche angemessene Massnahmen zur Wahrung der berechtigten Interessen der betroffenen Person zu treffen, wozu mindestens das Recht auf Erwirkung des Eingreifens einer Person seitens des Verantwortlichen, auf Darlegung des eigenen Standpunktes und auf Anfechtung der Entscheidung zählt; der Verantwortliche informiert die betroffene Person über diese Rechte spätestens zum Zeitpunkt der Mitteilung, aus der sich ergibt, dass dem Antrag der betroffenen Person nicht vollumfänglich stattgegeben wird oder die betroffene Person von der automatisierten Entscheidung negativ betroffen sein könnte.

2) Entscheidungen nach Abs. 1 Bst. a dürfen auf der Verarbeitung von Gesundheitsdaten im Sinne von Art. 4 Ziff. 15 der Verordnung (EU) 2016/679 beruhen. Der Verantwortliche sieht angemessene und spezifische Massnahmen zur Wahrung der Interessen der betroffenen Person vor.

## Kapitel 3

Pflichten der Verantwortlichen und Auftragsverarbeiter

### Art. 35
*Akkreditierung*

1) Die Erteilung der Befugnis, als Zertifizierungsstelle gemäss Art. 43 Abs. 1 Satz 1 der Verordnung (EU) 2016/679 tätig zu werden, erfolgt durch die Liechtensteinische Akkreditierungsstelle.

2) Die Regierung erlässt mit Verordnung Vorschriften über die Akkreditierung von Zertifizierungsverfahren und die Einführung von Datenschutzsiegeln und -prüfzeichen. Sie berücksichtigt dabei das internationale Recht und die international anerkannten technischen Normen.

## Kapitel 4

Sanktionen

### Art. 36
*Geldbussen nach der Verordnung (EU) 2016/679, Verfahrensvorschriften*

1) Mit den in Art. 83 Abs. 4 bis 6 der Verordnung (EU) 2016/679 festgelegten Bussen wird vom Landgericht wegen Übertretung bestraft, wer die ebenda festgelegten Verstösse begeht.

2) Soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, werden gegen Behörden und sonstige öffentliche Stellen keine Bussen verhängt.

3) Die Staatsanwaltschaft kann von der Verfolgung nur zurücktreten, wenn die Datenschutzstelle dazu ihr Einverständnis gibt.

Art. 37

*Strafvorschriften*

1) Mit Freiheitsstrafe bis zu drei Jahren oder mit Geldstrafe bis zu 360 Tagessätzen wird vom Landgericht bestraft, wer wissentlich nicht allgemein zugängliche personenbezogene Daten einer grossen Zahl von Personen, ohne hierzu berechtigt zu sein,

1. einem Dritten übermittelt oder
2. auf andere Art und Weise zugänglich macht

und hierbei gewerbsmässig handelt.

2) Mit Freiheitsstrafe bis zu zwei Jahren oder mit Geldstrafe bis zu 240 Tagessätzen wird vom Landgericht bestraft, wer personenbezogene Daten, die nicht allgemein zugänglich sind,

1. ohne hierzu berechtigt zu sein, verarbeitet oder
2. durch unrichtige Angaben erschleicht

und hierbei gegen Entgelt oder in der Absicht handelt, sich oder einen anderen zu bereichern oder einen anderen zu schädigen.

3) Die Tat wird nur auf Antrag verfolgt. Antragsberechtigt sind die betroffene Person, der Verantwortliche und die Datenschutzstelle.

4) Eine Meldung nach Art. 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Art. 34 Abs. 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 108 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

Art. 38

*Geldstrafen*

1) Wegen Übertretung mit Busse bis zu 60 000 Franken wird vom Landgericht bestraft, wer vorsätzlich oder fahrlässig entgegen Art. 4 Abs. 6 eine Videoüberwachung vor der Bewilligung durch die Datenschutzstelle installiert.

2) Soweit sie nicht als öffentlich-rechtliche Unternehmen am Wettbewerb teilnehmen, werden gegen Behörden und sonstige öffentliche Stellen keine Bussen verhängt.

3) Eine Meldung nach Art. 33 der Verordnung (EU) 2016/679 oder eine Benachrichtigung nach Art. 34 Abs. 1 der Verordnung (EU) 2016/679 darf in einem Strafverfahren gegen den Meldepflichtigen oder Benachrichtigenden oder seine in § 108 Abs. 1 der Strafprozessordnung bezeichneten Angehörigen nur mit Zustimmung des Meldepflichtigen oder Benachrichtigenden verwendet werden.

## Kapitel 5

Rechtsschutz

### Art. 39

*Haftung und Recht auf Schadenersatz*

1) Jede Person, der wegen eines Verstosses gegen die Verordnung (EU) 2016/679 oder gegen die Art. 1 bis 39 ein materieller oder immaterieller Schaden entstanden ist, hat Anspruch auf Schadenersatz gegen den Verantwortlichen oder gegen den Auftragsverarbeiter nach Art. 82 Verordnung (EU) 2016/679. Im Einzelnen gelten für diesen Schadenersatzanspruch die allgemeinen Bestimmungen des bürgerlichen Rechts.

2) Hat der Verantwortliche oder Auftragsverarbeiter einen Vertreter nach Art. 27 Abs. 1 der Verordnung (EU) 2016/679 benannt, gilt dieser auch als bevollmächtigt, Zustellungen in zivilgerichtlichen Verfahren entgegenzunehmen. Art. 12 Zustellgesetz bleibt unberührt.

# Teil 3

## Bestimmungen für Verarbeitungen zu Zwecken gemäss Art. 1 Abs. 1 der Richtlinie (EU) 2016/680

### Kapitel 1

Anwendungsbereich, Begriffsbestimmungen und allgemeine Grundsätze für die Verarbeitung personenbezogener Daten

Art. 40

*Anwendungsbereich*

Die Vorschriften dieses Teils gelten für die Verarbeitung personenbezogener Daten durch die für die Verhütung, Ermittlung, Aufdeckung, Verfolgung oder Ahndung von Straftaten oder Verwaltungsstraftaten zuständigen öffentlichen Stellen, soweit sie Daten zum Zweck der Erfüllung dieser Aufgaben verarbeiten. Die öffentlichen Stellen gelten dabei als Verantwortliche. Die Verhütung von Straftaten im Sinne des Satzes 1 umfasst den Schutz vor und die Abwehr von Gefahren für die öffentliche Sicherheit. Die Sätze 1 und 2 finden zudem Anwendung auf diejenigen öffentlichen Stellen, die für die Vollstreckung von Strafen, von Massnahmen des Strafgesetzbuchs, von Erziehungsmassnahmen oder weiteren Massnahmen im Sinne des Jugendgerichtsgesetzes und von Geldbussen zuständig sind. Soweit dieser Teil Vorschriften für Auftragsverarbeiter enthält, gilt er auch für diese.

Art. 41

*Begriffsbestimmungen*

Es bezeichnen die Begriffe:

1. „personenbezogene Daten“: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (betroffene Person) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser Person sind, identifiziert werden kann;

2. „Verarbeitung“: jeden mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung, die Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich, die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

3. „Einschränkung der Verarbeitung“: die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

4. „Profiling“: jede Art der automatisierten Verarbeitung personenbezogener Daten, bei der diese Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte der Arbeitsleistung, der wirtschaftlichen Lage, der Gesundheit, der persönlichen Vorlieben, der Interessen, der Zuverlässigkeit,

des Verhaltens, der Aufenthaltsorte oder der Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

5. „Pseudonymisierung“: die Verarbeitung personenbezogener Daten in einer Weise, in der die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Massnahmen unterliegen, die gewährleisten, dass die Daten keiner betroffenen Person zugewiesen werden können;

6. „Dateisystem“: jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

7. „Verantwortlicher“: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet;

8. „Auftragsverarbeiter“: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

9. „Empfänger“: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht; Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem EU/Schengen-Recht oder anderen Rechtsvorschriften personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung

dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäss den Zwecken der Verarbeitung;

10. „Verletzung des Schutzes personenbezogener Daten“: eine Verletzung der Sicherheit, die zur unbeabsichtigten oder unrechtmässigen Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von oder zum unbefugten Zugang zu personenbezogenen Daten geführt hat, die verarbeitet wurden;

11. „genetische Daten“: personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser Person liefern, insbesondere solche, die aus der Analyse einer biologischen Probe der Person gewonnen wurden;

12. „biometrische Daten“: mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, insbesondere Gesichtsbilder oder daktyloskopische Daten;

13. „Gesundheitsdaten“: personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschliesslich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

14. „besondere Kategorien personenbezogener Daten“:

    a) Daten, aus denen die rassische oder ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen,

    b) genetische Daten,

c) biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person,

d) Gesundheitsdaten und

e) Daten zum Sexualleben oder zur sexuellen Orientierung;

15. „Aufsichtsbehörde“: eine von einem EU/Schengen-Staat gemäss Art. 41 der Richtlinie (EU) 2016/680 eingerichtete unabhängige staatliche Stelle;

16. „internationale Organisation“: eine völkerrechtliche Organisation und ihre nachgeordneten Stellen sowie jede sonstige Einrichtung, die durch eine von zwei oder mehr Staaten geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde;

17. „Einwilligung“: jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist.

Art. 42

*Allgemeine Grundsätze für die Verarbeitung personenbezogener Daten*

Personenbezogene Daten müssen

1. auf rechtmässige Weise und nach Treu und Glauben verarbeitet werden;

2. für festgelegte, eindeutige und rechtmässige Zwecke erhoben und nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise verarbeitet werden;

3. dem Verarbeitungszweck entsprechen, für das Erreichen des Verarbeitungszwecks erforderlich sein und ihre Verarbeitung nicht ausser Verhältnis zu diesem Zweck stehen;

4. sachlich richtig und erforderlichenfalls auf dem neuesten Stand sein; dabei sind alle angemessenen Massnahmen zu treffen, damit personenbezogene Daten, die im Hinblick auf die Zwecke ihrer Verarbeitung unrichtig sind, unverzüglich gelöscht oder berichtigt werden;
5. nicht länger als es für die Zwecke, für die sie verarbeitet werden, erforderlich ist, in einer Form gespeichert werden, die die Identifizierung der betroffenen Personen ermöglicht, und
6. in einer Weise verarbeitet werden, die eine angemessene Sicherheit der personenbezogenen Daten gewährleistet; hierzu gehört auch ein durch geeignete technische und organisatorische Massnahmen zu gewährleistender Schutz vor unbefugter oder unrechtmässiger Verarbeitung, unbeabsichtigtem Verlust, unbeabsichtigter Zerstörung oder unbeabsichtigter Schädigung.

## Kapitel 2

### Rechtsgrundlagen der Verarbeitung personenbezogener Daten

#### Art. 43

*Verarbeitung besonderer Kategorien personenbezogener Daten*

1) Die Verarbeitung besonderer Kategorien personenbezogener Daten ist nur zulässig, wenn sie zur Aufgabenerfüllung unbedingt erforderlich ist.

2) Werden besondere Kategorien personenbezogener Daten verarbeitet, sind geeignete Garantien für die Rechtsgüter der betroffenen Personen vorzusehen. Geeignete Garantien können insbesondere sein:

1. spezifische Anforderungen an die Datensicherheit oder die Datenschutzkontrolle;
2. die Festlegung von besonderen Aussonderungsprüffristen;
3. die Sensibilisierung der an Verarbeitungsvorgängen Beteiligten;
4. die Beschränkung des Zugangs zu den personenbezogenen Daten innerhalb der verantwortlichen Stelle;
5. die von anderen Daten getrennte Verarbeitung;
6. die Pseudonymisierung personenbezogener Daten;
7. die Verschlüsselung personenbezogener Daten oder
8. spezifische Verfahrensregelungen, die im Fall einer Übermittlung oder Verarbeitung für andere Zwecke die Rechtmässigkeit der Verarbeitung sicherstellen.

Art. 44

*Verarbeitung zu anderen Zwecken*

Eine Verarbeitung personenbezogener Daten zu einem anderen Zweck als zu demjenigen, zu dem sie erhoben wurden, ist zulässig, wenn es sich bei dem anderen Zweck um einen der in Art. 40 genannten Zwecke handelt, der Verantwortliche befugt ist, Daten zu diesem Zweck zu verarbeiten, und die Verarbeitung zu diesem Zweck erforderlich und verhältnismässig ist. Die Verarbeitung personenbezogener Daten zu einem anderen, in Art. 40 nicht genannten Zweck ist zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

Art. 45

*Verarbeitung zu archivarischen, wissenschaftlichen und statistischen Zwecken*

Personenbezogene Daten dürfen im Rahmen der in Art. 40 genannten Zwecke in archivarischer, wissenschaftlicher oder statistischer Form verarbeitet werden, wenn hieran ein öffentliches Interesse besteht und geeignete Garantien für die Rechtsgüter der betroffenen Personen vorgesehen werden. Solche Garantien können in einer so zeitnah wie möglich erfolgenden Anonymisierung der personenbezogenen Daten, in Vorkehrungen gegen ihre unbefugte Kenntnisnahme durch Dritte oder in ihrer räumlich und organisatorisch von den sonstigen Fachaufgaben getrennten Verarbeitung bestehen.

Art. 46

*Einwilligung*

1) Soweit die Verarbeitung personenbezogener Daten nach einer Rechtsvorschrift auf der Grundlage einer Einwilligung erfolgen kann, muss der Verantwortliche die Einwilligung der betroffenen Person nachweisen können.

2) Erfolgt die Einwilligung der betroffenen Person durch eine schriftliche Erklärung, die noch andere Sachverhalte betrifft, muss das Ersuchen um Einwilligung in verständlicher und leicht zugänglicher Form in einer klaren und einfachen Sprache so erfolgen, dass es von den anderen Sachverhalten klar zu unterscheiden ist.

3) Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Durch den Widerruf der Einwilligung wird die Rechtmässigkeit der aufgrund der Einwilligung bis zum Widerruf erfolgten Verarbeitung nicht berührt.

Die betroffene Person ist vor Abgabe der Einwilligung hiervon in Kenntnis zu setzen.

4) Die Einwilligung ist nur wirksam, wenn sie auf der freien Entscheidung der betroffenen Person beruht. Bei der Beurteilung, ob die Einwilligung freiwillig erteilt wurde, müssen die Umstände der Erteilung berücksichtigt werden. Die betroffene Person ist auf den vorgesehenen Zweck der Verarbeitung hinzuweisen. Ist dies nach den Umständen des Einzelfalles erforderlich oder verlangt die betroffene Person dies, ist sie auch über die Folgen der Verweigerung der Einwilligung zu belehren.

5) Soweit besondere Kategorien personenbezogener Daten verarbeitet werden, muss sich die Einwilligung ausdrücklich auf diese Daten beziehen.

Art. 47

*Verarbeitung auf Weisung des Verantwortlichen*

Jede einem Verantwortlichen oder einem Auftragsverarbeiter unterstellte Person, die Zugang zu personenbezogenen Daten hat, darf diese Daten ausschliesslich auf Weisung des Verantwortlichen verarbeiten, es sei denn, dass sie nach einer Rechtsvorschrift zur Verarbeitung verpflichtet ist.

Art. 48

*Datengeheimnis*

Mit Datenverarbeitung befasste Personen dürfen personenbezogene Daten nicht unbefugt verarbeiten (Datengeheimnis). Sie sind bei der Aufnahme ihrer Tätigkeit dem Datengeheimnis zu verpflichten. Das Datengeheimnis besteht auch nach der Beendigung ihrer Tätigkeit fort.

Art. 49

*Automatisierte Einzelentscheidung*

1) Eine ausschliesslich auf einer automatischen Verarbeitung beruhende Entscheidung, die mit einer nachteiligen Rechtsfolge für die betroffene Person verbunden ist oder sie erheblich beeinträchtigt, ist nur zulässig, wenn sie in einer Rechtsvorschrift vorgesehen ist.

2) Entscheidungen nach Abs. 1 dürfen nicht auf besonderen Kategorien personenbezogener Daten beruhen, sofern nicht geeignete Massnahmen zum Schutz der Rechtsgüter sowie der berechtigten Interessen der betroffenen Personen getroffen wurden.

3) Profiling, das zur Folge hat, dass betroffene Personen auf der Grundlage von besonderen Kategorien personenbezogener Daten diskriminiert werden, ist verboten.

**Kapitel 3**

Rechte der betroffenen Person

Art. 50

*Allgemeine Informationen zu Datenverarbeitungen*

Der Verantwortliche hat in allgemeiner Form und für jedermann zugänglich Informationen zur Verfügung zu stellen über

1. die Zwecke der von ihm vorgenommenen Verarbeitungen;

2. die im Hinblick auf die Verarbeitung ihrer personenbezogenen Daten bestehenden Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung;

3. den Namen und die Kontaktdaten des Verantwortlichen und der oder des Datenschutzbeauftragten;

4. das Recht, die Datenschutzstelle anzurufen, und

5. die Erreichbarkeit der Datenschutzstelle.

Art. 51

*Benachrichtigung betroffener Personen*

1) Ist die Benachrichtigung betroffener Personen über die Verarbeitung sie betreffender personenbezogener Daten in speziellen Rechtsvorschriften, insbesondere bei verdeckten Massnahmen, vorgesehen oder angeordnet, so hat diese Benachrichtigung zumindest die folgenden Angaben zu enthalten:

1. die in Art. 50 genannten Angaben;

2. die Rechtsgrundlage der Verarbeitung;

3. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;

4. gegebenenfalls die Kategorien von Empfängern der personenbezogenen Daten sowie

5. erforderlichenfalls weitere Informationen, insbesondere, wenn die personenbezogenen Daten ohne Wissen der betroffenen Person erhoben wurden.

2) In den Fällen des Abs. 1 kann der Verantwortliche die Benachrichtigung insoweit und solange aufschieben, einschränken oder unterlassen, wie andernfalls

1. die Erfüllung der in Art. 40 genannten Aufgaben,
2. die öffentliche Sicherheit oder
3. Rechtsgüter Dritter

gefährdet würden, wenn das Interesse an der Vermeidung dieser Gefahren das Informationsinteresse der betroffenen Person überwiegt.

3) Bezieht sich die Benachrichtigung auf die Übermittlung personenbezogener Daten an die Landespolizei zum Zweck ihrer Tätigkeit im Rahmen des Staatsschutzes (Art. 2 Abs. 2 PolG), ist sie nur mit Zustimmung der Landespolizei zulässig.

4) Im Fall der Einschränkung nach Abs. 2 gilt Art. 52 Abs. 7 entsprechend.

Art. 52

*Auskunftsrecht*

1) Der Verantwortliche hat betroffenen Personen auf Antrag Auskunft darüber zu erteilen, ob er sie betreffende Daten verarbeitet. Betroffene Personen haben darüber hinaus das Recht, Informationen zu erhalten über

1. die personenbezogenen Daten, die Gegenstand der Verarbeitung sind, und die Kategorie, zu der sie gehören;
2. die verfügbaren Informationen über die Herkunft der Daten;
3. die Zwecke der Verarbeitung und deren Rechtsgrundlage;

4. die Empfänger oder die Kategorien von Empfängern, gegenüber denen die Daten offengelegt worden sind, insbesondere bei Empfängern in Drittstaaten oder bei internationalen Organisationen;
5. die für die Daten geltende Speicherdauer oder, falls dies nicht möglich ist, die Kriterien für die Festlegung dieser Dauer;
6. das Bestehen eines Rechts auf Berichtigung, Löschung oder Einschränkung der Verarbeitung der Daten durch den Verantwortlichen;
7. das Recht nach Art. 55, die Datenschutzstelle anzurufen, sowie
8. Angaben zur Erreichbarkeit der Datenschutzstelle.

2) Abs. 1 gilt nicht für personenbezogene Daten, die nur deshalb verarbeitet werden, weil sie aufgrund gesetzlicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder die ausschliesslich Zwecken der Datensicherung oder der Datenschutzkontrolle dienen, wenn die Auskunftserteilung einen unverhältnismässigen Aufwand erfordern würde und eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Massnahmen ausgeschlossen ist.

3) Von der Auskunftserteilung ist abzusehen, wenn die betroffene Person keine Angaben macht, die das Auffinden der Daten ermöglichen, und deshalb der für die Erteilung der Auskunft erforderliche Aufwand ausser Verhältnis zu dem von der betroffenen Person geltend gemachten Informationsinteresse steht.

4) Der Verantwortliche kann unter den Voraussetzungen des Art. 51 Abs. 2 von der Auskunft nach Abs. 1 Satz 1 absehen oder die Auskunftserteilung nach Abs. 1 Satz 2 teilweise oder vollständig einschränken.

5) Bezieht sich die Auskunftserteilung auf die Übermittlung personenbezogener Daten an die Landespolizei zum Zweck ihrer Tätigkeit im Rahmen des Staatsschutzes (Art. 2 Abs. 2 PolG), ist sie nur mit Zustimmung der Landespolizei zulässig.

6) Der Verantwortliche hat die betroffene Person über das Absehen von oder die Einschränkung einer Auskunft unverzüglich schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des Art. 51 Abs. 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von oder der Einschränkung der Auskunft verfolgten Zweck gefährden würde.

7) Wird die betroffene Person nach Abs. 6 über das Absehen von oder die Einschränkung der Auskunft unterrichtet, kann sie ihr Auskunftsrecht auch über die Datenschutzstelle ausüben. Der Verantwortliche hat die betroffene Person über diese Möglichkeit sowie darüber zu unterrichten, dass sie gemäss Art. 55 die Datenschutzstelle anrufen oder gerichtlichen Rechtsschutz suchen kann. Macht die betroffene Person von ihrem Recht nach Satz 1 Gebrauch, ist die Auskunft auf ihr Verlangen der Datenschutzstelle zu erteilen, soweit nicht die Regierung im Einzelfall feststellt, dass dadurch die Sicherheit des Landes gefährdet würde. Die Datenschutzstelle hat die betroffene Person zumindest darüber zu unterrichten, dass alle erforderlichen Prüfungen erfolgt sind oder eine Überprüfung durch sie stattgefunden hat. Diese Mitteilung kann die Information enthalten, ob datenschutzrechtliche Verstösse festgestellt wurden. Die Mitteilung der Datenschutzstelle an die betroffene Person darf keine Rückschlüsse auf den Erkenntnisstand des Verantwortlichen zulassen, sofern dieser keiner weitergehenden Auskunft zustimmt. Der Verantwortliche darf die Zustimmung nur insoweit und solange verweigern, wie er nach Abs. 4 von einer Auskunft absehen oder sie

einschränken könnte. Die Datenschutzstelle hat zudem die betroffene Person über ihr Recht auf gerichtlichen Rechtsschutz zu unterrichten.

8) Der Verantwortliche hat die sachlichen oder rechtlichen Gründe für die Entscheidung zu dokumentieren.

Art. 53

*Rechte auf Berichtigung und Löschung sowie Einschränkung der Verarbeitung*

1) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Berichtigung sie betreffender unrichtiger Daten zu verlangen. Insbesondere im Fall von Aussagen oder Beurteilungen betrifft die Frage der Richtigkeit nicht den Inhalt der Aussage oder Beurteilung. Wenn die Richtigkeit oder Unrichtigkeit der Daten nicht festgestellt werden kann, tritt an die Stelle der Berichtigung eine Einschränkung der Verarbeitung. In diesem Fall hat der Verantwortliche die betroffene Person zu unterrichten, bevor er die Einschränkung wieder aufhebt. Die betroffene Person kann zudem die Vervollständigung unvollständiger personenbezogener Daten verlangen, wenn dies unter Berücksichtigung der Verarbeitungszwecke angemessen ist.

2) Die betroffene Person hat das Recht, von dem Verantwortlichen unverzüglich die Löschung sie betreffender Daten zu verlangen, wenn deren Verarbeitung unzulässig ist, deren Kenntnis für die Aufgabenerfüllung nicht mehr erforderlich ist oder diese zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen.

3) Anstatt die personenbezogenen Daten zu löschen, kann der Verantwortliche deren Verarbeitung einschränken, wenn

1. Grund zu der Annahme besteht, dass eine Löschung schutzwürdige Interessen einer betroffenen Person beeinträchtigen würde,
2. die Daten zu Beweiszwecken in Verfahren, die Zwecken des Art. 40 dienen, weiter aufbewahrt werden müssen oder
3. eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismässigem Aufwand möglich ist.

In ihrer Verarbeitung nach Satz 1 eingeschränkte Daten dürfen nur zu dem Zweck verarbeitet werden, der ihrer Löschung entgegenstand.

4) Bei automatisierten Dateisystemen ist technisch sicherzustellen, dass eine Einschränkung der Verarbeitung eindeutig erkennbar ist und eine Verarbeitung für andere Zwecke nicht ohne weitere Prüfung möglich ist.

5) Hat der Verantwortliche eine Berichtigung vorgenommen, hat er einer Stelle, die ihm die personenbezogenen Daten zuvor übermittelt hat, die Berichtigung mitzuteilen. In Fällen der Berichtigung, Löschung oder Einschränkung der Verarbeitung nach den Abs. 1 bis 3 hat der Verantwortliche Empfängern, denen die Daten übermittelt wurden, diese Massnahmen mitzuteilen. Der Empfänger hat die Daten zu berichtigen, zu löschen oder ihre Verarbeitung einzuschränken.

6) Der Verantwortliche hat die betroffene Person über ein Absehen von der Berichtigung oder Löschung personenbezogener Daten oder über die an deren Stelle tretende Einschränkung der Verarbeitung schriftlich zu unterrichten. Dies gilt nicht, wenn bereits die Erteilung dieser Informationen eine Gefährdung im Sinne des Art. 51 Abs. 2 mit sich bringen würde. Die Unterrichtung nach Satz 1 ist zu begründen, es sei denn, dass die Mitteilung der Gründe den mit dem Absehen von der Unterrichtung verfolgten Zweck gefährden würde.

7) Art. 52 Abs. 7 und 8 findet entsprechende Anwendung.

Art. 54

*Verfahren für die Ausübung der Rechte der betroffenen Person*

1) Der Verantwortliche hat mit betroffenen Personen unter Verwendung einer klaren und einfachen Sprache in präziser, verständlicher und leicht zugänglicher Form zu kommunizieren. Unbeschadet besonderer Formvorschriften soll er bei der Beantwortung von Anträgen grundsätzlich die für den Antrag gewählte Form verwenden.

2) Bei Anträgen hat der Verantwortliche die betroffene Person unbeschadet des Art. 52 Abs. 6 und des Art. 53 Abs. 6 unverzüglich schriftlich darüber in Kenntnis zu setzen, wie verfahren wurde.

3) Die Erteilung von Informationen nach Art. 50, die Benachrichtigungen nach den Art. 51 und 61 und die Bearbeitung von Anträgen nach den Art. 52 und 53 erfolgen unentgeltlich. Bei offenkundig unbegründeten oder exzessiven Anträgen nach den Art. 52 und 53 kann der Verantwortliche entweder eine angemessene Gebühr verlangen oder sich weigern, aufgrund des Antrags tätig zu werden. In diesem Fall muss der Verantwortliche den offenkundig unbegründeten oder exzessiven Charakter des Antrags belegen können.

4) Hat der Verantwortliche begründete Zweifel an der Identität einer betroffenen Person, die einen Antrag nach den Art. 52 oder 53 gestellt hat, kann er von ihr zusätzliche Informationen anfordern, die zur Bestätigung ihrer Identität erforderlich sind.

Art. 55

*Anrufung der Datenschutzstelle*

1) Jede betroffene Person kann sich unbeschadet anderweitiger Rechtsbehelfe mit einer Beschwerde an die Datenschutzstelle wenden, wenn sie der Auffassung ist, bei der Verarbeitung ihrer personenbezogenen Daten durch öffentliche Stellen zu den in Art. 40 genannten Zwecken in ihren Rechten verletzt worden zu sein. Dies gilt nicht für die Verarbeitung von personenbezogenen Daten durch Gerichte, soweit diese die Daten im Rahmen ihrer justiziellen Tätigkeit verarbeitet haben. Die Datenschutzstelle hat die betroffene Person über den Stand und das Ergebnis der Beschwerde zu unterrichten und sie hierbei auf die Möglichkeit gerichtlichen Rechtsschutzes nach Art. 56 hinzuweisen.

2) Die Datenschutzstelle hat eine bei ihr oder ihm eingelegte Beschwerde über eine Verarbeitung, die in die Zuständigkeit einer Aufsichtsbehörde in einem anderen EU/Schengen-Staat fällt, unverzüglich an die zuständige Aufsichtsbehörde des anderen Staates weiterzuleiten. Sie oder er hat in diesem Fall die betroffene Person über die Weiterleitung zu unterrichten und ihr auf deren Ersuchen weitere Unterstützung zu leisten.

Art. 56

*Rechtsschutz gegen Entscheidungen der Datenschutzstelle oder bei deren Untätigkeit*

1) Jede natürliche oder juristische Person kann unbeschadet anderer Rechtsbehelfe im Verwaltungsrechtsweg gegen eine verbindliche Entscheidung der Datenschutzstelle vorgehen.

2) Abs. 1 gilt entsprechend zugunsten betroffener Personen, wenn sich die Datenschutzstelle mit einer Beschwerde nach Art. 55 nicht befasst oder die betroffene Person nicht innerhalb von drei Monaten nach Einlegung der Beschwerde über den Stand oder das Ergebnis der Beschwerde in Kenntnis gesetzt hat.

## Kapitel 4

Pflichten der Verantwortlichen und Auftragsverarbeiter

### Art. 57
*Auftragsverarbeitung*

1) Werden personenbezogene Daten im Auftrag eines Verantwortlichen durch andere Personen oder Stellen verarbeitet, hat der Verantwortliche für die Einhaltung der Vorschriften dieses Gesetzes und anderer Vorschriften über den Datenschutz zu sorgen. Die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung und Schadensersatz sind in diesem Fall gegenüber dem Verantwortlichen geltend zu machen.

2) Ein Verantwortlicher darf nur solche Auftragsverarbeiter mit der Verarbeitung personenbezogener Daten beauftragen, die mit geeigneten technischen und organisatorischen Massnahmen sicherstellen, dass die Verarbeitung im Einklang mit den gesetzlichen Anforderungen erfolgt und der Schutz der Rechte der betroffenen Personen gewährleistet wird.

3) Auftragsverarbeiter dürfen ohne vorherige schriftliche Genehmigung des Verantwortlichen keine weiteren Auftragsverarbeiter hinzuziehen. Hat der Verantwortliche dem Auftragsverarbeiter eine allgemeine Genehmigung zur Hinzu-

ziehung weiterer Auftragsverarbeiter erteilt, hat der Auftragsverarbeiter den Verantwortlichen über jede beabsichtigte Hinzuziehung oder Ersetzung zu informieren. Der Verantwortliche kann in diesem Fall die Hinzuziehung oder Ersetzung untersagen.

4) Zieht ein Auftragsverarbeiter einen weiteren Auftragsverarbeiter hinzu, so hat er diesem dieselben Verpflichtungen aus seinem Vertrag mit dem Verantwortlichen nach Abs. 5 aufzuerlegen, die auch für ihn gelten, soweit diese Pflichten für den weiteren Auftragsverarbeiter nicht schon aufgrund anderer Vorschriften verbindlich sind. Erfüllt ein weiterer Auftragsverarbeiter diese Verpflichtungen nicht, so haftet der ihn beauftragende Auftragsverarbeiter gegenüber dem Verantwortlichen für die Einhaltung der Pflichten des weiteren Auftragsverarbeiters.

5) Die Verarbeitung durch einen Auftragsverarbeiter hat auf der Grundlage eines Vertrags oder eines anderen Rechtsinstruments zu erfolgen, der oder das den Auftragsverarbeiter an den Verantwortlichen bindet und der oder das den Gegenstand, die Dauer, die Art und den Zweck der Verarbeitung, die Art der personenbezogenen Daten, die Kategorien betroffener Personen und die Rechte und Pflichten des Verantwortlichen festlegt. Der Vertrag oder das andere Rechtsinstrument haben insbesondere vorzusehen, dass der Auftragsverarbeiter

1. nur auf dokumentierte Weisung des Verantwortlichen handelt; ist der Auftragsverarbeiter der Auffassung, dass eine Weisung rechtswidrig ist, hat er den Verantwortlichen unverzüglich zu informieren;

2. gewährleistet, dass die zur Verarbeitung der personenbezogenen Daten befugten Personen zur Vertraulichkeit verpflichtet werden, soweit sie keiner angemessenen gesetzlichen Verschwiegenheitspflicht unterliegen;

3. den Verantwortlichen mit geeigneten Mitteln dabei unterstützt, die Einhaltung der Bestimmungen über die Rechte der betroffenen Person zu gewährleisten;

4. alle personenbezogenen Daten nach Abschluss der Erbringung der Verarbeitungsleistungen nach Wahl des Verantwortlichen zurückgibt oder löscht und bestehende Kopien vernichtet, wenn nicht nach einer Rechtsvorschrift eine Verpflichtung zur Speicherung der Daten besteht;

5. dem Verantwortlichen alle erforderlichen Informationen, insbesondere die gemäss Art. 71 erstellten Protokolle, zum Nachweis der Einhaltung seiner Pflichten zur Verfügung stellt;

6. Überprüfungen, die von dem Verantwortlichen oder einem von diesem beauftragten Prüfer durchgeführt werden, ermöglicht und dazu beiträgt;

7. die in den Absätzen 3 und 4 aufgeführten Bedingungen für die Inanspruchnahme der Dienste eines weiteren Auftragsverarbeiters einhält;

8. alle gemäss Art. 59 erforderlichen Massnahmen ergreift und

9. unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen den Verantwortlichen bei der Einhaltung der in den Art. 59 bis 62 und Art. 64 genannten Pflichten unterstützt.

6) Der Vertrag im Sinne des Abs. 5 ist schriftlich oder elektronisch abzufassen.

7) Ein Auftragsverarbeiter, der die Zwecke und Mittel der Verarbeitung unter Verstoss gegen diese Vorschrift bestimmt, gilt in Bezug auf diese Verarbeitung als Verantwortlicher.

Art. 58

*Gemeinsam Verantwortliche*

Legen zwei oder mehr Verantwortliche gemeinsam die Zwecke und die Mittel der Verarbeitung fest, gelten sie als gemeinsam Verantwortliche. Gemeinsam Verantwortliche haben ihre jeweiligen Aufgaben und datenschutzrechtlichen Verantwortlichkeiten in transparenter Form in einer Vereinbarung festzulegen, soweit diese nicht bereits in Rechtsvorschriften festgelegt sind. Aus der Vereinbarung muss insbesondere hervorgehen, wer welchen Informationspflichten nachzukommen hat und wie und gegenüber wem betroffene Personen ihre Rechte wahrnehmen können. Eine entsprechende Vereinbarung hindert die betroffene Person nicht, ihre Rechte gegenüber jedem der gemeinsam Verantwortlichen geltend zu machen.

Art. 59

*Anforderungen an die Sicherheit der Datenverarbeitung*

1) Der Verantwortliche und der Auftragsverarbeiter haben unter Berücksichtigung des Stands der Technik, der Implementierungskosten, der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Eintrittswahrscheinlichkeit und der Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen die erforderlichen technischen und organisatorischen Massnahmen zu treffen, um bei der Verarbeitung personenbezogener Daten ein dem Risiko angemessenes Schutzniveau zu gewährleisten, insbesondere im Hinblick auf die Verarbeitung besonderer Kategorien personenbezogener Daten. Der Verantwortliche hat hierbei die einschlägigen allgemein anerkannten technischen Richtlinien und Empfehlungen in der Informationstechnik zu berücksichtigen.

2) Die in Abs. 1 genannten Massnahmen können unter anderem die Pseudonymisierung und Verschlüsselung personenbezogener Daten umfassen, soweit solche Mittel in Anbetracht der Verarbeitungszwecke möglich sind. Die Massnahmen nach Abs. 1 sollen dazu führen, dass

1. die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sichergestellt werden und
2. die Verfügbarkeit der personenbezogenen Daten und der Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederhergestellt werden können.

3) Im Fall einer automatisierten Verarbeitung haben der Verantwortliche und der Auftragsverarbeiter nach einer Risikobewertung Massnahmen zu ergreifen, die Folgendes bezwecken:

1. Verwehrung des Zugangs zu Verarbeitungsanlagen, mit denen die Verarbeitung durchgeführt wird, für Unbefugte (Zugangskontrolle);
2. Verhinderung des unbefugten Lesens, Kopierens, Veränderns oder Löschens von Datenträgern (Datenträgerkontrolle);
3. Verhinderung der unbefugten Eingabe von personenbezogenen Daten sowie der unbefugten Kenntnisnahme, Veränderung und Löschung von gespeicherten personenbezogenen Daten (Speicherkontrolle);
4. Verhinderung der Nutzung automatisierter Verarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung durch Unbefugte (Benutzerkontrolle);
5. Gewährleistung, dass die zur Benutzung eines automatisierten Verarbeitungssystems Berechtigten ausschliesslich zu den von ihrer Zugangsberech-

tigung umfassten personenbezogenen Daten Zugang haben (Zugriffskontrolle);

6. Gewährleistung, dass überprüft und festgestellt werden kann, an welche Stellen personenbezogene Daten mit Hilfe von Einrichtungen zur Datenübertragung übermittelt oder zur Verfügung gestellt wurden oder werden können (Übertragungskontrolle);

7. Gewährleistung, dass nachträglich überprüft und festgestellt werden kann, welche personenbezogenen Daten zu welcher Zeit und von wem in automatisierte Verarbeitungssysteme eingegeben oder verändert worden sind (Eingabekontrolle);

8. Gewährleistung, dass bei der Übermittlung personenbezogener Daten sowie beim Transport von Datenträgern die Vertraulichkeit und Integrität der Daten geschützt werden (Transportkontrolle),

9. Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können (Wiederherstellbarkeit);

10. Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden (Zuverlässigkeit);

11. Gewährleistung, dass gespeicherte personenbezogene Daten nicht durch Fehlfunktionen des Systems beschädigt werden können (Datenintegrität);

12. Gewährleistung, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle);

13. Gewährleistung, dass personenbezogene Daten gegen Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle);

14. Gewährleistung, dass zu unterschiedlichen Zwecken erhobene personenbezogene Daten getrennt verarbeitet werden können (Trennbarkeit).

Ein Zweck nach Satz 1 Ziff. 2 bis 5 kann insbesondere durch die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren erreicht werden.

Art. 60

*Meldung von Verletzungen des Schutzes personenbezogener Daten an die Datenschutzstelle*

1) Der Verantwortliche hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich und möglichst innerhalb von 72 Stunden, nachdem sie ihm bekannt geworden ist, der Datenschutzstelle zu melden, es sei denn, dass die Verletzung voraussichtlich keine Gefahr für die Rechtsgüter natürlicher Personen mit sich gebracht hat. Erfolgt die Meldung an die Datenschutzstelle nicht innerhalb von 72 Stunden, so ist die Verzögerung zu begründen.

2) Ein Auftragsverarbeiter hat eine Verletzung des Schutzes personenbezogener Daten unverzüglich dem Verantwortlichen zu melden.

3) Die Meldung nach Abs. 1 hat zumindest folgende Informationen zu enthalten:

1. eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten, die, soweit möglich, Angaben zu den Kategorien und der ungefähren Anzahl der betroffenen Personen, zu den betroffenen Kategorien personenbezogener Daten und zu der ungefähren Anzahl der betroffenen personenbezogenen Datensätze zu enthalten hat;
2. den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten oder einer sonstigen Person oder Stelle, die weitere Informationen erteilen kann;

3. eine Beschreibung der wahrscheinlichen Folgen der Verletzung und

4. eine Beschreibung der von dem Verantwortlichen ergriffenen oder vorgeschlagenen Massnahmen zur Behandlung der Verletzung und der getroffenen Massnahmen zur Abmilderung ihrer möglichen nachteiligen Auswirkungen.

4) Wenn die Informationen nach Abs. 3 nicht zusammen mit der Meldung übermittelt werden können, hat der Verantwortliche sie unverzüglich nachzureichen, sobald sie ihm vorliegen.

5) Der Verantwortliche hat Verletzungen des Schutzes personenbezogener Daten zu dokumentieren. Die Dokumentation hat alle mit den Vorfällen zusammenhängenden Tatsachen, deren Auswirkungen und die ergriffenen Abhilfemassnahmen zu umfassen.

6) Soweit von einer Verletzung des Schutzes personenbezogener Daten personenbezogene Daten betroffen sind, die von einem oder an einen Verantwortlichen in einem anderen EU/Schengen-Staat übermittelt wurden, sind die in Abs. 3 genannten Informationen dem dortigen Verantwortlichen unverzüglich zu übermitteln.

7) Art. 37 Abs. 4 findet entsprechende Anwendung.

8) Weitere Pflichten des Verantwortlichen zu Benachrichtigungen über Verletzungen des Schutzes personenbezogener Daten bleiben unberührt.

Art. 61

*Benachrichtigung betroffener Personen bei Verletzungen des Schutzes personenbezogener Daten*

1) Hat eine Verletzung des Schutzes personenbezogener Daten voraussichtlich eine erhebliche Gefahr für Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche die betroffenen Personen unverzüglich über den Vorfall zu benachrichtigen.

2) Die Benachrichtigung nach Abs. 1 hat in klarer und einfacher Sprache die Art der Verletzung des Schutzes personenbezogener Daten zu beschreiben und zumindest die in Art. 60 Abs. 3 Ziff. 2 bis 4 genannten Informationen und Massnahmen zu enthalten.

3) Von der Benachrichtigung nach Abs. 1 kann abgesehen werden, wenn

1. der Verantwortliche geeignete technische und organisatorische Sicherheitsvorkehrungen getroffen hat und diese Vorkehrungen auf die von der Verletzung des Schutzes personenbezogener Daten betroffenen Daten angewandt wurden; dies gilt insbesondere für Vorkehrungen wie Verschlüsselungen, durch die die Daten für unbefugte Personen unzugänglich gemacht wurden;
2. der Verantwortliche durch im Anschluss an die Verletzung getroffene Massnahmen sichergestellt hat, dass aller Wahrscheinlichkeit nach keine erhebliche Gefahr im Sinne des Abs. 1 mehr besteht, oder
3. dies mit einem unverhältnismässigen Aufwand verbunden wäre; in diesem Fall hat stattdessen eine öffentliche Bekanntmachung oder eine ähnliche Massnahme zu erfolgen, durch die die betroffenen Personen vergleichbar wirksam informiert werden.

4) Wenn der Verantwortliche die betroffenen Personen über eine Verletzung des Schutzes personenbezogener Daten nicht benachrichtigt hat, kann die Datenschutzstelle förmlich feststellen, dass seiner Auffassung nach die in Abs. 3 genannten Voraussetzungen nicht erfüllt sind. Hierbei hat er die Wahrscheinlichkeit zu berücksichtigen, dass die Verletzung eine erhebliche Gefahr im Sinne des Abs. 1 zur Folge hat.

5) Die Benachrichtigung der betroffenen Personen nach Abs. 1 kann unter den in Art. 51 Abs. 2 genannten Voraussetzungen aufgeschoben, eingeschränkt oder unterlassen werden, soweit nicht die Interessen der betroffenen Person aufgrund der von der Verletzung ausgehenden erheblichen Gefahr im Sinne des Abs. 1 überwiegen.

6) Art. 37 Abs. 4 findet entsprechende Anwendung.

Art. 62

*Durchführung einer Datenschutz-Folgenabschätzung*

1) Hat eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich eine erhebliche Gefahr für die Rechtsgüter betroffener Personen zur Folge, so hat der Verantwortliche vorab eine Abschätzung der Folgen der vorgesehenen Verarbeitungsvorgänge für die betroffenen Personen durchzuführen.

2) Für die Untersuchung mehrerer ähnlicher Verarbeitungsvorgänge mit ähnlich hohem Gefahrenpotential kann eine gemeinsame Datenschutz-Folgenabschätzung vorgenommen werden.

3) Der Verantwortliche hat die Datenschutzstelle an der Durchführung der Folgenabschätzung zu beteiligen.

4) Die Folgenabschätzung hat den Rechten der von der Verarbeitung betroffenen Personen Rechnung zu tragen und zumindest Folgendes zu enthalten:

1. eine systematische Beschreibung der geplanten Verarbeitungsvorgänge und der Zwecke der Verarbeitung;
2. eine Bewertung der Notwendigkeit und Verhältnismässigkeit der Verarbeitungsvorgänge in Bezug auf deren Zweck;
3. eine Bewertung der Gefahren für die Rechtsgüter der betroffenen Personen und
4. die Massnahmen, mit denen bestehenden Gefahren abgeholfen werden soll, einschliesslich der Garantien, der Sicherheitsvorkehrungen und der Verfahren, durch die der Schutz personenbezogener Daten sichergestellt und die Einhaltung der gesetzlichen Vorgaben nachgewiesen werden sollen.

5) Soweit erforderlich, hat der Verantwortliche eine Überprüfung durchzuführen, ob die Verarbeitung den Massgaben folgt, die sich aus der Folgenabschätzung ergeben haben.

Art. 63

*Zusammenarbeit mit der Datenschutzstelle*

Der Verantwortliche hat mit der Datenschutzstelle bei der Erfüllung seiner Aufgaben zusammenzuarbeiten.

Art. 64

*Anhörung der Datenschutzstelle*

1) Der Verantwortliche hat vor der Inbetriebnahme von neu anzulegenden Dateisystemen die Datenschutzstelle anzuhören, wenn

1. aus einer Datenschutz-Folgenabschätzung nach Art. 62 hervorgeht, dass die Verarbeitung eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hätte, wenn der Verantwortliche keine Abhilfemassnahmen treffen würde, oder
2. die Form der Verarbeitung, insbesondere bei der Verwendung neuer Technologien, Mechanismen oder Verfahren, eine erhebliche Gefahr für die Rechtsgüter der betroffenen Personen zur Folge hat.

Die Datenschutzstelle kann eine Liste der Verarbeitungsvorgänge erstellen, die der Pflicht zur Anhörung nach Satz 1 unterliegen.

2) Die Datenschutzstelle sind im Fall des Abs. 1 vorzulegen:

1. die nach Art. 62 durchgeführte Datenschutz-Folgenabschätzung;
2. gegebenenfalls Angaben zu den jeweiligen Zuständigkeiten des Verantwortlichen, der gemeinsam Verantwortlichen und der an der Verarbeitung beteiligten Auftragsverarbeiter;
3. Angaben zu den Zwecken und Mitteln der beabsichtigten Verarbeitung;
4. Angaben zu den zum Schutz der Rechtsgüter der betroffenen Personen vorgesehenen Massnahmen und Garantien und
5. Name und Kontaktdaten der oder des Datenschutzbeauftragten.

Auf Anforderung sind ihr zudem alle sonstigen Informationen zu übermitteln, die sie benötigt, um die Rechtmässigkeit der Verarbeitung sowie insbesondere die in

Bezug auf den Schutz der personenbezogenen Daten der betroffenen Personen bestehenden Gefahren und die diesbezüglichen Garantien bewerten zu können.

3) Falls die Datenschutzstelle der Auffassung ist, dass die geplante Verarbeitung gegen gesetzliche Vorgaben verstossen würde, insbesondere weil der Verantwortliche das Risiko nicht ausreichend ermittelt oder keine ausreichenden Abhilfemassnahmen getroffen hat, kann sie dem Verantwortlichen und gegebenenfalls dem Auftragsverarbeiter innerhalb eines Zeitraums von sechs Wochen nach Einleitung der Anhörung schriftliche Empfehlungen unterbreiten, welche Massnahmen noch ergriffen werden sollten. Die Datenschutzstelle kann diese Frist um einen Monat verlängern, wenn die geplante Verarbeitung besonders komplex ist. Sie hat in diesem Fall innerhalb eines Monats nach Einleitung der Anhörung den Verantwortlichen und gegebenenfalls den Auftragsverarbeiter über die Fristverlängerung zu informieren.

4) Hat die beabsichtigte Verarbeitung erhebliche Bedeutung für die Aufgabenerfüllung des Verantwortlichen und ist sie daher besonders dringlich, kann er mit der Verarbeitung nach Beginn der Anhörung, aber vor Ablauf der in Abs. 3 Satz 1 genannten Frist beginnen. In diesem Fall sind die Empfehlungen der Datenschutzstelle im Nachhinein zu berücksichtigen und sind die Art und Weise der Verarbeitung daraufhin gegebenenfalls anzupassen.

Art. 65

*Verzeichnis von Verarbeitungstätigkeiten*

1) Der Verantwortliche hat ein Verzeichnis aller Kategorien von Verarbeitungstätigkeiten zu führen, die in seine Zuständigkeit fallen. Dieses Verzeichnis hat die folgenden Angaben zu enthalten:

1. den Namen und die Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie den Namen und die Kontaktdaten der oder des Datenschutzbeauftragten;
2. die Zwecke der Verarbeitung;
3. die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden sollen;
4. eine Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
5. gegebenenfalls die Verwendung von Profiling;
6. gegebenenfalls die Kategorien von Übermittlungen personenbezogener Daten an Stellen in einem Drittstaat oder an eine internationale Organisation;
7. Angaben über die Rechtsgrundlage der Verarbeitung;
8. die vorgesehenen Fristen für die Löschung oder die Überprüfung der Erforderlichkeit der Speicherung der verschiedenen Kategorien personenbezogener Daten und
9. eine allgemeine Beschreibung der technischen und organisatorischen Massnahmen gemäss Art. 59.

2) Der Auftragsverarbeiter hat ein Verzeichnis aller Kategorien von Verarbeitungen zu führen, die er im Auftrag eines Verantwortlichen durchführt, das Folgendes zu enthalten hat:

1. den Namen und die Kontaktdaten des Auftragsverarbeiters, jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Datenschutzbeauftragten;

2. gegebenenfalls Übermittlungen von personenbezogenen Daten an Stellen in einem Drittstaat oder an eine internationale Organisation unter Angabe des Staates oder der Organisation und
3. eine allgemeine Beschreibung der technischen und organisatorischen Massnahmen gemäss Art. 59.

3) Die in den Abs. 1 und 2 genannten Verzeichnisse sind schriftlich oder elektronisch zu führen.

4) Verantwortliche und Auftragsverarbeiter haben auf Anforderung ihre Verzeichnisse der Datenschutzstelle zur Verfügung zu stellen.

Art. 66

*Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen*

1) Der Verantwortliche hat sowohl zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung als auch zum Zeitpunkt der Verarbeitung selbst angemessene Vorkehrungen zu treffen, die geeignet sind, die Datenschutzgrundsätze wie etwa die Datensparsamkeit wirksam umzusetzen, und die sicherstellen, dass die gesetzlichen Anforderungen eingehalten und die Rechte der betroffenen Personen geschützt werden. Er hat hierbei den Stand der Technik, die Implementierungskosten und die Art, den Umfang, die Umstände und die Zwecke der Verarbeitung sowie die unterschiedliche Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Gefahren für die Rechtsgüter der betroffenen Personen zu berücksichtigen. Insbesondere sind die Verarbeitung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu verarbeiten. Personenbezogene Daten sind zum frühestmöglichen Zeitpunkt zu

anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verarbeitungszweck möglich ist.

2) Der Verantwortliche hat geeignete technische und organisatorische Massnahmen zu treffen, die sicherstellen, dass durch Voreinstellungen grundsätzlich nur solche personenbezogenen Daten verarbeitet werden können, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist. Dies betrifft die Menge der erhobenen Daten, den Umfang ihrer Verarbeitung, ihre Speicherfrist und ihre Zugänglichkeit. Die Massnahmen müssen insbesondere gewährleisten, dass die Daten durch Voreinstellungen nicht automatisiert einer unbestimmten Anzahl von Personen zugänglich gemacht werden können.

Art. 67

*Unterscheidung zwischen verschiedenen Kategorien betroffener Personen*

Der Verantwortliche hat bei der Verarbeitung personenbezogener Daten so weit wie möglich zwischen den verschiedenen Kategorien betroffener Personen zu unterscheiden. Dies betrifft insbesondere folgende Kategorien:

1. Personen, gegen die ein begründeter Verdacht besteht, dass sie eine Straftat begangen haben;
2. Personen, gegen die ein begründeter Verdacht besteht, dass sie in naher Zukunft eine Straftat begehen werden;
3. verurteilte Straftäter;
4. Opfer einer Straftat oder Personen, bei denen bestimmte Tatsachen darauf hindeuten, dass sie Opfer einer Straftat sein könnten, und
5. andere Personen wie insbesondere Zeugen, Hinweisgeber oder Personen, die mit den in den Ziff. 1 bis 4 genannten Personen in Kontakt oder Verbindung stehen.

Art. 68

*Unterscheidung zwischen Tatsachen und persönlichen Einschätzungen*

Der Verantwortliche hat bei der Verarbeitung so weit wie möglich danach zu unterscheiden, ob personenbezogene Daten auf Tatsachen oder auf persönlichen Einschätzungen beruhen. Zu diesem Zweck soll er, soweit dies im Rahmen der jeweiligen Verarbeitung möglich und angemessen ist, Beurteilungen, die auf persönlichen Einschätzungen beruhen, als solche kenntlich machen. Es muss ausserdem feststellbar sein, welche Stelle die Unterlagen führt, die der auf einer persönlichen Einschätzung beruhenden Beurteilung zugrunde liegen.

Art. 69

*Verfahren bei Übermittlungen*

1) Der Verantwortliche hat angemessene Massnahmen zu ergreifen, um zu gewährleisten, dass personenbezogene Daten, die unrichtig oder nicht mehr aktuell sind, nicht übermittelt oder sonst zur Verfügung gestellt werden. Zu diesem Zweck hat er, soweit dies mit angemessenem Aufwand möglich ist, die Qualität der Daten vor ihrer Übermittlung oder Bereitstellung zu überprüfen. Bei jeder Übermittlung personenbezogener Daten hat er zudem, soweit dies möglich und angemessen ist, Informationen beizufügen, die es dem Empfänger gestatten, die Richtigkeit, die Vollständigkeit und die Zuverlässigkeit der Daten sowie deren Aktualität zu beurteilen.

2) Gelten für die Verarbeitung von personenbezogenen Daten besondere Bedingungen, so hat bei Datenübermittlungen die übermittelnde Stelle den Empfänger auf diese Bedingungen und die Pflicht zu ihrer Beachtung hinzuweisen. Die Hinweispflicht kann dadurch erfüllt werden, dass die Daten entsprechend markiert werden.

3) Die übermittelnde Stelle darf auf Empfänger in anderen EWR/Schengen-Staaten und auf Einrichtungen und sonstige Stellen, die nach den Kapiteln 4 und 5 des Titels V des Dritten Teils des Vertrags über die Arbeitsweise der Europäischen Union errichtet wurden, keine Bedingungen anwenden, die nicht auch für entsprechende innerstaatliche Datenübermittlungen gelten.

Art. 70

*Berichtigung und Löschung personenbezogener Daten sowie Einschränkung der Verarbeitung*

1) Der Verantwortliche hat personenbezogene Daten zu berichtigen, wenn sie unrichtig sind.

2) Der Verantwortliche hat personenbezogene Daten unverzüglich zu löschen, wenn ihre Verarbeitung unzulässig ist, sie zur Erfüllung einer rechtlichen Verpflichtung gelöscht werden müssen oder ihre Kenntnis für seine Aufgabenerfüllung nicht mehr erforderlich ist.

3) Art. 53 Abs. 3 bis 5 ist entsprechend anzuwenden. Sind unrichtige personenbezogene Daten oder personenbezogene Daten unrechtmässig übermittelt worden, ist auch dies dem Empfänger mitzuteilen.

4) Unbeschadet in Rechtsvorschriften festgesetzter Höchstspeicher- oder Löschfristen hat der Verantwortliche für die Löschung von personenbezogenen Daten oder eine regelmässige Überprüfung der Notwendigkeit ihrer Speicherung angemessene Fristen vorzusehen und durch verfahrensrechtliche Vorkehrungen sicherzustellen, dass diese Fristen eingehalten werden.

Art. 71

*Protokollierung*

1) In automatisierten Verarbeitungssystemen haben Verantwortliche und Auftragsverarbeiter mindestens die folgenden Verarbeitungsvorgänge zu protokollieren:

1. Erhebung,
2. Veränderung,
3. Abfrage,
4. Offenlegung einschliesslich Übermittlung,
5. Kombination und
6. Löschung.

2) Die Protokolle über Abfragen und Offenlegungen müssen es ermöglichen, die Begründung, das Datum und die Uhrzeit dieser Vorgänge und so weit wie möglich die Identität der Person, die die personenbezogenen Daten abgefragt oder offengelegt hat, und die Identität des Empfängers der Daten festzustellen.

3) Die Protokolle dürfen ausschliesslich für die Überprüfung der Rechtmässigkeit der Datenverarbeitung durch den Datenschutzbeauftragten, die Datenschutzstelle und die betroffene Person sowie für die Eigenüberwachung, für die Gewährleistung der Integrität und Sicherheit der personenbezogenen Daten und für Strafverfahren verwendet werden.

4) Die Protokolldaten sind am Ende des auf deren Generierung folgenden Jahres zu löschen.

5) Der Verantwortliche und der Auftragsverarbeiter haben die Protokolle der Datenschutzstelle auf Anforderung zur Verfügung zu stellen.

Art. 72

*Vertrauliche Meldung von Verstössen*

Der Verantwortliche hat zu ermöglichen, dass ihm vertrauliche Meldungen über in seinem Verantwortungsbereich erfolgende Verstösse gegen Datenschutzvorschriften zugeleitet werden können.

**Kapitel 5**

Datenübermittlungen an Drittstaaten und an internationale Organisationen

Art. 73

*Allgemeine Voraussetzungen*

1) Die Übermittlung personenbezogener Daten an Stellen in Drittstaaten oder an internationale Organisationen ist bei Vorliegen der übrigen für Datenübermittlungen geltenden Voraussetzungen zulässig, wenn

1. die Stelle oder internationale Organisation für die in Art. 40 genannten Zwecke zuständig ist und
2. die Europäische Kommission gemäss Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 einen Angemessenheitsbeschluss gefasst hat, welcher in Liechtenstein anwendbar ist.

2) Die Übermittlung personenbezogener Daten hat trotz des Vorliegens eines Angemessenheitsbeschlusses im Sinne des Abs. 1 Ziff. 2 und des zu berück-

sichtigenden öffentlichen Interesses an der Datenübermittlung zu unterbleiben, wenn im Einzelfall ein datenschutzrechtlich angemessener und die elementaren Grundrechte wahrender Umgang mit den Daten beim Empfänger nicht hinreichend gesichert ist oder sonst überwiegende schutzwürdige Interessen einer betroffenen Person entgegenstehen. Bei seiner Beurteilung hat der Verantwortliche massgeblich zu berücksichtigen, ob der Empfänger im Einzelfall einen angemessenen Schutz der übermittelten Daten garantiert.

3) Wenn personenbezogene Daten, die aus einem anderen EU/Schengen-Staat übermittelt oder zur Verfügung gestellt wurden, nach Abs. 1 übermittelt werden sollen, muss diese Übermittlung zuvor von der zuständigen Stelle des anderen EU/Schengen-Staats genehmigt werden. Übermittlungen ohne vorherige Genehmigung sind nur dann zulässig, wenn die Übermittlung erforderlich ist, um eine unmittelbare und ernsthafte Gefahr für die öffentliche Sicherheit eines Staates oder für die wesentlichen Interessen eines EU/Schengen-Staates abzuwehren, und die vorherige Genehmigung nicht rechtzeitig eingeholt werden kann. Im Fall des Satzes 2 ist die Stelle des anderen EU/Schengen-Staats, die für die Erteilung der Genehmigung zuständig gewesen wäre, unverzüglich über die Übermittlung zu unterrichten.

4) Der Verantwortliche, der Daten nach Abs. 1 übermittelt, hat durch geeignete Massnahmen sicherzustellen, dass der Empfänger die übermittelten Daten nur dann an andere Drittstaaten oder andere internationale Organisationen weiterübermittelt, wenn der Verantwortliche diese Übermittlung zuvor genehmigt hat. Bei der Entscheidung über die Erteilung der Genehmigung hat der Verantwortliche alle massgeblichen Faktoren zu berücksichtigen, insbesondere die Schwere der Straftat, den Zweck der ursprünglichen Übermittlung und das in dem Drittstaat oder der internationalen Organisation, an das oder an die die Daten weiterübermittelt werden sollen, bestehende Schutzniveau für personenbe-

zogene Daten. Eine Genehmigung darf nur dann erfolgen, wenn auch eine direkte Übermittlung an den anderen Drittstaat oder die andere internationale Organisation zulässig wäre. Die Zuständigkeit für die Erteilung der Genehmigung kann auch abweichend geregelt werden.

Art. 74

*Datenübermittlung bei geeigneten Garantien*

1) Liegt entgegen Art. 73 Abs. 1 Ziff. 2 kein Beschluss nach Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des Art. 73 auch dann zulässig, wenn

1. in einem rechtsverbindlichen Instrument geeignete Garantien für den Schutz personenbezogener Daten vorgesehen sind oder
2. der Verantwortliche nach Beurteilung aller Umstände, die bei der Übermittlung eine Rolle spielen, zu der Auffassung gelangt ist, dass geeignete Garantien für den Schutz personenbezogener Daten bestehen.

2) Der Verantwortliche hat Übermittlungen nach Abs. 1 Ziff. 2 zu dokumentieren. Die Dokumentation hat den Zeitpunkt der Übermittlung, die Identität des Empfängers, den Grund der Übermittlung und die übermittelten personenbezogenen Daten zu enthalten. Sie ist der Datenschutzstelle auf Anforderung zur Verfügung zu stellen.

3) Der Verantwortliche hat die Datenschutzstelle zumindest jährlich über Übermittlungen zu unterrichten, die aufgrund einer Beurteilung nach Abs. 1 Ziff. 2 erfolgt sind. In der Unterrichtung kann er die Empfänger und die Übermittlungszwecke angemessen kategorisieren.

Art. 75

*Datenübermittlung ohne geeignete Garantien*

1) Liegt entgegen Art. 73 Abs. 1 Ziff. 2 kein Beschluss nach Art. 36 Abs. 3 der Richtlinie (EU) 2016/680 vor und liegen auch keine geeigneten Garantien im Sinne des Art. 74 Abs. 1 vor, ist eine Übermittlung bei Vorliegen der übrigen Voraussetzungen des Art. 73 auch dann zulässig, wenn die Übermittlung erforderlich ist

1. zum Schutz lebenswichtiger Interessen einer natürlichen Person;
2. zur Wahrung berechtigter Interessen der betroffenen Person;
3. zur Abwehr einer gegenwärtigen und erheblichen Gefahr für die öffentliche Sicherheit eines Staates;
4. im Einzelfall für die in Art. 40 genannten Zwecke oder
5. im Einzelfall zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen im Zusammenhang mit den in Art. 40 genannten Zwecken.

2) Der Verantwortliche hat von einer Übermittlung nach Abs. 1 abzusehen, wenn die Grundrechte der betroffenen Person das öffentliche Interesse an der Übermittlung überwiegen.

3) Für Übermittlungen nach Abs. 1 gilt Art. 74 Abs. 2 entsprechend.

Art. 76

*Sonstige Datenübermittlung an Empfänger in Drittstaaten*

1) Verantwortliche können bei Vorliegen der übrigen für die Datenübermittlung in Drittstaaten geltenden Voraussetzungen im besonderen Einzelfall

personenbezogene Daten unmittelbar an nicht in Art. 73 Abs. 1 Ziff. 1 genannte Stellen in Drittstaaten übermitteln, wenn die Übermittlung für die Erfüllung ihrer Aufgaben unbedingt erforderlich ist und

1. im konkreten Fall keine Grundrechte der betroffenen Person das öffentliche Interesse an einer Übermittlung überwiegen;
2. die Übermittlung an die in Art. 73 Abs. 1 Ziff. 1 genannten Stellen wirkungslos oder ungeeignet wäre, insbesondere weil sie nicht rechtzeitig durchgeführt werden kann, und
3. der Verantwortliche dem Empfänger die Zwecke der Verarbeitung mitteilt und ihn darauf hinweist, dass die übermittelten Daten nur in dem Umfang verarbeitet werden dürfen, in dem ihre Verarbeitung für diese Zwecke erforderlich ist.

2) Im Fall des Abs. 1 hat der Verantwortliche die in Art. 73 Abs. 1 Ziff. 1 genannten Stellen unverzüglich über die Übermittlung zu unterrichten, sofern dies nicht wirkungslos oder ungeeignet ist.

3) Für Übermittlungen nach Abs. 1 gilt Art. 74 Abs. 2 und 3 entsprechend.

4) Bei Übermittlungen nach Abs. 1 hat der Verantwortliche den Empfänger zu verpflichten, die übermittelten personenbezogenen Daten ohne seine Zustimmung nur für den Zweck zu verarbeiten, für den sie übermittelt worden sind.

5) Abkommen im Bereich der justiziellen Zusammenarbeit in Strafsachen und der polizeilichen Zusammenarbeit bleiben unberührt.

## Kapitel 6

## Zusammenarbeit der Aufsichtsbehörden

### Art. 77
*Gegenseitige Amtshilfe*

1) Die Datenschutzstelle hat den Datenschutzaufsichtsbehörden in anderen EU/Schengen-Staaten Informationen zu übermitteln und Amtshilfe zu leisten, soweit dies für eine einheitliche Umsetzung und Anwendung der Richtlinie (EU) 2016/680 erforderlich ist. Die Amtshilfe betrifft insbesondere Auskunftsersuchen und aufsichtsbezogene Massnahmen, beispielsweise Ersuchen um Konsultation oder um Vornahme von Nachprüfungen und Untersuchungen.

2) Die Datenschutzstelle hat alle geeigneten Massnahmen zu ergreifen, um Amtshilfeersuchen unverzüglich und spätestens innerhalb eines Monats nach deren Eingang nachzukommen.

3) Die Datenschutzstelle darf Amtshilfeersuchen nur ablehnen, wenn

1. sie für den Gegenstand des Ersuchens oder für die Massnahmen, die sie durchführen soll, nicht zuständig ist oder
2. ein Eingehen auf das Ersuchen gegen Rechtsvorschriften verstossen würde.

4) Die Datenschutzstelle hat die ersuchende Aufsichtsbehörde des anderen Staates über die Ergebnisse oder gegebenenfalls über den Fortgang der Massnahmen zu informieren, die getroffen wurden, um dem Amtshilfeersuchen nachzukommen. Sie hat im Fall des Abs. 3 die Gründe für die Ablehnung des Ersuchens zu erläutern.

5) Die Datenschutzstelle hat die Informationen, um die sie von der Aufsichtsbehörde des anderen Staates ersucht wurde, in der Regel elektronisch und in einem standardisierten Format zu übermitteln.

6) Die Datenschutzstelle hat Amtshilfeersuchen kostenfrei zu erledigen, soweit sie nicht im Einzelfall mit der Aufsichtsbehörde des anderen Staates die Erstattung entstandener Ausgaben vereinbart hat.

7) Ein Amtshilfeersuchen der Datenschutzstelle hat alle erforderlichen Informationen zu enthalten; hierzu gehören insbesondere der Zweck und die Begründung des Ersuchens. Die auf das Ersuchen übermittelten Informationen dürfen ausschliesslich zu dem Zweck verwendet werden, zu dem sie angefordert wurden.

## Kapitel 7

## Haftung und Sanktionen

### Art. 78

### *Schadensersatz und Entschädigung*

1) Hat ein Verantwortlicher einer betroffenen Person durch eine Verarbeitung personenbezogener Daten, die nach diesem Gesetz oder nach anderen auf ihre Verarbeitung anwendbaren Vorschriften rechtswidrig war, einen Schaden zugefügt, ist er oder sein Rechtsträger der betroffenen Person zum Schadenersatz verpflichtet. Die Ersatzpflicht entfällt, soweit bei einer nicht automatisierten Verarbeitung der Schaden nicht auf ein Verschulden des Verantwortlichen zurückzuführen ist.

2) Wegen eines Schadens, der nicht Vermögensschaden ist, kann die betroffene Person eine angemessene Entschädigung in Geld verlangen.

3) Lässt sich bei einer automatisierten Verarbeitung personenbezogener Daten nicht ermitteln, welche von mehreren beteiligten Verantwortlichen den Schaden verursacht hat, so haftet jeder Verantwortliche beziehungsweise sein Rechtsträger.

4) Hat bei der Entstehung des Schadens ein Verschulden der betroffenen Person mitgewirkt, sind §§ 1301 bis 1304 des Allgemeinen Bürgerlichen Gesetzbuchs entsprechend anzuwenden.

5) Auf die Verjährung finden die für widerrechtliche Handlungen geltenden Verjährungsvorschriften des Allgemeinen Bürgerlichen Gesetzbuchs entsprechende Anwendung.

Art. 79

*Strafvorschriften*

Für Verarbeitungen personenbezogener Daten durch öffentliche Stellen im Rahmen von Tätigkeiten nach Art. 40 Satz 1, 3 oder 4 findet Art. 37 entsprechende Anwendung.

## Teil 4

## Besondere Bestimmungen für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten

### Art. 80

*Verarbeitung personenbezogener Daten im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten*

1) Die Übermittlung personenbezogener Daten an einen Drittstaat oder an supra- oder internationale Organisationen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten ist über die bereits gemäss der Verordnung (EU) 2016/679 zulässigen Fälle hinaus auch dann zulässig, wenn sie zur Erfüllung eigener Aufgaben aus zwingenden Gründen der Landesverteidigung oder zur Erfüllung vertraglicher Verpflichtungen des Staates auf dem Gebiet der Krisenbewältigung oder Konfliktverhinderung oder für humanitäre Massnahmen erforderlich ist. Der Empfänger ist darauf hinzuweisen, dass die übermittelten Daten nur zu dem Zweck verwendet werden dürfen, zu dem sie übermittelt wurden.

2) Für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätigkeiten durch die Landespolizei gilt Art. 16 Abs. 4 nicht, soweit die Regierung im Einzelfall feststellt, dass die Erfüllung der dort genannten Pflichten die Sicherheit des Landes gefährden würde.

3) Für Verarbeitungen im Rahmen von nicht in die Anwendungsbereiche der Verordnung (EU) 2016/679 und der Richtlinie (EU) 2016/680 fallenden Tätig-

keiten durch öffentliche Stellen besteht keine Informationspflicht gemäss Art. 13 Abs. 1 und 2 der Verordnung (EU) 2016/679, wenn

1. es sich um Fälle des Art. 29 Abs. 1 Ziff. 1 bis 3 handelt oder
2. durch ihre Erfüllung Informationen offenbart würden, die gemäss einer Rechtsvorschrift oder ihrem Wesen nach, insbesondere wegen der überwiegenden berechtigten Interessen eines Dritten, geheim gehalten werden müssen, und deswegen das Interesse der betroffenen Person an der Erteilung der Information zurücktreten muss.

Ist die betroffene Person in den Fällen des Satzes 1 nicht zu informieren, besteht auch kein Recht auf Auskunft. Art. 29 Abs. 2 und Art. 30 Abs. 2 finden keine Anwendung.

## II.

## Übergangs- und Schlussbestimmungen

### Art. 81

*Durchführungsverordnungen*

Die Regierung erlässt die zur Durchführung dieses Gesetzes notwendigen Verordnungen, insbesondere über:

a) Voraussetzungen, unter welchen eine Behörde Personendaten durch einen Dritten bearbeiten lassen oder für Dritte bearbeiten darf;

b) das Verfahren zur Bewilligung von Videoüberwachungen;

c) das Zertifizierungsverfahren.

Art. 82

*Aufhebung bisherigen Rechts*

Das Datenschutzgesetz (DSG) vom 14. März 2002, LGBL. 2002 Nr. 55, in der geltenden Fassung, wird aufgehoben.

Art. 83

*Datenschutzstelle*

1) Der bisherige Datenschutzbeauftragte übernimmt ab Inkrafttreten dieses Gesetzes die Leitung der nach Art. 8 eingerichteten Datenschutzstelle.

2) Bestehende Dienstverhältnisse des übrigen Personals der Datenschutzstelle bleiben nach Inkrafttreten dieses Gesetzes weiterhin aufrecht.

3) Die Amtszeit des zum Zeitpunkt des Inkrafttretens dieses Gesetzes bestellten Datenschutzbeauftragten endet nach Ablauf von acht Jahren nach seiner Wahl durch den Landtag. Für eine allfällige vorzeitige Abberufung des Datenschutzbeauftragten im Sinne von Art. 12 Abs. 2 und für allfällige personalrechtliche Entscheide im Sinne von Art. 12 Abs. 6 Bst. b ist nach Inkrafttreten dieses Gesetzes die Regierung zuständig.

Art. 84

*Datenschutzkommission, laufende Verfahren*

1) Die Amtszeit der Datenschutzkommission endet mit dem Inkrafttreten dieses Gesetzes.

2) Die zum Zeitpunkt des Inkrafttretens dieses Gesetzes vor der Datenschutzkommission hängigen Beschwerdeverfahren werden von der Beschwerde-

kommission für Verwaltungsangelegenheiten nach Massgabe des neuen Rechts behandelt.

3) Die zum Zeitpunkt des Inkrafttretens dieses Gesetzes vor der Datenschutzkommission hängigen Verfahren über Empfehlungen der Datenschutzstelle werden der Datenschutzstelle zur neuerlichen Behandlung nach Massgabe des neuen Rechts übergeben.

Art. 85

*Bewilligungen Videoüberwachung*

1) Die zum Zeitpunkt des Inkrafttretens dieses Gesetzes bereits erteilten Bewilligungen für eine Videoüberwachung behalten ihre Gültigkeit.

2) Die Verlängerung einer zum Zeitpunkt des Inkrafttretens dieses Gesetzes bereits bewilligten Videoüberwachung richtet sich ab dem Inkrafttreten dieses Gesetzes nach diesem.

Art. 86

*Abänderung von Bezeichnungen*

1) In nachfolgenden Gesetzen ist die Bezeichnung "Personendaten" durch die Bezeichnung "personenbezogene Daten", in der jeweils grammatikalisch richtigen Form, zu ersetzen:

a) Gemeindegesetz (GemG) vom 20. März 1996, LGBl. 1996 Nr. 76;

b) Gesetz vom 17. Mai 2006 über die Versicherungsvermittlung (Versicherungsvermittlungsgesetz; VersVermG), LGBl. 2006 Nr. 125;

c) Gesetz vom 4. Januar 1934 über den Erwerb und Verlust des Landesbürgerrechtes (Bürgerrechtsgesetz; BüG), LGBl. 1960 Nr. 23;

d) Gesetz vom 17. September 2008 über die Ausländer (Ausländergesetz; AuG), LGBl. 2008 Nr. 311;

e) Asylgesetz (AsylG) vom 14. Dezember 2011, LGBl. 2012 Nr. 29;

f) Heimatschriftengesetz (HSchG) vom 18. Dezember 1985, LGBl. 1986 Nr. 27;

g) Gesetz vom 19. Mai 1999 über die Information der Bevölkerung (Informationsgesetz), LGBl. 1999 Nr. 159;

h) Gesetz vom 21. September 2011 über das Zentrale Personenregister (ZPRG), LGBl. 2011 Nr. 574;

i) Richterdienstgesetz (RDG) vom 24. Oktober 2007, LGBl. 2007 Nr. 347;

j) Staatsanwaltschaftsgesetz (StAG) vom 15. Dezember 2010, LGBl. 2011 Nr. 49;

k) Gesetz vom 24. April 2008 über das Dienstverhältnis des Staatspersonals (Staatspersonalgesetz; StPG), LGBl. 2008 Nr. 144;

l) Gesetz vom 24. Oktober 2007 über das Mobilitätsmanagement des Landes (Landes-Mobilitätsmanagement-Gesetz; LMMG), LGBl. 2007 Nr. 333;

m) Allgemeines bürgerliches Gesetzbuch vom 1. Juni 1811, LGBl. 1003 Nr. 1;

n) Patientenverfügungsgesetz (PatVG) vom 13. April 2011, LGBl. 2011 Nr. 209;

o) Gesetz vom 15. Dezember 2004 über die Mediation in Zivilrechtssachen (Zivilrechts-Mediations-Gesetz; ZMG), LGBl. 2005 Nr. 31;

p) Strafprozessordnung (StPO) vom 18. Oktober 1988, LGBl. 1988 Nr. 62;

q) Gesetz vom 13. September 2000 über die Bewährungshilfe (Bewährungshilfegesetz, BewHG), LGBl. 2002 Nr. 21;

r) Gesetz vom 5. November 2015 über den internationalen automatischen Informationsaustausch in Steuersachen (AIA-Gesetz), LGBl. 2015 Nr. 355;

s) Gesetz vom 4. November 2016 über den internationalen automatischen Austausch länderbezogener Berichte multinationaler Konzerne (CbC-Gesetz), LGBl. 2016 Nr. 502;

t) Gesetz vom 4. Dezember 2014 über die Umsetzung des FATCA-Abkommens zwischen dem Fürstentum Liechtenstein und den Vereinigten Staaten von Amerika (FATCA-Gesetz), LGBl. 2015 Nr. 7;

u) Schulgesetz (SchulG) vom 15. Dezember 1971, LGBl. 1972 Nr. 7;

v) Gesetz vom 26. November 2003 über das Dienstverhältnis der Lehrer (Lehrerdienstgesetz, LdG), LGBl. 2004 Nr. 4;

w) Gesetz vom 25. November 2004 über das Hochschulwesen (Hochschulgesetz; HSG), LGBl. 2005 Nr. 2;

x) Gesetz vom 25. November 2004 über die Universität Liechtenstein (LUG), LGBl. 2005 Nr. 3;

y) Gesetz vom 20. Oktober 2004 über die staatlichen Ausbildungsbeihilfen (Stipendiengesetz; StipG), LGBl. 2004 Nr. 262;

z) Gesetz vom 19. September 2012 über die Kinder- und Jugendzahnpflege (KJZG), LGBl. 2012 Nr. 343;

aa) Statistikgesetz (StatG) vom 17. September 2008, LGBl. 2008 Nr. 271;

ab) Archivgesetz vom 23. Oktober 1997, LGBl. 1997 Nr. 215;

ac) Mediengesetz (MedienG) vom 19. Oktober 2005, LGBl. 2005 Nr. 25;

ad) Tierschutzgesetz (TSchG) vom 23. September 2010, LGBl. 2010 Nr. 333;

ae) Gesetz vom 17. September 2008 über Waffen, Waffenzubehör und Munition (Waffengesetz; WaffG), LGBl. 2008 Nr. 275;

af) Gesetz vom 22. Oktober 2009 über die Finanzkontrolle (Finanzkontrollgesetz; FinKG), LGBl. 2009 Nr. 324;

ag) Gesetz vom 23. September 2010 über die Landes- und Gemeindesteuern (Steuergesetz; SteG), LGBl. 2010 Nr. 34;

ah) Gesetz vom 22. Oktober 2009 über die Mehrwertsteuer (Mehrwertsteuergesetz; MWSTG), LGBl. 2009 Nr. 33;

ai) Gesetz vom 24. April 2008 über die Förderung der Energieeffizienz und der erneuerbaren Energien (Energieeffizienzgesetz; EEG), LGBl. 2008 Nr. 116;

aj) Strassenverkehrsgesetz (SVG) vom 30. Juni 1978, LGBl. 1978 Nr. 18;

ak) Gesetz vom 22. Juni 2006 über die Zulassung als Strassentransportunternehmen und die grenzüberschreitenden Personen- und Gütertransporte auf der Strasse (Strassentransportgesetz; STG), LGBl. 2006 Nr. 185;

al) Eisenbahngesetz (EBG) vom 16. März 2011, LGBl. 2011 Nr. 182;

am) Gesundheitsgesetz (GesG) vom 13. Dezember 2007, LGBl. 2008 Nr. 3;

an) Gesetz vom 22. Oktober 2003 über die Ärzte (Ärztegesetz), LGBl. 2003 Nr. 239;

ao) Gesetz vom 20. November 2008 über die Tierärzte und andere Tiergesundheitsberufe (Tiergesundheitsberufegesetz; TGBG), LGBl. 2009 Nr. 6;

ap) Gesetz vom 4. Dezember 2014 über Arzneimittel und Medizinprodukte (Heilmittelgesetz; HMG), LGBl. 2015 Nr. 23;

aq) Umweltschutzgesetz (USG) vom 29. Mai 2008, LGBl. 2008 Nr. 199;

ar) Gesetz vom 5. Dezember 2013 über die Umweltverträglichkeitsprüfung (UVPG), LGBl. 2014 Nr. 19;

as) Gesetz vom 25. November 2010 über den Umgang mit genetisch veränderten, pathogenen oder gebietsfremden Organismen (Organismengesetz; OrgG), LGBl. 2011 Nr. 4;

at) Gesetz vom 29. Dezember 1966 über die Arbeit in Industrie, Gewerbe und Handel (Arbeitsgesetz), LGBl. 1967 Nr. 6;

au) Gesetz vom 14. Dezember 1952 über die Alters- und Hinterlassenenversicherung (AHVG), LGBl. 1952 Nr. 29;

av) Gesetz vom 23. Dezember 1959 über die Invalidenversicherung (IVG), LGBl. 1960 Nr. 5;

aw) Gesetz vom 10. Dezember 1965 über Ergänzungsleistungen zur Alters-, Hinterlassenen- und Invalidenversicherung (ELG), LGBl. 1965 Nr. 46;

ax) Gesetz vom 20. Oktober 1987 über die betriebliche Personalvorsorge (BPVG), LGBl. 1988 Nr. 12;

ay) Gesetz vom 24. November 2006 betreffend die Aufsicht über Einrichtungen der betrieblichen Altersversorgung (Pensionsfondsgesetz; PFG), LGBl. 2007 Nr. 11;

az) Gesetz vom 24. November 1971 über die Krankenversicherung (KVG), LGBl. 1971 Nr. 5;

ba) Gesetz vom 28. November 1989 über die obligatorische Unfallversicherung (Unfallversicherungsgesetz; UVersG), LGBl. 1990 Nr. 46;

bb) Gesetz vom 25. November 1981 betreffend Ausrichtung einer Mutterschaftszulage, LGBl. 1982 Nr. 8;

bc) Gesetz vom 18. Dezember 1985 über die Familienzulagen (Familienzulagengesetz; FZG), LGBl. 1986 Nr. 28;

bd) Gesetz vom 24. November 2010 über die Arbeitslosenversicherung und die Insolvenzentschädigung (Arbeitslosenversicherungsgesetz; ALVG), LGBl. 2010 Nr. 452;

be) Gesetz vom 30. Juni 1977 über die Förderung des Wohnungsbaues (Wohnbauförderungsgesetz; WBFG), LGBl. 1977 Nr. 46;

bf) Gesetz vom 13. September 2000 über Mietbeiträge für Familien, LGBl. 2000 Nr. 202;

bg) Sozialhilfegesetz vom 15. November 1984, LGBl. 1985 Nr. 17;

bh) Kinder- und Jugendgesetz (KJG) vom 10. Dezember 2008, LGBl. 2009 Nr. 29;

bi) Gesetz vom 17. Dezember 1970 über die Gewährung von Blindenbeihilfen, LGBl. 1971 Nr. 7;

bj) Landwirtschaftsgesetz (LWG) vom 11. Dezember 2008, LGBl. 2009 Nr. 42;

bk) Gesetz vom 13. Juli 1966 über die Organisation der Tierseuchenpolizei (Tierseuchenpolizeigesetz; TSPG), LGBl. 1966 Nr. 17;

bl) Gewerbegesetz (GewG) vom 22. Juni 2006, LGBl. 2006 Nr. 184;

bm) Gesetz vom 20. Oktober 2010 über die Erbringung von Dienstleistungen (Dienstleistungsgesetz; DLG), LGBl. 2010 Nr. 385;

bn) Gesetz vom 29. Mai 2008 über die Architekten und andere qualifizierte Berufe im Bereich des Bauwesens (Bauwesen-Berufe-Gesetz; BWBG), LGBl. 2008 Nr. 188;

bo) Geldspielgesetz (GSG) vom 30. Juni 2010, LGBl. 2010 Nr. 235;

bp) Zahlungsdienstegesetz (ZDG) vom 17. September 2009, LGBl. 2009 Nr. 271;

bq) E-Geldgesetz (EGG) vom 17. März 2011, LGBl. 2011 Nr. 151;

br) Gesetz vom 25. November 2005 über die Vermögensverwaltung (Vermögensverwaltungsgesetz; VVG), LGBl. 2005 Nr. 278;

bs) Investmentunternehmensgesetz (IUG) vom 2. Dezember 2015, LGBl. 2016 Nr. 45;

bt) Gesetz vom 28. Juni 2011 über bestimmte Organismen für gemeinsame Anlagen in Wertpapieren (UCITSG), LGBl. 2011 Nr. 295;

bu) Gesetz vom 19. Dezember 2012 über die Verwalter alternativer Investmentfonds (AIFMG), LGBl. 2013 Nr. 49;

bv) Gesetz vom 21. Oktober 1992 über die Banken und Wertpapierfirmen (Bankengesetz; BankG), LGBl. 1992 Nr. 108;

bw) Gesetz vom 14. März 2002 über die Stabsstelle Financial Intelligence Unit (FIU-Gesetz; FIUG), LGBl. 2002 Nr. 57;

bx) Wertpapierprospektgesetz (WPPG) vom 23. Mai 2007, LGBl. 2007 Nr. 196;

by) Gesetz vom 2. März 2016 zur Durchführung der Verordnung (EU) Nr. 648/2012 über OTC-Derivate, zentrale Gegenparteien und Transaktionsregister (EMIR-Durchführungsgesetz; EMIR-DG), LGBl. 2016 Nr. 156;

bz) Gesetz vom 12. Juni 2015 betreffend die Aufsicht über Versicherungsunternehmen (Versicherungsaufsichtsgesetz; VersAG), LGBl. 2015 Nr. 231.

2) In nachfolgenden Verordnungen ist die Bezeichnung "Personendaten" durch die Bezeichnung "personenbezogene Daten", in der jeweils grammatikalisch richtigen Form, zu ersetzen:

a) Verordnung vom 22. August 2000 über den Dienstbetrieb und die Organisation der Landespolizei (PolDOV), LGBl. 2000 Nr. 195;

b) Verordnung vom 7. Juni 2016 über die Informationssysteme der Landespolizei (Pol-ISV) , LGBl. 2016 Nr. 202;

c) Verordnung vom 15. März 2011 über das Schengener Informationssystem (SIS) und das SIRENE-Büro (Nationale SIS-Verordnung; N-SIS-V), LGBl. 2011 Nr. 14;

d) Verordnung vom 15. November 2011 über das zentrale Visa-Informationssystem und das nationale Visumsystem (Visa-Informationssystem-Verordnung; VISV), LGBl. 2011 Nr. 503;

e) Heimatschriftenverordnung (HSchV) vom 28. September 2011, LGBl. 2011 Nr. 453;

f) Verordnung vom 19. Oktober 1999 zum Informationsgesetz (Informationsverordnung), LGBl. 1999 Nr. 206;

g) Verordnung vom 20. Dezember 2011 über den elektronischen Geschäftsverkehr mit Behörden (E-Government-Verordnung; E-GovV), LGBl. 2011 Nr. 6;

h) Verordnung vom 20. Dezember 2011 über das Zentrale Personenregister (ZPRV), LGBl. 2011 Nr. 602;

i) Verordnung vom 2. Dezember 2008 über das Dienstverhältnis des Staatspersonals (Staatspersonalverordnung; StPV), LGBl. 2008 Nr. 303;

j) Verordnung vom 27. November 2007 über das Mobilitätsmanagement des Landes (Landes-Mobilitätsmanagement-Verordnung; LMMV), LGBl. 2007 Nr. 334;

k) Grundbuchverordnung (GBV) vom 29. November 2016, LGBl. 2016 Nr. 418;

l) Grundverkehrsverordnung (GVV) vom 3. Juli 2007, LGBl. 2007 Nr. 168;

m) Verordnung vom 10. Dezember 2013 über die Datenschutzzertifizierungen (VDSZ), LGBl. 2013 Nr. 403;

n) Verordnung vom 20. März 2013 über die staatlichen Ausbildungsbeihilfen (Stipendienverordnung; StipV), LGBl. 2013 Nr. 144;

o) Verordnung vom 16. Juni 2009 über Waffen, Waffenzubehör und Munition (Waffenverordnung; WaffV), LGBl. 2009 Nr. 166;

p) Verordnung vom 19. Juni 2012 über die Feuerwehreinsatzpläne (FWEV), LGBl. 2012 Nr. 169;

q) Verordnung vom 3. April 2007 über die Aufgaben und Befugnisse der Regulierungsbehörde im Bereich der elektronischen Kommunikation (RKV), LGBl. 2007 Nr. 68;

r) Verordnung vom 8. Mai 2007 über Identifikationsmittel und Frequenzen im Bereich der elektronischen Kommunikation (IFV), LGBl. 2007 Nr. 118;

s) Verordnung vom 28. April 2015 über die Betäubungsmittel und die psychotropen Stoffe (Betäubungsmittelverordnung; BMV), LGBl. 2015 Nr. 132;

t) Verordnung I vom 22. März 2005 zum Arbeitsgesetz (ArGV I), LGBl. 2005 Nr. 67;

u) Verordnung vom 14. Dezember 2010 über die Arbeitslosenversicherung und die Insolvenzentschädigung (Arbeitslosenversicherungsverordnung; ALVV), LGBl. 2010 Nr. 465;

v) Spielbankenverordnung (SPBV) vom 21. Dezember 2010, LGBl. 2010 Nr. 439;

w) Verordnung vom 27. Oktober 2009 über die aussergerichtliche Schlichtungsstelle im Finanzdienstleistungsbereich (Finanzdienstleistungs-Schlichtungsstellen-Verordnung; FSV), LGBl. 2009 Nr. 279.

## III.

## Inkrafttreten

Dieses Gesetz tritt unter Vorbehalt des ungenutzten Ablaufs der Referendumsfrist am … in Kraft, andernfalls am Tag nach der Kundmachung.

## 2. ABÄNDERUNG DES GESETZES ÜBER DIE BETRIEBLICHE PERSONALVORSORGE DES STAATES

# Gesetz

vom …

# über die Abänderung des Gesetzes über die betriebliche Personalvorsorge des Staates

Dem nachstehend vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

### I.

### Abänderung bisherigen Rechts

Das Gesetz über die betriebliche Personalvorsorge des Staates (SBPVG) vom 6. September 2013, LGBl. 2013 Nr. 329, wird wie folgt abgeändert:

Art. 1 Bst. d

Dieses Gesetz regelt die betriebliche Alters-, Invaliden- und Hinterlassenenversicherung (betriebliche Vorsorge) für:

d) das Personal des Parlamentsdienstes und der Finanzkontrolle;

## II.

## Inkrafttreten

Dieses Gesetz tritt gleichzeitig mit dem Gesetz vom … über die Abänderung des Datenschutzgesetzes in Kraft.

## 3. ABÄNDERUNG DES GESETZES ÜBER DIE FINANZKONTROLLE

# Gesetz

vom …

# über die Abänderung des Gesetzes über die Finanzkontrolle

Dem nachstehend vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

**I.**

**Abänderung bisherigen Rechts**

Das Gesetz über die Finanzkontrolle (Finanzkontrollgesetz; FinKG) vom 22. Oktober 2009, LGBl. 2009 Nr. 324, in der geltenden Fassung, wird wie folgt abgeändert:

Art. 14 Abs. 4

4) Stellt die Finanzkontrolle Mängel oder Missstände von erheblicher finanzieller oder grundsätzlicher Bedeutung fest, informiert sie unverzüglich nach Abschluss der Prüfung die Regierung und die Geschäftsprüfungskommission. Soweit die Justizverwaltung betroffen ist, benachrichtigt sie die Konferenz der Gerichtspräsidenten oder, soweit der Parlamentsdienst betroffen ist, das Landtagspräsidium. In dringenden Fällen informiert der Leiter der Finanzkontrolle den Regie-

rungschef und den Vorsitzenden der Geschäftsprüfungskommission mündlich und hält dies auch protokollarisch fest.

Art. 15

Weist die geprüfte Stelle eine Beanstandung zurück, so kann die Finanzkontrolle bei der Regierung die entsprechenden Massnahmen beantragen. Bei Beanstandungen von Stellen der Justizverwaltung richtet die Finanzkontrolle ihre Anträge an die Konferenz der Gerichtspräsidenten oder, bei Beanstandungen von Stellen des Parlamentsdienstes an das Landtagspräsidium.

## II.
## Inkrafttreten

Dieses Gesetz tritt gleichzeitig mit dem Gesetz vom … über die Abänderung des Datenschutzgesetzes in Kraft.

## 4. ABÄNDERUNG DES BESCHWERDEKOMMISSIONSGESETZES

# Gesetz

vom ….

# über die Abänderung des Beschwerdekommissionsgesetzes

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

### I.

### Abänderung bisherigen Rechts

Das Beschwerdekommissionsgesetz vom 25. Oktober 2000, LGBl. 2000 Nr. 248, in der geltenden Fassung, wird wie folgt abgeändert:

Art. 4 Abs. 1 Bst. s

1) Die Beschwerdekommission ist zuständig für Beschwerden gegen Verfügungen und Entscheidungen im Bereich:

s) Datenschutz:

der Datenschutzstelle und der zuständigen Behörde aufgrund der Datenschutzgesetzgebung und der darauf gestützten Verordnungen.

## II.

## Inkrafttreten

Dieses Gesetz tritt gleichzeitig mit dem Gesetz vom … über die Abänderung des Datenschutzgesetzes in Kraft.

## 5. ABÄNDERUNG DES POLIZEIGESETZES

# Gesetz

vom ….

# über die Abänderung des Polizeigesetzes

Dem nachstehenden vom Landtag gefassten Beschluss erteile Ich Meine Zustimmung:

### I.

### Abänderung bisherigen Rechts

Das Gesetz vom 21. Juni 1989 über die Landespolizei (Polizeigesetz; PolG), LGBl. 1989 Nr. 48, in der geltenden Fassung, wird wie folgt abgeändert:

Art. 24d Abs. 5

5) Die Landespolizei kann die Daten der Einwohnerkontrollen der Gemeinden über Personen, die in Liechtenstein ihren ordentlichen Wohnsitz angemeldet haben, mit den Personenfahndungen nach Abs. 1 abgleichen. Bis die entsprechenden technischen Möglichkeiten für einen automatisierten Datenabgleich zur Verfügung stehen, kann die Regierung mit Verordnung vorsehen, dass die Gemeinden für den Abgleich mit den Personenfahndungen die personenbezogene Daten von neu zuziehenden Personen der Landespolizei innerhalb einer bestimmten Frist bekannt zu geben haben.

Art. 30a Abs. 1 Bst. d

1) Die Landespolizei führt im Rahmen des Staatsschutzes (Art. 2 Abs. 2) für Bedienstete des Landes und Dritte, die an klassifizierten Projekten im Bereich der inneren und äusseren Sicherheit mitwirken, Sicherheitsprüfungen durch, wenn sie bei ihrer Tätigkeit:

d) regelmässig Zugang zu besonderen Kategorien personenbezogener Daten haben, deren Offenbarung die Persönlichkeitsrechte der Betroffenen schwerwiegend beeinträchtigen könnte.

Art. 30c Abs. 2

2) Die geprüfte Person kann innert zehn Tagen Einsicht in die Prüfungsunterlagen nehmen und die Berichtigung falscher personenbezogener Daten verlangen sowie bei Akten des Landes die Entfernung überholter personenbezogener Daten verlangen oder einen Bestreitungsvermerk anbringen lassen. Vorbehalten bleiben Art. 35s Abs. 2 dieses Gesetzes und Art. 52 Abs. 4 des Datenschutzgesetzes.

Art. 30f, Sachüberschrift und Bst. a

*c) Sperre der Datenoffenlegung; Mitteilungs- und Aushändigungspflicht*

Die Landespolizei kann von Amtsstellen der Landesverwaltung, Verwaltungsbehörden und Gerichten sowie von Privaten verlangen, dass diese:

a) bestimmte personenbezogene Daten von Personen nach Art. 2 Abs. 1 Bst. p nicht offenlegen, soweit die bestehenden technischen Möglichkeiten dies erlauben; diese haben bei ihrer Datenverarbeitung sicherzustellen, dass der Zeugenschutz nicht beeinträchtigt wird;

Überschrift vor Art. 31

IV. Verarbeitung von polizeilichen Daten

Art. 31, Sachüberschrift, Abs. 1 Einleitungssatz, Abs. 2 bis 4

*Datenverarbeitung im Allgemeinen*

1) Die Landespolizei ist zur Verarbeitung personenbezogener Daten, einschliesslich besonderer Kategorien personenbezogener Daten, wie insbesondere genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person und Gesundheitsdaten, und zum Profiling von nachstehend aufgeführten Personen befugt, soweit dies zur Erfüllung ihrer gesetzlichen Aufgaben erforderlich ist:

2) Die Verarbeitung der personenbezogenen Daten nach Abs. 1 darf nur zu dem Zweck erfolgen, zu dem diese Daten beschafft wurden. Die Weiterverarbeitung zu anderen Zwecken ist jedoch zulässig, soweit die Landespolizei diese Daten auch zu diesem Zweck beschaffen darf.

3) Die Beschaffung von personenbezogenen Daten nach Abs. 1 muss für die betroffene Person erkennbar erfolgen, ausser wenn dadurch:

a) die Erfüllung der polizeilichen Aufgaben gefährdet oder erheblich erschwert würde; oder

b) ein unverhältnismässiger Aufwand entstehen würde.

4) Ist die Beschaffung der personenbezogenen Daten nach Abs. 1 für die betroffene Person nicht erkennbar, so muss diese nachträglich nach Massgabe von Art. 51 des Datenschutzgesetzes informiert werden.

Art. 34a Abs. 8 Einleitungssatz, Bst. b und c

8) Personen, gegen die sich die Massnahmen nach Abs. 2 richten, sind nach Abschluss der Massnahme hierüber zu unterrichten, sobald der Zweck der Datenverarbeitung dadurch nicht mehr gefährdet wird. Eine Unterrichtung durch die Landespolizei unterbleibt, wenn:

b) keine Aufzeichnung mit personenbezogenen Daten erstellt oder sie unverzüglich nach Beendigung der Massnahme vernichtet worden sind; oder

c) zu ihrer Durchführung in unverhältnismässiger Weise weitere personenbezogene Daten beschafft werden müssten.

Art. 34b Abs. 1, Abs. 2 Bst. d, Abs. 3 Bst. a Einleitungssatz, Abs. 4, 6 und 6a

1) Die Landespolizei kann zur Erfüllung ihrer Aufgaben elektronische Informationssysteme führen, die auch besondere Kategorien personenbezogener Daten, wie insbesondere genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person und Gesundheitsdaten, enthalten können.

2) Die Informationssysteme nach Abs. 1 dienen folgenden Zwecken:

d) Analyse, Recherche und Profiling;

3) Informationssysteme nach Abs. 1 können insbesondere folgende Daten enthalten:

a) personenbezogene Daten, wie:

4) Die Daten der Informationssysteme nach Abs. 1 dürfen nach Personen, Objekten und Ereignissen erschliessbar gemacht und untereinander verknüpft

werden. Werden Daten untereinander verknüpft, unterliegen diese Daten den entsprechenden Datenverarbeitungsregeln und Zugriffsbeschränkungen. Vorbehalten bleibt Abs. 6.

6) Personenbezogene Daten, die im Zusammenhang mit der vorbeugenden Bekämpfung von Straftaten (Art. 2 Abs. 1 Bst. d) oder im Rahmen des Staatsschutzes (Art. 2 Abs. 2) in Informationssystemen verarbeitet werden, sind von anderen Informationssystemen getrennt zu führen.

6a) Werden personenbezogene Daten im Zusammenhang mit der Betreuung des Sanitätsnotrufs (Art. 2 Abs. 1 Bst. $p^{bis}$) in Informationssystemen verarbeitet, ist sicherzustellen, dass der Zugriff ausschliesslich für diesen Zweck erfolgt.

Art. 34c

*Datenverwendung zu besonderen Zwecken*

1) Die Verwendung von personenbezogenen Daten für wissenschaftliche und statistische Zwecke ist nur zulässig, sofern die Identifizierung betroffener Personen verunmöglicht wird.

2) Die Landespolizei kann von ihr verarbeitete personenbezogene Daten zur polizeilichen Aus- und Weiterbildung in anonymisierter Form nutzen. Auf eine Anonymisierung kann nur dann verzichtet werden, wenn dies dem Aus- oder Weiterbildungszweck entgegensteht und die berechtigten Interessen der betroffenen Person an der Geheimhaltung nicht überwiegen.

Art 34d Abs. 1, Abs. 2 Einleitungssatz, Abs. 3 Einleitungssatz und Abs. 4

1) Die Landespolizei kann Amtsstellen der Landesverwaltung, Verwaltungsbehörden und Gerichten sowie dem schweizerischen Grenzwachtkorps perso-

nenbezogene Daten, einschliesslich besonderer Kategorien personenbezogener Daten sowie Daten aus dem Profiling, offenlegen oder übermitteln (Datenbekanntgabe), sofern dies zur Erfüllung ihrer gesetzlichen Aufgaben oder der Aufgaben der Datenempfänger notwendig ist.

2) Die Landespolizei kann personenbezogene Daten anderen Stellen oder Personen bekannt geben, soweit dies gesetzlich vorgesehen oder unerlässlich ist für:

3) Die Landespolizei kann geeigneten sozialen und therapeutischen Fachstellen personenbezogene Daten bekannt geben, soweit dies zum Schutz gefährdeter Menschen erforderlich ist, insbesondere:

4) Die Landespolizei kann Daten von Personen, die sich nachweislich anlässlich von Sportveranstaltungen im In- und Ausland gewalttätig verhalten haben, an Organisatoren von Sportveranstaltungen in Liechtenstein bekannt geben, wenn diese Daten für die Anordnung von Massnahmen zur Verhinderung von Gewalttätigkeiten anlässlich bestimmter Veranstaltungen nötig sind. Die Empfänger dieser Daten dürfen diese nur im Rahmen des Vollzuges der Massnahmen an Dritte weitergeben.

Art. 34e Abs. 1 und 3

1) Personenbezogene Daten dürfen solange bearbeitet werden, als sie für die Aufgabenerfüllung erforderlich sind, längstens aber bis zum Ablauf der durch die Regierung mit Verordnung festgelegten Aufbewahrungsdauer; sie sind danach zu löschen.

3) Besteht berechtigter Grund zur Annahme, dass eine Sperrung oder Löschung die schutzwürdigen Interessen der betroffenen Person beeinträchtigen

würde, so werden die personenbezogenen Daten lediglich gekennzeichnet und die Bearbeitung eingeschränkt. Gekennzeichnete Daten dürfen nur für den Zweck bearbeitet werden, der ihrer Sperrung oder Löschung entgegenstand.

Art. 34f

*Aufgehoben.*

Art. 34g Abs. 1 und 2

1) Jede Person kann bei der Landespolizei nach Massgabe der Art. 52 des Datenschutzgesetzes Auskunft über die polizeilichen Daten, die ihre Person betreffen, verlangen. Vorbehalten bleibt Art. 34h.

2) Über Auskunftsgesuche betreffend personenbezogene Daten, die die Landespolizei im Rahmen der internationalen Polizeikooperation verarbeitet, entscheidet die Landespolizei nach Rücksprache mit der ersuchenden Behörde. Das Untersuchungsgeheimnis muss gewahrt bleiben.

Art. 34h Abs. 1, 3, 4, 6 und 7

1) Jede Person kann bei der Datenschutzstelle verlangen, dass diese prüfe, ob bei der Landespolizei rechtmässig personenbezogene Daten im Rahmen des Staatsschutzes (Art. 2 Abs. 2) über sie bearbeitet werden. Die Datenschutzstelle teilt der Gesuch stellenden Person in einer stets gleich lautenden Antwort mit, dass in Bezug auf sie entweder keine personenbezogene Daten unrechtmässig verarbeitet werden oder dass sie bei Vorhandensein allfälliger Fehler in der Datenverarbeitung eine Empfehlung zu deren Behebung verfügt habe.

3) Bevor nach Abs. 1 vorgegangen wird, hat die Landespolizei zu prüfen, ob ein überwiegendes Geheimhaltungsinteresse besteht und ob vorhandene perso-

nenbezogenen Daten noch benötigt werden. Besteht kein überwiegendes Geheimhaltungsinteresse, ist unverzüglich Auskunft nach Massgabe von Art. 34g zu erteilen.

4) Der Landespolizei steht gegen Entscheidungen der Datenschutzstelle im Zusammenhang mit der Überprüfung nach Abs. 1, die auch die Offenlegung der personenbezogenen Daten beim Fehlen eines überwiegenden Geheimhaltungsinteresses beinhalten können, Beschwerde an den Verwaltungsgerichtshof zu.

6) Gesuch stellenden Personen, denen nicht bereits nach Massgabe von Art. 34g Auskunft erteilt worden ist und über die zum Prüfzeitpunkt keine personenbezogenen Daten im Sinne des Abs. 1 verarbeitet worden sind, wird innert 12 Monaten nach Gesuchseinreichung, allen anderen Personen, die ein Auskunftsgesuch gestellt haben und die als solche bei der Datenschutzstelle erfasst worden sind, beim Dahinfallen der entsprechenden Geheimhaltungsinteressen, spätestens wenn die personenbezogenen Daten nicht mehr benötigt werden, nach Massgabe des Art. 34g Auskunft erteilt.

7) Die Datenschutzstelle kann auch ohne Anlassfall die Datenverarbeitung im Rahmen des Staatsschutzes (Art. 2 Abs. 2) bei der Landespolizei auf ihre Rechtmässigkeit hin überprüfen.

Art. 34i

*Aufgehoben.*

Art. 35 Abs. 1, Abs. 3 Bst. c, Abs. 4 und 6

1) Die Landespolizei kann ausländische Sicherheitsbehörden und -organisationen um Übermittlung von personenbezogenen Daten oder um Vor-

nahme anderer Amtshandlungen ersuchen, wenn dies zur Erfüllung ihrer Aufgaben erforderlich ist.

3) Die Leistung von Amtshilfe hat zu unterbleiben, wenn Grund zur Annahme besteht dass:

c) schutzwürdige Interessen der betroffenen Person oder Dritter verletzt werden, insbesondere wenn im Empfängerstaat jene Rechte verletzt werden, welche die Konvention vom 4. November 1950 zum Schutze der Menschenrechte und Grundfreiheiten gewährt oder wenn geeignete Garantien nach Art. 74 des Datenschutzgesetzes für ein angemessener Datenschutz nicht gewährleistet wäre; vorbehalten bleibt Art. 75 des Datenschutzgesetzes;

4) Personenbezogene Daten, die an ausländische Sicherheitsbehörden oder -organisationen übermittelt worden sind, dürfen nur mit vorheriger Zustimmung der Landespolizei zu anderen als den der Übermittlung zugrunde liegenden Zwecken verwendet werden. Dies ist der ersuchenden Stelle mitzuteilen. Die Zustimmung ist nur zu geben, wenn diese Daten auch zu diesem Zweck hätten übermittelt werden dürfen.

6) Die Landespolizei hat einer ausländischen Sicherheitsbehörde oder -organisation mitzuteilen, wenn personenbezogene Daten, die an diese übermittelt wurden, unrichtig oder unrechtmässig verarbeitet wurden und deshalb richtig zu stellen oder zu löschen sind.

Art 35a Abs. 1 Bst. a und Abs. 2 Einleitungssatz und Bst. a.

1) Die Landespolizei kann Amtshilfe leisten durch:

a) die Übermittlung von personenbezogenen Daten, einschliesslich besonderer Kategorien personenbezogener Daten, wie insbesondere genetische Daten, biometrische Daten zur eindeutigen Identifizierung einer natürlichen Person und Gesundheitsdaten, und Daten aus dem Profiling;

2) Die Beschaffung von personenbezogenen Daten zum Zwecke der Amtshilfe nach Abs. 1 Bst. a ist nur zulässig durch:

a) Verwenden von personenbezogenen Daten, die die Landespolizei in Erfüllung ihrer Aufgaben verarbeitet hat;

Art. 35p

*Datenübermittlung an einen Drittstaat oder eine internationales Organisation*

Die Landespolizei kann personenbezogene Daten nach Massgabe der Art. 73 bis 75 des Datenschutzgesetzes einer zuständigen Behörde eines Drittstaates oder einer internationalen Organisation übermitteln.

Art. 35q

*Übermittlung von personenbezogenen Daten an in Drittstaaten niedergelassene Empfänger*

An in Drittstaaten niedergelassene Empfänger, die nicht für die Erfüllung von Aufgaben nach Art. 2 zuständig sind, darf die Landespolizei personenbezogene Daten nur in besonderen Einzelfällen und nur nach Massgabe von Art. 76 des Datenschutzgesetzes übermitteln.

## II.

## Inkrafttreten

Dieses Gesetz tritt gleichzeitig mit dem Gesetz vom … über die Abänderung des Datenschutzgesetzes in Kraft.