Musterhandbuch Öffentliches Recht

herausgegeben von

Dr. Wilhelm Bergthaler
Rechtsanwalt in Wien
Hon.-Prof. an der Universität Linz

DDr. Christoph Grabenwarter
Univ.-Prof. an der Wirtschaftsuniversität Wien
Mitglied des Verfassungsgerichtshofes

BESONDERER TEIL
11. Lieferung

Datenschutzrecht

verfasst von

Dr. Rainer Knyrim
Rechtsanwalt in Wien

Wien 2014
Manzsche Verlags- und Universitätsbuchhandlung

ISBN 978-3-214-15841-5

Druck: Ferdinand Berger & Söhne Ges. m. b. H., 3580 Horn

Datenschutzrecht

Rainer Knyrim

Literatur:

Altenburger/Kneihs, Schriftsätze an den VfGH und VwGH[2] (2009); *Bauer/Reimer,* Handbuch Datenschutzrecht (2009); *Dammann/Simitis,* EG-Datenschutzrichtlinie (1997); *Dohr/Pollirer/Weiss/Knyrim,* Kommentar Datenschutzrecht[2] (2010); *Drobesch/Grosinger,* Das neue Österreichische Datenschutzgesetz (2000); *Duschanek/Rosenmayr-Klemenz,* Datenschutzgesetz 2000 (2000); *Jahnel,* Begriff und Arten von personenbezogenen Daten, in *Jahnel* (Hrsg), Datenschutzrecht und E-Government. Jahrbuch 2008 (2008); *Jahnel,* Handbuch Datenschutzrecht (2010); *Knyrim,* Datenschutzrecht[2] (2012); *Knyrim,* Datenübermittlung in Drittländer: Standardvertragsklauseln der Europäischen Kommission, AnwBl 2001, 634; *Knyrim,* Outsourcing und Datenschutzrecht: Achtung, die Welt ist flach, ecolex 2009, 85; *Knyrim/Horn,* Datenschutzverfahren nach der neuen Verwaltungsgerichtsbarkeit, in *Jahnel* (Hrsg), Datenschutzrecht. Jahrbuch 2013 (2013) 191; *Knyrim/Leissler,* Die Datenschutzgesetznovelle 2010 – ein Überblick, ecolex 2010, 29; *Knyrim/Pawelka,* Datenschutzrechtliche Meldeprozesse und die Einführung von DVR-Online, Compliance Praxis 4/2011, 26; *Knyrim/Pawelka,* Datenverarbeitungsregister-Online: Anleitung und erster Erfahrungsbericht, Compliance Praxis 2/2013, 36; *Mayer-Schönberger/Brandl,* Datenschutzgesetz[2] (2006); *Pollirer/Weiss/Knyrim,* Datenschutzgesetz 2000[2] (2014); *Raschauer,* Datenschutzrecht 2010 (2011); *Twardosz,* Die erfolgreiche VwGH-Beschwerde (2010).

Inhaltsübersicht

I. Grundprinzipien des Datenschutzes

1 § 1 Abs 1 DSG 2000 enthält nicht nur das Grundrecht auf Datenschutz, sondern schreibt auch gleichzeitig die Grundprinzipien des Datenschutzes fest. Zusätzlich zu den in § 1 Abs 1 DSG 2000 enthaltenen Grundprinzipien wird das Grundrecht auf Datenschutz in § 1 Abs 2 DSG 2000 noch weiter ausgestaltet. **Voraussetzung für die Anwendbarkeit** des § 1 DSG 2000 ist, dass überhaupt **personenbezogene Daten vorliegen.**

2 Aus § 1 Abs 1 und 2 DSG 2000 lässt sich grob folgendes Prinzip ableiten:

Jegliche Datenanwendung ist an Regeln gebunden (insb Zweckbestimmung), ansonsten ist sie unzulässig.

Dies bedeutet, dass man bei jeder Datenanwendung zunächst Gründe für ihre Zulässigkeit finden muss.

3 Selbst dann, wenn die Einschränkung des Grundrechts zulässig ist, darf der Eingriff nur in der gelindesten zum Ziel führenden Art vorgenommen werden **(Verhältnismäßigkeitsgrundsatz).**

4 Das Grundrecht auf Datenschutz des § 1 DSG 2000 beinhaltet in Abs 3 auch verschiedene **verfassungsgesetzliche Rechte der Betroffenen,** nämlich

- das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden;
- das Recht auf Richtigstellung unrichtiger Daten und das
- Recht auf Löschung unzulässigerweise verarbeiteter Daten.

II. Sachlicher Anwendungsbereich des DSG 2000

5 Das DSG 2000 schützt, wie aus dem oben beschriebenen Grundrecht auf Datenschutz in § 1 Abs 1 DSG 2000 hervorgeht, personenbezogene Daten von jedermann.

Mit jedermann ist der Betroffene gemeint, also jene Person, deren Daten verarbeitet oder übermittelt werden sollen. Betroffen kann aber nicht nur eine **natürliche Person,** also ein bestimmter Mensch, sein, sondern auch eine **juristische Person oder Personengemeinschaft.** Das Datenschutzgesetz ist nicht nur auf automationsunterstützt verarbeitete Daten, sondern auch auf manuell verarbeitete Dateien[1] nach § 58 DSG 2000 anwendbar.

III. Definitionen

Zusätzlich zu den oben bereits erklärten Begriffen sind die Definitionen der folgenden termini technici des DSG 2000 von wesentlicher Bedeutung:

A. Daten und sensible Daten

Die Datenschutzrichtlinie (RL 95/46/EG ABl L 1995/281, 31) unterscheidet zwischen „normalen" Daten und „sensiblen" Daten. Diese Unterscheidung wurde im DSG 2000 wie folgt umgesetzt:

1. „Normale" personenbezogene und indirekt personenbezogene Daten

„Normale" Daten, auch „personenbezogene" Daten, sind nach § 4 Z 1 DSG 2000 Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. **6**

Angaben können sämtliche Informationen sein, die mit einer Person oder einem Unternehmen in Verbindung stehen oder gebracht werden können, zB Name, Firmenname, Geburtsdatum, Adresse, Einkommen, Lebenslauf, Umsatz, Lieblingsfarbe, Kleidergröße, aber auch Werturteile. Ebenso fallen auch Bild- und Tondokumente darunter wie zB Fotos, Mitschnitte von akustischen Abhöranlagen oder Videoaufnahmen einer Überwachungskamera. Auch Standortdaten, die zB bei Mobiltelefonen oder GPS „anfallen", zählen dazu. **7**

Ist der Personenbezug der Daten so, dass ein Auftraggeber, Dienstleister oder Empfänger einer Übermittlung die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann, dann sind die Daten nach § 4 Z 1 DSG 2000 **indirekt personenbezogene Daten.**[2] **8**

Wenn die **Identität** des Betroffenen **überhaupt nicht mehr feststellbar** ist, so sind die Daten anonym. Da anonyme Daten keinen Personenbezug aufweisen, sind die **Regelungen des DSG 2000 nicht auf sie anwendbar.** **9**

2. Sensible Daten

Die Datenschutzrichtlinie hat eine besondere Kategorie von Daten geschaffen, die sog sensiblen Daten nach § 4 Z 2 DSG 2000, die besonders schutzwürdig sind: rassische **10**

[1]) § 4 Z 6 DSG 2000.

[2]) Ausführlich dazu *Bergauer,* Indirekt personenbezogene Daten – datenschutzrechtliche Kuriosa, in *Jahnel,* Datenschutzrecht. Jahrbuch 2011 (2011) 55 ff.

und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder Sexualleben.

11 Die Zulässigkeit der Verwendung sensibler Daten wurde im DSG 2000 sehr eingeschränkt, sie unterliegen einem allgemeinen Verwendungsverbot und dürfen nur aus den in § 9 DSG 2000 genannten Gründen verwendet werden.

B. Datenanwendung

12 Eine Datenanwendung ist nach § 4 Z 7 DSG 2000 die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte (Z 8), die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen (automationsunterstützte Datenanwendung).

C. Die drei „Akteure"

Das DSG 2000 kennt drei „Akteure", nämlich den Betroffenen, den Auftraggeber und den Dienstleister:

13 **Betroffener** ist nach § 4 Z 3 DSG 2000 jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet werden, also immer jene Person oder jenes Unternehmen, deren Daten verwendet werden.

14 **Auftraggeber** sind nach § 4 Z 4 DSG 2000

- natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe,
- wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verwenden (Z 8),
- und zwar unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen.

15 **Dienstleister** sind nach § 4 Z 5 DSG 2000 natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden (Z 8).

16 Der Auftraggeber bleibt im Gegensatz zum Dienstleister immer „Herr der Daten" und ist für die Einhaltung der Qualitätsgrundsätze (§ 6 DSG 2000), die Überprüfung der Zulässigkeitsvoraussetzungen (§ 7 DSG 2000), die Einhaltung der schutzwürdigen Geheimhaltungsinteressen (§§ 8 und 9 DSG 2000), die Prüfung der Zulässigkeitskriterien für den Einsatz eines Dienstleisters (§§ 10 und 11 DSG 2000), die Beantragung einer Genehmigung für genehmigungspflichtige Übermittlungen und Überlassungen von Daten in das Ausland (§ 13 DSG 2000), die Einhaltung der Meldepflichten (§§ 17 ff DSG 2000) uvm verantwortlich.

17 Neben den drei Akteuren kommt bei Datenübermittlungen auch noch eine vierte Person hinzu, nämlich der **Empfänger** der Daten, der, da er zu den drei Akteuren Außenstehender ist, oft auch „Dritter" genannt wird.

IV. Zur Meldepflicht von Datenanwendungen

Die Kontrolle der Einhaltung der datenschutzrechtlichen Meldepflichten obliegt der Datenschutzbehörde.[3] Für die Einhaltung der Meldepflichten ist der Auftraggeber verantwortlich. Dieser muss daher zunächst anhand der gesetzlichen Regelungen (§§ 17 ff DSG 2000) und insbes anhand der Standard- und Musterverordnung (StMV 2004) prüfen, ob ihn eine Meldepflicht trifft. **18**

Um die Zulässigkeit von Datenverwendungen sicherzustellen, hat sich derjenige Auftraggeber, der sich entschieden hat, personenbezogene Daten zu verwenden, vor Inbetriebnahme der Datenanwendung bei der Datenschutzbehörde zu registrieren, wenn ihn eine Meldepflicht trifft (§§ 17 ff DSG 2000, StMV 2004). Anschließend wird dem Auftraggeber eine eindeutige Identifikationsnummer („DVR-Nummer") zugewiesen, die in der Folge auf allen Mitteilungen an Betroffene angeführt werden muss (§ 25 Abs 1 2. Satz DSG 2000). **19**

→ *Siehe Muster BT/DSR-2: Meldung eines Auftraggebers.*

Gleichzeitig hat er bei der Datenschutzbehörde eine Meldung der von ihm betriebenen Datenanwendungen zu erstatten.

→ *Siehe Muster BT/DSR-3: Meldung einer Datenanwendung.*

Die Meldung des Auftraggebers kann nur gemeinsam mit der Meldung der ersten Datenanwendung erfolgen.[4] Es ist daher entgegen häufiger Ansicht nicht möglich, eine DVR-Nummer bei der Datenschutzbehörde zu beantragen, wenn vom Auftraggeber keine melde- oder genehmigungspflichtigen Datenanwendungen betrieben werden. Selbstverständlich ist in diesem Fall auch keine DVR-Nummer in Geschäftspapieren oder auf der Website des Auftraggebers anzuführen. **20**

Die DVR-Meldung hat die vom Auftraggeber verwendeten personenbezogenen Daten, deren jeweils zugeordneten betroffenen Personenkreis sowie all jene vom Auftraggeber verschiedenen Personen, die diese Daten ebenfalls mit Eigeninteresse nutzen (Übermittlungsempfänger), unter Angabe der jeweiligen Rechtsgrundlagen zu enthalten. Zusätzlich hat der Auftraggeber Angaben zu den von ihm ergriffenen Maßnahmen zu machen, welche die Sicherheit der Daten gewährleisten sollen (Datensicherheitsmaßnahmen).

→ *Siehe Muster BT/DSR-3.*

Nach § 17 Abs 1 letzter Satz DSG 2000 müssen Änderungen einer bereits registrierten Datenanwendung vor ihrer Durchführung ebenfalls gemeldet werden. Dies bedeutet, dass die Meldung beim Datenverarbeitungsregister immer aktuell zu halten ist. **21**

Die Meldung selbst erfolgte bis 31. 8. 2012 mittels Formularen, die per Post, Telefax oder E-Mail an die Datenschutzkommission übermittelt werden konnten. Seit 1. 9. 2012 sind DVR-Meldungen grundsätzlich über die Internetanwendung **„DVR-Online"** einzubringen.[5] Nur bei der Meldung manueller Dateien, also Dateien, die ohne Automations- **22**

[3]) Zur Prüfung, ob Meldepflicht vorliegt, s näher bei *Knyrim,* Datesnchutzrecht[2] Kap 3.
[4]) Siehe auch § 21 DSG 2000.
[5]) § 17 Abs 1a DSG 2000.

unterstützung geführt werden, und bei einem längeren technischen Ausfall der Internetanwendung „DVR-Online" ist eine Meldung in nicht-elektronischer Form zulässig. Die für eine nicht-elektronische Meldung erforderlichen Formulare sind im Falle der Meldung einer manuellen Datei bei der Datenschutzbehörde anzufordern, im Falle eines längeren technischen Ausfalls der Internetanwendung „DVR-Online" werden sie auf der Internetseite der Datenschutzbehörde allgemein zur Verfügung gestellt.

Der **Zugang** zu DVR-Online erfolgt grundsätzlich mittels Signaturkarte oder Handy-Signatur unter der Internetadresse https://dvr.dsk.gv.at/. Alternativ ist eine Anmeldung über das Unternehmensserviceportal (USP)[6], das Bürgerportal[7] oder für Behörden über den Behördenportalverbund möglich. Für die Anmeldung in Vertretung eines Dritten muss bei der Anmeldung das Auswahlfeld „In Vertretung anmelden" ausgewählt werden. Nach erfolgreicher Anmeldung werden dem Nutzer sämtliche für ihn elektronisch eingerichtete Vertretungsbefugnisse angezeigt. Die Vertretungsbefugnis kann auf der Website der Datenschutzbehörde als Stammzahlenregisterbehörde[8] oder über das Unternehmensserviceportal (USP) erteilt werden.

Mittels DVR-Online können **Auftraggeber angelegt, geändert und gestrichen sowie Datenanwendungen und Informationsverbundsysteme gemeldet, beantragt, geändert und gestrichen** werden. **Videoüberwachungen** unterliegen ebenfalls der Meldepflicht für Datenanwendungen gem §§ 17 ff DSG 2000[9] und sind daher ebenfalls über DVR-Online zu beantragen. Andere Anträge, wie **Anträge auf Genehmigung internationaler Datenüberlassungen und -übermittlungen** können nicht mittels DVR-Online eingebracht werden, sondern sind **in Papierform oder per E-Mail** zu beantragen.

→ *Siehe Muster BT/DSR-4 und BT/DSR-5.*

V. Zulässigkeit der Verarbeitung von Daten

23 Die Frage der formellen Meldepflicht der Datenanwendung (§§ 17 ff DSG 2000, StMV 2004) ist von der Frage zu trennen, ob die Verwendung von Daten inhaltlich (materiell) zulässig ist. Bei der Prüfung der Zulässigkeit einer Datenanwendung ist zunächst die Zulässigkeit der Verwendung der Daten zu prüfen, dann kann die Zulässigkeit der Übermittlung geprüft werden.

24 Die Prüfung, ob eine Datenverarbeitung zulässig ist, muss daher zunächst mit der **Feststellung beginnen, ob diese überhaupt zulässig ist.**

Eine Datenanwendung ist nach § 7 Abs 1 DSG 2000 nur soweit zulässig, als

- Zweck und Inhalt der Datenanwendung
- von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und
- die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen (§§ 8 und 9 DSG 2000).

---

[6]) www.usp.gv.at [zuletzt abgerufen am 7. 1. 2014].
[7]) www.help.gv.at [zuletzt abgerufen am 7. 1. 2014].
[8]) www.stammzahlenregister.gv.at/site/5983/default.aspx [zuletzt abgerufen am 7. 1. 2014].
[9]) § 50 c Abs 1 DSG 2000.

Das letzte Kriterium, welches das DSG 2000 hinsichtlich der Zulässigkeit einer Datenanwendung, somit sowohl einer Datenverarbeitung als auch einer Datenübermittlung, in § 7 Abs 3 aufstellt, ist, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und dass die Grundsätze des § 6 eingehalten werden. 25

VI. Zulässigkeit der Datenübermittlung

A. Übermittlung innerhalb des Unternehmens, Österreichs und des EWR

1. Arten von Übermittlungen

Nach der Definition des § 4 Z 12 DSG 2000 ist eine Datenübermittlung 26

- die **Weitergabe** von Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister,
- das **Veröffentlichen** von Daten,
- die **Verwendung** von Daten für ein anderes Aufgabengebiet des Auftraggebers.

Die Weitergabe der Daten an den Betroffenen selbst ist keine Übermittlung im Sinn des § 4 Z 12 DSG 2000. Auch die Weitergabe der Daten an einen Dienstleister (zB externe Buchhalter) ist keine Datenübermittlung, sondern eine Datenüberlassung nach § 4 Z 11 DSG 2000. 27

Bei der Übermittlung von Daten an Dritte macht es keinen Unterschied, ob sich dieser Dritte in Österreich oder innerhalb des EWR befindet. Lediglich bei Übermittlungen an Auftraggeber außerhalb des EWR sind besondere Voraussetzungen zu erfüllen (s Rz 34 ff). 28

Eine **Veröffentlichung** von Daten kann zB durch Abdruck in einem Register, Pressemitteilungen, aber auch durch die Veröffentlichung auf einer Homepage im Internet geschehen.[10] Bei der Veröffentlichung von Daten im Internet – sei es die Angabe von Mitarbeitern eines Unternehmens oder der Gewinner der letzten Vereinsmeisterschaften – wird oft übersehen, dass es sich dabei um Übermittlungen handelt, für die die Zulässigkeit geprüft werden muss. 29

Besonders zu beachten ist auch die dritte Übermittlungsform, die innerhalb eines Unternehmens auftreten kann, nämlich die Übermittlung zwischen **verschiedenen Aufgabengebieten desselben Auftraggebers.** Ein „Aufgabengebiet" ist dabei eines von mehreren Tätigkeitsfeldern eines Auftraggebers, das in seinem Umfang nach der Verkehrsauffassung geeignet ist, für sich alleine den gesamten Geschäftsbereich eines Auftraggebers zu bilden. Im privaten Unternehmensbereich ist ein Aufgabengebiet in etwa mit dem Umfang einer Gewerbeberechtigung gleichzusetzen.[11] 30

Liegt eine Datenübermittlung vor, so darf diese nur unter bestimmten Voraussetzungen durchgeführt werden. 31

[10]) EuGH 6. 11. 2003, C-101/01, *Lindqvist,* Slg 2003, I-12971.
[11]) ErläutRV 1613 BlgNR 20. GP 39 (zu § 4 Z 12 DSG 2000).

2. Zulässigkeit der Übermittlung

32 Zuvor wurde festgestellt, dass bei jeder Datenverarbeitung zunächst vom Grundsatz auszugehen ist, dass die Zulässigkeit geprüft werden muss. Dies gilt auch für jede Datenübermittlung, denn § 7 Abs 2 DSG 2000 schreibt vor, dass Daten nur in bestimmten Ausnahmefällen übermittelt werden dürfen.

Nach § 7 Abs 2 DSG 2000 dürfen Daten nur dann übermittelt werden, wenn

1. sie aus einer gemäß § 7 Abs 1 DSG 2000 zulässigen Datenanwendung stammen und
2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht – im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und
3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

33 § 7 Abs 3 DSG 2000 gilt gleichermaßen für eine Datenverarbeitung wie für eine Datenübermittlung und besagt, dass Eingriffe in das Grundrecht auf Datenschutz **nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln** erfolgen dürfen und dass die Grundsätze des § 6 DSG 2000 einzuhalten sind. So auch schon in Rz 25.

B. Übermittlung an Auftraggeber außerhalb des EWR

34 § 12 Abs 1 DSG 2000 bestimmt, dass die Übermittlung und Überlassung von Daten an Empfänger in Mitgliedstaaten des Europäischen Wirtschaftsraums (EWR) keinen Beschränkungen iSd § 13 DSG 2000 unterworfen ist. Übermittlungen und Überlassungen an Empfänger außerhalb des EWR bedürfen hingegen einer **Genehmigung der Datenschutzbehörde.** Davon gibt es jedoch eine **Reihe von Ausnahmen,** wie insbesondere jene des **§ 12 Abs 3 DSG 2000.**

1. Gleichgestellte Drittstaaten

35 Ebenso bedarf eine Datenweitergabe (Übermittlung oder Überlassung) an Empfänger in gleichgestellten Drittstaaten mit angemessenem Datenschutz nach § 12 Abs 2 DSG 2000 **keiner Genehmigung** der Datenschutzbehörde. Welche Drittstaaten als gleichgestellt gelten, ergibt sich aus der Datenschutzangemessenheits-Verordnung (DSAV)[12]: **Andorra, Argentinien, Färöer Inseln, Guernsey, Isle of Man, (unter bestimmten Voraussetzungen) Israel**[13]**, Jersey, (unter bestimmten Voraussetzungen) Kanada**[14]**, Neuseeland, Schweiz und Uruguay.**

36 Weiters ist eine Datenweitergabe an einzelne Unternehmen in den **USA** genehmigungsfrei, die sich zu den so genannten **„Safe Harbor"-Bestimmungen** des US-Handelsministeriums verpflichtet haben.[15] Ist ein US-Unternehmen vom US Department of

---

[12]) BGBl II 1999/521 idF BGBl II 2013/150.
[13]) B 2011/61/EU der Kommission vom 31. 1. 2011, ABl L 2011/27, 39.
[14]) E 2002/2/EG der Kommission vom 20. 12. 2001, ABl L 2002/2, 13.
[15]) http://safeharbor.export.gov/list.aspx [zuletzt abgerufen am 7. 1. 2014].

Commerce als „Safe Harbor" zertifiziert worden, so ist nach der Entscheidung der EU-Kommission[16] eine Datenübermittlung von einem Datenübermittler in der EU **an dieses US-Unternehmen ohne weiteres zulässig.** Jeder, der Daten von der EU an ein US-Unternehmen übermitteln möchte, braucht daher nur die Online-Liste des US Department of Commerce unter http://safeharbor.export.gov/list.aspx einsehen, um zu wissen, ob sich dieses US-Unternehmen den „Safe Harbor"-Bestimmungen unterworfen hat und er daher ohne weiteres Daten an dieses übermitteln kann oder nicht.

2. Standardvertragsklauseln

37 Art 26 Abs 2 Datenschutzrichtlinie ermöglicht es den Mitgliedstaaten, eine Übermittlung oder eine Kategorie von Übermittlungen personenbezogener Daten in ein Drittland ohne angemessenes Schutzniveau zu genehmigen, wenn der für die Verarbeitung Verantwortliche ausreichende Garantien hinsichtlich des Schutzes der Privatsphäre, der Grundrechte und der Grundfreiheiten der Personen sowie hinsichtlich der Ausübung der damit verbundenen Rechte bietet (s Kapitel VI.B.3 unten). Diese Garantien können sich dabei insbesondere aus entsprechenden Vertragsklauseln ergeben. Dazu sieht Art 26 Abs 4 Datenschutzrichtlinie vor, dass die Kommission befinden kann, dass bestimmte Standardvertragsklauseln ausreichende Garantien nach Absatz 2 bieten können. Genau dies hat die Kommission in zwei Entscheidungen[17] getan, in denen sie zwei Versionen von Standardvertragsklauseln festlegte, die es Datenübermittlern in Mitgliedstaaten ermöglichen sollen, Daten an Datenempfänger außerhalb des EWR zu übermitteln, die diese Klauseln unterschrieben haben.

→ *Siehe Muster BT/DSR-4 und BT/DSR-5.*

38 Die erste Version der Standardvertragsklauseln vom 15. 6. 2001[18] (s Muster *BT/DSR-5*) ist nur **auf eine Datenübermittlung iSd § 4 Z 12 DSG 2000 anwendbar,** nicht jedoch auf eine bloße Datenüberlassung an einen Dienstleister in einem Drittstaat iSd § 4 Z 11 DSG 2000, also zB im Falle des Auslagerns einer betrieblichen Datenverarbeitung in ein Drittland. Für diesen Fall gibt es eine zweite Version der Standardvertragsklauseln vom 5. 2. 2010, die so genannten **„Auftragsverarbeiter-Standardvertragsklauseln".**[19] Diese gelten ausdrücklich nur für die Übermittlung an Datenverarbeiter in Drittstaaten, die als Auftragsverarbeiter fungieren (s Muster *BT/DSR-4*).[20] Im Jahr 2010 wurden diese Standardvertragsklauseln geändert und um Unterauftragsverarbeiter erweitert.

---

16) E 2000/520/EG der Kommission vom 26. 7. 2000, ABl L 2000/215, 7 idF ABl L 2001/115, 14.

17) E 2001/497/EC der Kommission vom 15. 6. 2001, ABl L 2001/181, 19 und B 2010/87/EU der Kommission vom 5. 2. 2010, ABl L 2010/39, 5 (Die alten Standardvertragsklauseln sind außer Kraft und sollen nicht mehr verwendet werden: E 2002/16/EC der Kommission vom 27. 12. 2001, ABl L 2002/6, 52).

18) E 2001/497/EC der Kommission vom 15. 6. 2001, ABl L 2001/181, 19.

19) E 2010/87/EU der Kommission vom 5. 2. 2010, ABl L 2010/39, 5.

20) E 2002/16/EC der Kommission vom 27. 12. 2001, Artikel 2.

39 Zu beachten ist, dass die Standardvertragsklauseln ein Vertragswerk sind, die einen Ist-Zustand abbilden. Bei Änderung der Gegebenheiten sind diese daher wieder neu abzuschließen, was besonders bei einer größeren Zahl von Vertragspartnern einen großen Aufwand bedeutet. Für Konzerne wurde daher das Modell der „Binding Corporate Rules" entwickelt.[21]

3. Genehmigung durch die Datenschutzbehörde

40 Wenn weder einer der materiellen Ausnahmegründe des § 12 Abs 3 DSG 2000 vorliegt noch der Drittstaat, in dem sich der Datenempfänger befindet, nach § 12 Abs 2 DSG 2000 gleichgestellt wurde, muss die Datenübermittlung durch die Datenschutzbehörde mittels individueller Prüfung **im Einzelfall genehmigt** werden.

Die Genehmigung einer Datenübermittlung oder Datenüberlassung ins EWR-Ausland ist nach § 13 Abs 2 DSG 2000 unter Beachtung der gemäß § 55 Z 2 ergangenen Kundmachungen zu erteilen,

1. wenn die Voraussetzungen des § 12 Abs 5 vorliegen und
2. der Auftraggeber glaubhaft macht, dass – insbesondere durch vertragliche Zusicherungen des Empfängers – die schutzwürdigen Geheimhaltungsinteressen auch im Empfängerstaat gewahrt sind. Hierunter fallen die **Standardvertragsklauseln der EU-Kommission** (s Rz 37 – 39). Darüber hinaus kann jede andere vertragliche Vereinbarung hinsichtlich des Datenschutzes in einem Vertrag diesem Punkt und damit einer Genehmigung durch die Datenschutzbehörde dienlich sein. Es ist daher sinnvoll, in internationalen Verträgen, die Datenübermittlungen vorsehen, die nicht nur der Vertragserfüllung selbst dienen, vertragliche Vereinbarungen zum Datenschutz aufzunehmen. **Je mehr diese den Standardvertragsklauseln angenähert sind, desto eher wird die Datenschutzbehörde die Datenübermittlung genehmigen.** Am besten ist jedoch die Verwendung des Originaltextes der Klauseln.

41 Bei einer Genehmigung durch die Datenschutzbehörde ist zu beachten, dass die Genehmigung für einen internationalen Datenverkehr sowohl im **Falle einer Übermittlung** von Daten an einen Auftraggeber in einem Drittstaat **als auch für die Überlassung** von Daten an einen Dienstleister in einem Drittstaat einzuholen ist, soweit nicht eine der Ausnahmen der §§ 12 und 13 DSG 2000 vorliegt.

42 Auf das Genehmigungsverfahren vor der Datenschutzbehörde ist das Allgemeine Verwaltungsverfahrensgesetz (AVG) anzuwenden. Das Genehmigungsverfahren wird auf Antrag eingeleitet, dh der Auftraggeber oder Dienstleister, der Daten in Drittstaaten übermitteln möchte, muss bei der Datenschutzbehörde einen Antrag stellen. Der Antrag ist formlos, sollte aber Angaben über die übermittelten Datenarten, den Zweck der Übermittlung und die Empfänger bzw die Angabe, in welche Drittstaaten übermittelt wird, enthalten.

43 Eine Unterlassung der Genehmigung kann nach § 52 Abs 2 Z 2 DSG 2000 eine Verwaltungsstrafe bis EUR 10.000,– nach sich ziehen.

---

[21]) Siehe *Knyrim,* Datenschutzrecht[2] 132 f.

VII. Rechtsschutz in Datenschutzangelegenheiten

Der Rechtsschutz der Betroffenen ist im DSG 2000 grundsätzlich zweigeteilt: **44**

- Ansprüche Betroffener gegen Auftraggeber des öffentlichen Bereichs sind vor der Datenschutzbehörde geltend zu machen, die darüber mit Bescheid entscheidet (§ 31 DSG 2000).
- Ansprüche Betroffener gegen Auftraggeber des privaten Bereichs sind bei den Zivilgerichten in einem Zivilprozess geltend zu machen (§ 32 DSG 2000).

Diese Trennung wird durch zwei Ausnahmen durchbrochen:

- Ein allgemeines Beschwerderecht der Betroffenen an die Datenschutzbehörde über Auftraggeber des öffentlichen und privaten Bereichs, damit diese ihre Kontrollbefugnisse ausübt (§ 30 Abs 1 DSG 2000)
- Ein Beschwerderecht der Betroffenen an die Datenschutzbehörde bei Verletzung ihres Auskunftsrechts auch durch private Auftraggeber (§ 31 Abs 1 DSG 2000)

Sämtlichen vorgenannten Ansprüchen, Beschwerden oder Klagen ist gemeinsam, **45** dass der Anspruch erlischt, wenn der Einschreiter sie nicht **binnen eines Jahres,** nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt. Bei Beschwerden, Eingaben oder Klagen nach Ablauf dieser Frist muss die Datenschutzbehörde bzw das angerufene Gericht zurückweisen (§ 34 Abs 1 DSG 2000).[22]

A. Kontrollbefugnisse der Datenschutzbehörde

Die Datenschutzbehörde kann im Fall eines begründeten Verdachtes auf Verletzung **46** von Rechten und Pflichten des Betroffenen die Datenanwendungen des Auftraggebers, über den sich der Betroffene beschwert hat, überprüfen. Sofern sich eine zulässige Eingabe nach § 30 Abs 1 DSG 2000 oder ein begründeter Verdacht nach § 30 Abs 2 DSG 2000 auf eine meldepflichtige Datenanwendung (Datei) bezieht, kann die Datenschutzbehörde die Erfüllung der Meldepflicht überprüfen und erforderlichenfalls nach §§ 22 und 22 a DSG 2000 vorgehen. Anzumerken ist, dass Datenanwendungen, die der Vorabkontrolle nach § 18 Abs 2 DSG 2000 unterliegen, auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden dürfen.

Zur Herstellung des rechtmäßigen Zustandes kann die Datenschutzbehörde, sofern nicht Maßnahmen nach §§ 22 und 22 a oder nach § 30 Abs 6 a DSG 2000 zu treffen sind, Empfehlungen aussprechen, für deren Befolgung erforderlichenfalls eine angemessene Frist zu setzen ist. Wird einer solchen Empfehlung innerhalb der gesetzten Frist nicht entsprochen, so kann die Datenschutzbehörde je nach Art des Verstoßes von Amts wegen nach § 30 Abs 6 DSG 2000 vorgehen. Liegt durch den Betrieb einer Datenanwendung eine wesentliche unmittelbare Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen (Gefahr im Verzug) vor, so kann die Datenschutzbehörde die Weiterführung der Datenanwendung mit Bescheid nach § 57 Abs 1 AVG untersagen.

[22]) Vgl *Jahnel,* Handbuch Datenschutzrecht Rz 9/1 ff.

B. Beschwerde an die Datenschutzbehörde

47 Erachtet sich ein Betroffener in seinen Rechten nach dem Datenschutzgesetz verletzt, so steht ihm die Möglichkeit offen, Beschwerde an die Datenschutzbehörde zu erheben. Die Möglichkeit der Ergebung einer Beschwerde nach § 31 DSG 2000 ist jedoch davon abhängig, ob es sich um einen Auftraggeber des öffentlichen oder des privaten Bereichs handelt.

→ *Siehe Muster BT/DSR-8 und BT/DSR-9.*

48 Die Datenschutzbehörde erkennt über Beschwerden von Personen oder Personengemeinschaften, die behaupten,

- in ihrem **Recht auf Auskunft** nach § 26 oder nach § 50 Abs 1 dritter Satz DSG 2000 oder
- in ihrem **Recht auf Darlegung einer automatisierten Einzelentscheidung** nach § 49 Abs 3 DSG 2000 verletzt zu sein,

soweit sich das Auskunftsverlangen (der Antrag auf Darlegung oder Bekanntgabe) nicht auf die Verwendung von Daten für Akte im Dienste der Gesetzgebung oder der Gerichtsbarkeit bezieht.

49 Die Datenschutzbehörde erkennt weiters über Beschwerden von Personen oder Personengemeinschaften, die behaupten,

- in ihrem **Recht auf Geheimhaltung** (§ 1 Abs 1 DSG 2000) oder
- in ihrem **Recht auf Richtigstellung** oder
- auf **Löschung** (§§ 27 und 28 DSG 2000) verletzt zu sein,

sofern der Anspruch nicht nach § 32 Abs 1 DSG 2000 vor einem Gericht geltend zu machen ist oder sich gegen ein Organ im Dienste der Gesetzgebung oder der Gerichtsbarkeit richtet.

50 Für Beschwerden über die behaupteten Verletzungen der Rechte eines Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung nach diesem Bundesgesetz ist die Datenschutzbehörde nur dann zuständig, wenn sich die Beschwerde gegen einen Auftraggeber des **öffentlichen Bereichs** richtet, ansonsten sind die Zivilgerichte berufen. Seit der DSG-Novelle 2010 hat die Beschwerde bestimmten inhaltlichen Erfordernissen nach § 31 Abs 3 DSG 2000 zu entsprechen, andernfalls wird die Beschwerde von der Datenschutzbehörde zurückgewiesen.

51 Soweit sich eine Beschwerde nach § 31 Abs 1 oder 2 DSG 2000 als berechtigt erweist, ist ihr Folge zu geben und die Rechtsverletzung festzustellen. Ist eine festgestellte Verletzung im Recht auf Auskunft (Abs 1) einem Auftraggeber des privaten Bereichs zuzurechnen, so ist diesem auf Antrag zusätzlich die – allenfalls erneute – Reaktion auf das Auskunftsbegehren in jenem Umfang aufzutragen, der erforderlich ist, um die festgestellte Rechtsverletzung zu beseitigen. Soweit sich die Beschwerde als nicht berechtigt erweist, ist sie abzuweisen. Die Entscheidung der Datenschutzbehörde erfolgt in Form eines Bescheides.

52 Durch die DSG-Novelle 2010 wurde § 31 a DSG 2000 neu eingefügt, der begleitende Maßnahmen im Beschwerdeverfahren vor der Datenschutzbehörde regelt.

C. Anrufung der Gerichte

Wie bereits festgestellt, muss ein Betroffener seine Ansprüche gegen **Auftraggeber des privaten Bereichs** – mit Ausnahme der Beschwerderechte nach §§ 30 und 31 Abs 1 DSG 2000 – nach § 32 DSG 2000 vor den Gerichten geltend machen. **53**

Der Betroffene hat, wenn der Auftraggeber bei der Verwendung seiner Daten gegen das DSG 2000 verstoßen hat, Anspruch auf Unterlassung und Beseitigung des rechtswidrigen Zustandes. Überdies kann das angerufene Gericht zur Sicherung von Unterlassungsansprüchen einstweilige Verfügungen erlassen. Daneben kann auch Schadenersatz nach § 33 DSG 2000 begehrt werden.

In Bezug auf Musterschriftsätze für diesbezügliche Klagen vor den Zivilgerichten wird auf Musterhandbücher für Schriftsätze im Zivilprozess verwiesen.[23] **54**

D. Einbringung einer Anzeige

Verletzt ein Auftraggeber bestimmte Strafbestimmungen (zB jene des StGB oder der §§ 51 oder 52 DSG 2000), so bietet sich einem Betroffenen die Möglichkeit, Anzeige bei der zuständigen Staatsanwaltschaft oder Bezirksverwaltungsbehörde einzubringen. **55**

Eine **Anzeige bei der Staatsanwaltschaft** kommt beispielsweise im Fall einer vorsätzlichen Datenbeschädigung nach § 126 a StGB, einer Denial-of-Service-Attacke nach § 126 b StGB oder einer Datenverwendung in Gewinn- oder Schädigungsabsicht nach § 51 DSG 2000 in Betracht. Opfer solcher Straftaten können sich im Verfahren als Privatbeteiligte anschließen und den ihnen durch die Straftat entstandenen Schaden oder die dadurch erlittene Beeinträchtigung direkt im Strafverfahren geltend machen. Das Opfer ist somit nicht auf einen separaten Zivilprozess angewiesen. Darüber hinaus haben Privatbeteiligte nach § 67 Abs 6 StPO über die Rechte der Opfer (§ 66 StPO) hinaus weitere Rechte, wie beispielsweise das Recht, die Aufnahme von Beweisen nach § 55 StPO zu beantragen, Beschwerde gegen die Einstellung des Verfahrens zu erheben oder das Verfahren als Subsidiarankläger fortzuführen.

Eine **Anzeige bei der Bezirksverwaltungsbehörde** ist beispielsweise im Fall der vorsätzlichen Verletzung des Datengeheimnisses nach § 15 DSG 2000, der unterlassenen oder mangelhaften Erfüllung der Meldepflichten bei der Datenschutzbehörde nach §§ 17 oder 50 c DSG 2000, der genehmigungslosen Weitergabe von Daten ins EWR-Ausland (zB durch Nutzung von Cloud-Diensten oder E-Mail-Diensteanbietern), bei Verletzung der Informationspflichten nach §§ 23 ff und 50 d DSG 2000 oder der gröblichen Außerachtlassung der erforderlichen Datensicherheitsmaßnahmen nach § 14 DSG 2000 möglich. In diesem Zusammenhang ist zu beachten, dass im Fall von juristischen Personen oder Personengesellschaften verwaltungsstrafrechtlich nur natürliche Personen verantwortlich sein können, die zur Vertretung nach außen berufen sind oder als verantwortliche Beauftragte bestellt wurden (§ 9 VStG). Juristische Personen oder Personengesellschaften haften jedoch neben diesen natürlichen Personen solidarisch für die verhängten Geldstrafen, für sonstige in Geld bemessene Unrechtsfolgen und für die Verfahrenskosten (§ 9 Abs 7 VStG).

[23]) ZB *Horn/Schöberl,* Mustersammlung Zivilverfahren (2012); *Ziehensack,* Schriftsätze für Rechtsanwälte – Streitiges Gerichtsverfahren (2012).

56 Der **Vorteil von Anzeigen** im Gegensatz zu Klagen ist, dass ein von der zuständigen Stelle eingeleitetes Verfahren in der Folge amtswegig durchzuführen ist und es somit zu keinen weiteren Belastungen der anzeigenden Person kommt. Nachteil von **Verwaltungsstrafverfahren** ist, dass die Person, die eine Anzeige eingebracht hat, im weiteren behördlichen Verfahren keine Parteistellung hat und den Verlauf des Verfahrens nicht weiter verfolgen oder kontrollieren kann. Es stehen ihr auch keine Rechtsmittel gegen Entscheidungen der Behörde oder gegen die Einstellung des Verfahrens offen. Anders ist dies in Bezug auf ein Strafverfahren zu beurteilen (vgl § 195 StPO).

→ *Siehe Muster BT/DSR-10.*

E. Beschwerde an das Bundesverwaltungsgericht

57 Neu für das Datenschutzrecht ist die im Zuge der Verwaltungsgerichtsbarkeits-Novelle 2012[24] geschaffene Möglichkeit der Erhebung des Rechtsmittels der **Beschwerde** gegen (Nicht-)Erledigungen der Datenschutzbehörde an das **Bundesverwaltungsgericht**[25]. Unter bestimmten Voraussetzungen ist in weiterer Folge auch eine Revision an den VwGH oder die Erhebung einer Beschwerde an den VfGH möglich (s *Grabenwarter/Lais,* Verfahren vor dem Verfassungsgerichtshof [AT/VfGH]).

58 **Beschwerdelegitimiert** in Bezug auf einen Bescheid ist jene Person, die in ihren Rechten verletzt zu sein behauptet. Hinsichtlich der Verletzung der Entscheidungspflicht ist dies nach Art 132 Abs 3 B-VG jene Person, die als Partei im Verwaltungsverfahren zur Geltendmachung der Entscheidungspflicht berechtigt gewesen zu sein behauptet. Für den Bereich des Datenschutzrechts sieht § 38 Abs 1 DSG 2000 darüber hinaus vor, dass auch Auftraggeber des öffentlichen Bereichs beschwerdelegitimiert sein können.

59 Für Beschwerden in Datenschutzangelegenheiten ist beim BVerwG ein **Senat** berufen (§ 39 Abs 1 DSG 2000).

60 Das VwGVG normiert in seinen §§ 11 bis 16 das **Vorverfahren,** das der Behörde die Möglichkeit geben soll, ihren Bescheid bzw ihre Säumnis entsprechend der erhobenen Beschwerde noch zu korrigieren, bevor tatsächlich das zuständige Verwaltungsgericht befasst wird (Beschwerdevorentscheidung nach § 14 VwGVG oder Nachholung des Bescheids nach § 16 VwGVG). Sämtliche **Schriftsätze sind im Vorverfahren bei der belangten Behörde einzubringen.** Erst wenn die Beschwerde dem Verwaltungsgericht vorgelegt wurde, sind die Schriftsätze bei diesem einzubringen (§§ 12 iVm 20 VwGVG). Dies bedeutet für den Bereich des Datenschutzrechts, dass Rechtsmittel gegen einen Bescheid oder die Säumnis der Datenschutzbehörde bei dieser einzubringen sind.

→ *Siehe Muster BT/DSR-11 und BT/DSR-12.*

61 Für eine detaillierte Beschreibung des Rechtsmittelverfahrens vor dem BVwG wird auf *Fischer/Steiner,* Verfahren vor den Verwaltungsgerichten (AT/VwG) verwiesen.

---

[24]) BGBl I 2012/51.

[25]) Bis zum 1. 1. 2014 war im Datenschutzrecht kein ordentliches Rechtsmittel vorgesehen (§ 40 Abs 2 Satz 1 DSG 2000 aF).

Muster BT/DSR-1: Bekanntgabe eines Vertreters nach § 6 Abs 3 DSG 2000[1])

An die
Datenschutzbehörde
[Adresse]

EINSCHREIBEN

[Datum]

Antragsteller:
Muster OOO[2])
[Adresse]
Russische Föderation

[gegebenenfalls]
vertreten durch: RA Dr. Moritz Mustermann
[Adresse]
Vollmacht erteilt

Bekanntgabe eines Vertreters nach § 6 Abs 3 DSG 2000

1-fach

1. Sachverhalt

Der Antragsteller ist nicht im Gebiet der Europäischen Union niedergelassen und betreibt die Datenanwendung „ABC“, die dem österreichischen Datenschutzgesetz (DSG 2000) unterliegt. Er ist daher nach § 6 Abs 3 DSG 2000 verpflichtet, einen in Österreich ansässigen Vertreter zu benennen, der namens des Antragstellers für den Betrieb der Datenanwendung verantwortlich gemacht werden kann.

2. Bekanntgabe

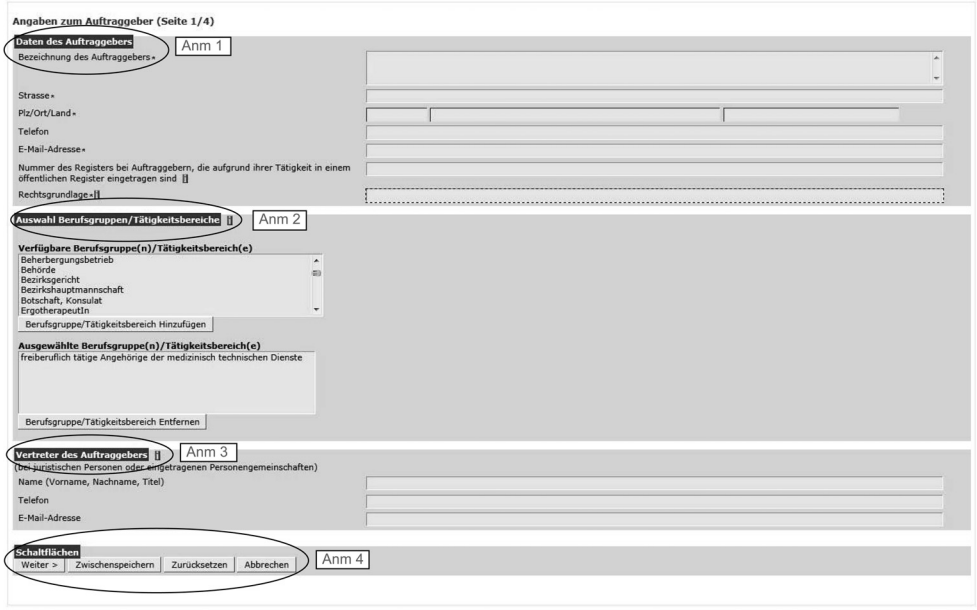
Der Antragsteller benennt die XY AG Österreich, *[Adresse],* DVR-Nummer 1234567 als deren Vertreter für den Betrieb der Datenanwendung „ABC“ im Sinne des § 6 Abs 3 DSG 2000.

[Ort, Datum] Muster OOO

Anmerkungen

1) Nach § 6 Abs 3 DSG 2000 hat der Auftraggeber einer dem DSG 2000 unterliegenden Datenanwendung, wenn er nicht im Gebiet der Europäischen Union niedergelassen ist, einen in Österreich ansässigen Vertreter zu benennen, der unbeschadet der Möglichkeit eines Vorgehens gegen den Auftraggeber selbst namens des Auftraggebers verantwortlich gemacht werden kann. Ist der Betrieb der Datenanwendung der Datenschutzbehörde zu melden oder genehmigen zu lassen, erfolgt die Namhaftmachung eines in Österreich ansässigen Vertreters über DVR-Online (s Muster BT/DSR-2 Schritt 2/4 „Vertreter des AG in der EU“). Ein eigenständiger Antrag ist daher nur in jenen Fällen notwendig, in denen ein Auftraggeber, der nicht in der Europäischen Union niedergelassen ist, nur solche dem DSG 2000 unterliegende Datenanwendung betreibt, die der Datenschutzbehörde nicht zu melden sind.
2) Bedeutet Общество с ограниченной ответственностью und ist das russische Pendant zur österreichischen GmbH.

Muster BT/DSR-2: Meldung eines Auftraggebers



Angaben zum Auftraggeber (Seite 3/4) Anm 7

Beilagen für AG

Keine Beilagen vorhanden.

Neu

Schaltflächen

< Zurück | Weiter > | Zwischenspeichern | Zurücksetzen | Abbrechen

Angaben zum Auftraggeber (Seite 4/4) Anm 8

Bitte überprüfen Sie nun nochmals die unten stehenden Angaben. Sollten Korrekturen notwendig sein, können Sie mit "Zurück" wieder zurückblättern. Wenn Ihre Angaben korrekt sind, drücken Sie bitte "Angaben zur Datenanwendung".

Zusammenfassung Daten des Auftraggebers

Bezeichnung:	Testauftraggeberin
Adresse:	Musterstrasse 1, 1010 Wien, Österreich
Telefon:	
E-Mail Adresse:	testauftraggeberin@muster.at
Registernummer:	

Zusammenfassung Vertreter des Auftraggebers

Name (Vorname, Nachname, Titel):	
Telefon:	
E-Mail Adresse:	

Zusammenfassung Berufsgruppe(n)/Tätigkeitsbereich(e)

Berufsgruppe(n)/Tätigkeitsbereich(e)

Zusammenfassung Rechtsgrundlage

Rechtsgrundlage:	Gewerbeberechtigung

Schaltflächen

< Zurück | Angaben zur Datenanwendung | Zurücksetzen | Abbrechen | Drucken

Anmerkungen

1) Auftraggeber von Datenanwendungen, die einer Meldepflicht unterliegen, sind gemeinsam mit der Meldung der ersten Datenanwendung grundsätzlich elektronisch über das Internetportal https://dvr.dsk.gv.at/ einzubringen. Zu den Ausnahmen s Rz 18, 19. Auftraggeber sind natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe, wenn sie alleine oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden, unabhängig davon, ob sie die Daten selbst verwenden oder damit einen Dienstleister beauftragen (§ 4 Z 4 DSG 2000).
2) Die Zuordnung einer oder mehrerer Berufsgruppen bzw Tätigkeitsbereiche verwendet DVR-Online auch dazu, bei der Meldung von Datenanwendungen branchenspezifische Ausfüllhilfen zur Verfügung zu stellen.
3) Hier sind jene natürlichen Personen einzutragen, die zur Vertretung von juristischen Personen oder eingetragenen Personengemeinschaften befugt sind. Beispielsweise ist hier der Geschäftsführer einer GmbH einzutragen.
4) Die Meldung eines Auftraggebers erfolgt über vier Eingabemasken. Die praktische Erfahrung zeigt, dass es sich empfiehlt, die Eingaben regelmäßig zwischenzuspeichern. Insbesondere bei umfangreichen Eingaben kommt es gelegentlich (noch) zu Fehl-

funktionen von DVR-Online. Regelmäßiges Zwischenspeichern schützt in diesen Fällen vor Verlust der bereits erfassten Daten.

5) Etwaige Zustellbevollmächtigte, wie berufsmäßige Parteienvertreter oder Sachbearbeiter beim Auftraggeber, können optional angegeben werden.
6) Hier kann ein Vertreter des Auftraggebers in Österreich benannt werden. Zu einer solchen Benennung sind nach § 6 Abs 3 DSG 2000 jene Auftraggeber verpflichtet, die ihren Sitz außerhalb der EU haben und in Österreich eine Datenanwendung betreiben (s Anm 1 zu Muster BT/DSR-1). Bei dem Titeltext „Vertreter des AG in der EU" handelt es sich um ein Redaktionsversehen. Richtigerweise sollte der Titeltext „Vertreter des AG in Österreich" lauten.
7) Auftraggeber haben ihre gesetzliche Zuständigkeit oder rechtliche Befugnis für die erlaubte Ausübung ihrer Tätigkeit nachzuweisen (§ 19 Abs 1 Z 2 DSG 2000). Dieser Nachweis kann etwa durch Vorlage des Gesellschaftsvertrags oder von Vereinsstatuten erbracht werden. Diese Dokumente sind als Beilagen dem Antrag hinzuzufügen.
8) Die erfassten Daten zum Auftraggeber werden abschließend gesammelt dargestellt. Da Auftraggeber nur gemeinsam mit einer Datenanwendung gemeldet werden können, kann die Auftraggebermeldung noch nicht eingebracht werden. Durch Drücken der Schaltfläche „Angaben zur Datenanwendung", ist daher als nächster Schritt die erste Datenanwendung zu erfassen.