1. Datenschutz

(Kurs für ITSV MitarbeiterInnen zu wichtigen Themen der Österreichischen SV)

ITSV GMBH _ Raimundgasse 1
A-1020 Wien
T: 050124 844 56 19
Christoffer.Stiger@itsv.at
www.itsv.at

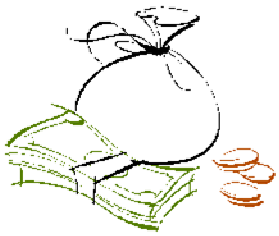
SV-allgemein Schulung: Modul 1.1
20./21. Juli 2009
Ort: ITSV-GmbH, Wien
Moderation: Christoffer Stiger
(BL Recht u. Personal)

Ideen, die wirken. itsv 1


Überblick
Einführung
Folgen der Nichtbeachtung datenschutzrechlicher Vorschriften
> persönliche (Haftungs)folgen
> Auswirkungen auf Projekte
elementare datenschutzrechtliche Begriffe
relevante Pflichten
Dienstleistung
Ideen, die wirken.
itSV
3


Überblick
Datensicherheit / Datengeheimnis
Publizitätsprinzip
>Meldepflichten
>Informationspflichten
Rechtschutz des Betroffenen
>Auskunftsrecht
>Löschungs- und Berichtigungsrecht
>(Widerspruchsrecht)
Die Befugnisse der DSK
Ideen, die wirken.
itSV
4

...die persönlichen Folgen



Amtshaftung
Geschäftsführerhaftung
Organhaftung
Dienstnehmerhaftung

Arbeitslosigkeit

Ideen, die wirken. itSV 5

Mögliche Strafen

Verwaltungsstrafen
Bis zu € 9.445,--
Ab 1.1.2010:
Bis zu € 10.000,--

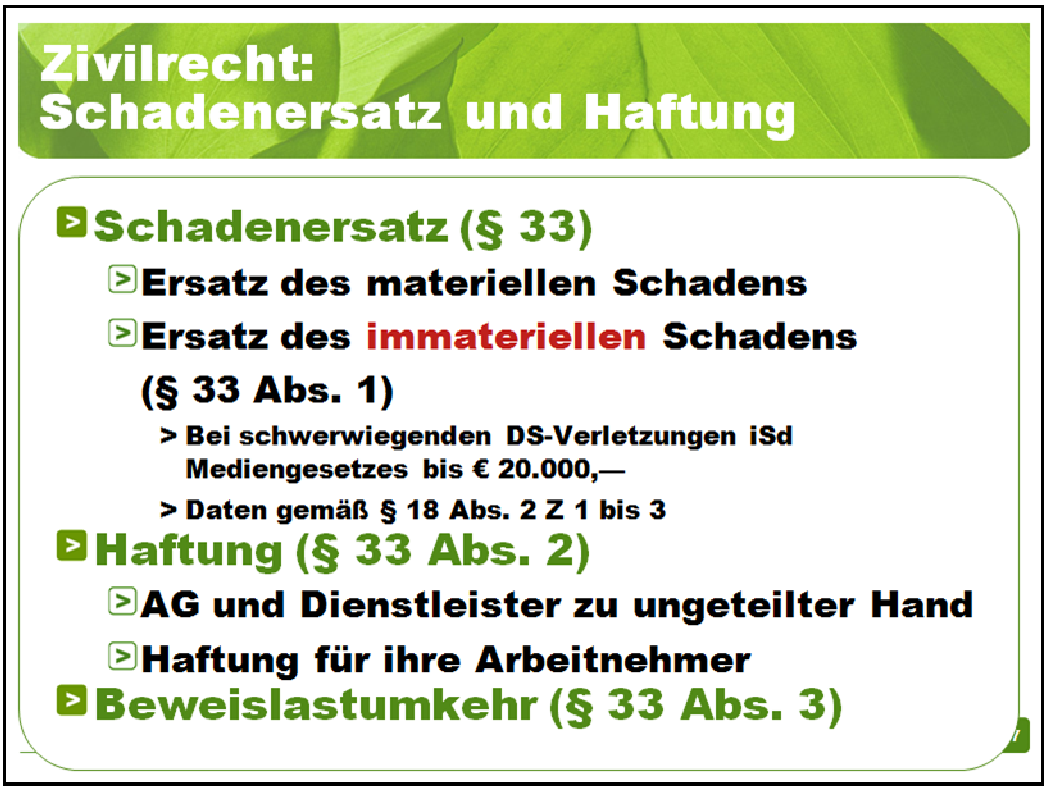
Verwaltungsstrafen
Bis zu € 18.890,--
Ab 1.1.2010:
Bis zu € 25.000,--

Vorstrafe bis zu einem Jahr

Schadenersatz materieller Schaden

Schadenersatz immaterieller Schaden

Ideen, die wirken. itSV 6

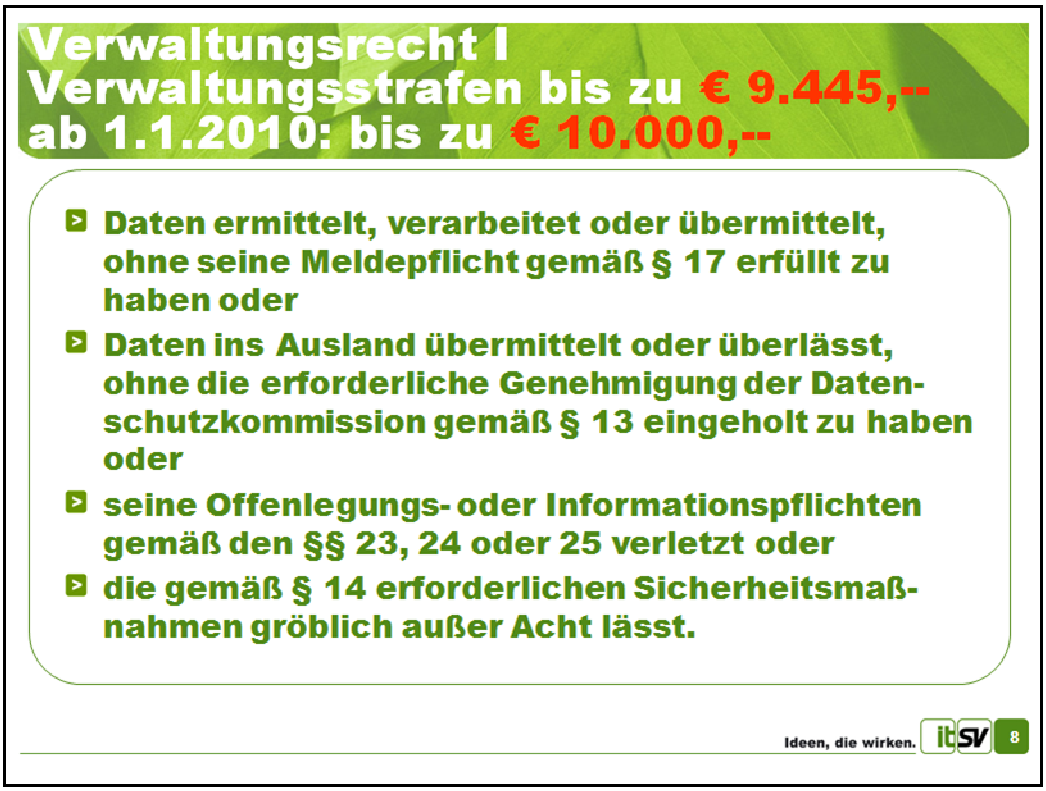


In Umsetzung von Art. 23 Abs. 1 der Richtlinie enthält § 33 DSG 2000 nunmehr ausdrückliche Bestimmung über den Ersatz erlittenen Schadens. Dafür gelten zunächst die allgemeinen Bestimmungen des Schadenersatzrechts; gehaftet wird nur bei Verschulden. Für besonders schwerwiegende Fälle rechtswidriger Datenverwendung, die ihrem Wesen nach Tatbeständen vergleichbar sind, die nach Mediengesetz zum Schadenersatz verpflichten, sieht Abs. 1 den Ersatz immaterieller Schäden vor, wobei sich die näheren Voraussetzungen und die Höhe der Entschädigung aus § 7 Abs. 1 des Mediengesetzes ergibt. Daraus folgt, dass die Höhe der Entschädigung derzeit mit € 20.000,-- begrenzt ist. Da nur Fälle besonders schwerwiegender Datenschutzverletzungen zum immateriellen Schadenersatz berechtigen sollten, wurde die hier relevanten Fälle auf die Verwendung von Daten iSd § 18 beschränkt. Hiebei ist neben der fehlerhaften insbesondere auch die rechtsmissbräuchliche Datenverwendung Regelungsgegenstand. Die Bestimmungen des DSG 2000 greifen im Einzelfall auch als Schutzgesetz iSd § 1311 ABGB. Das Grundrecht auf Datenschutz wird auch zu den - absolut geschützten - Persönlichkeitsrechten iSd § 16 ABGB zu zählen sein.

Verletzungen von Datenschutzbestimmungen erfolgen häufig außerhalb von Vertragsverhältnissen zum Geschädigten, so dass die Regelung des § 1313a ABGB nicht zur Anwendung kommt. Aus der bereits angesprochenen mangelnden Nachvollziehbarkeit der Datenverarbeitungsvorgänge für den Betroffenen erscheint es sachgemäß, dem Auftraggeber bzw. Dienstleister das Verhalten seiner Leute zuzurechnen und die Haftung bei ihm zu konzentrieren. § 33 Abs. 2 übernimmt daher die Regelung des § 1313a ABGB sinngemäß für sämtliche Haftungen aus rechtswidrigen Datenverwendungen.

Die in § 33 Abs. 3 vorgesehene Beweislastumkehr zugunsten des Betroffenen setzt die zwingende Bestimmung des Art. 23 Abs. 2 der Richtlinie um. Im übrigen gelten, etwa was Rückersatzansprüche oder die Haftung für Handlungen in Vollziehung der Gesetze betrifft, die allgemeinen Bestimmungen des bürgerlichen Rechts und des Amtshaftungsgesetzes.

Verjährungsfristen: Es gelten nicht die besonderen Verjährungsfristen für Schadenersatzansprüche, sondern die des § 1489 (drei bzw. 30 Jahre).



Verwaltungsübertretung, die mit Geldstrafe bis zu 130 000 S zu ahnden ist, wer

1. Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß § 17 erfüllt zu haben oder

2. Daten ins Ausland übermittelt oder überläßt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 eingeholt zu haben oder

3. seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24 oder 25 verletzt oder

4. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht läßt.

(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern und Programmen kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.

10. Abschnitt

Strafbestimmungen

Datenverwendung in Gewinn- oder Schädigungsabsicht

§ 51. (1) Wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen.

(2) Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen. (Abs. 2 entfällt mit 1.1.2010)

Verwaltungsstrafbestimmung

§ 52. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu € 18.890,-- (€ 25.000,-- ab 1.1.2010) zu ahnden ist, wer

sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder

Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder

Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht oder

Daten vorsätzlich entgegen § 26 Abs. 7 löscht.

sich unter Vortäuschung falscher Tatsachen vorsätzlich Daten gemäß § 48a verschafft.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu € 9.445,-- (€ 10.000,-- ab 1.1.2010) zu ahnden ist, wer

Daten ermittelt, verarbeitet oder übermittelt, ohne seine Meldepflicht gemäß § 17 („ oder 50c“ - ab 1.1.2010) erfüllt zu haben oder

Daten ins Ausland übermittelt oder überlässt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 eingeholt zu haben oder

seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24, oder 25 („oder 50d“ – ab 1.1.2010) verletzt oder

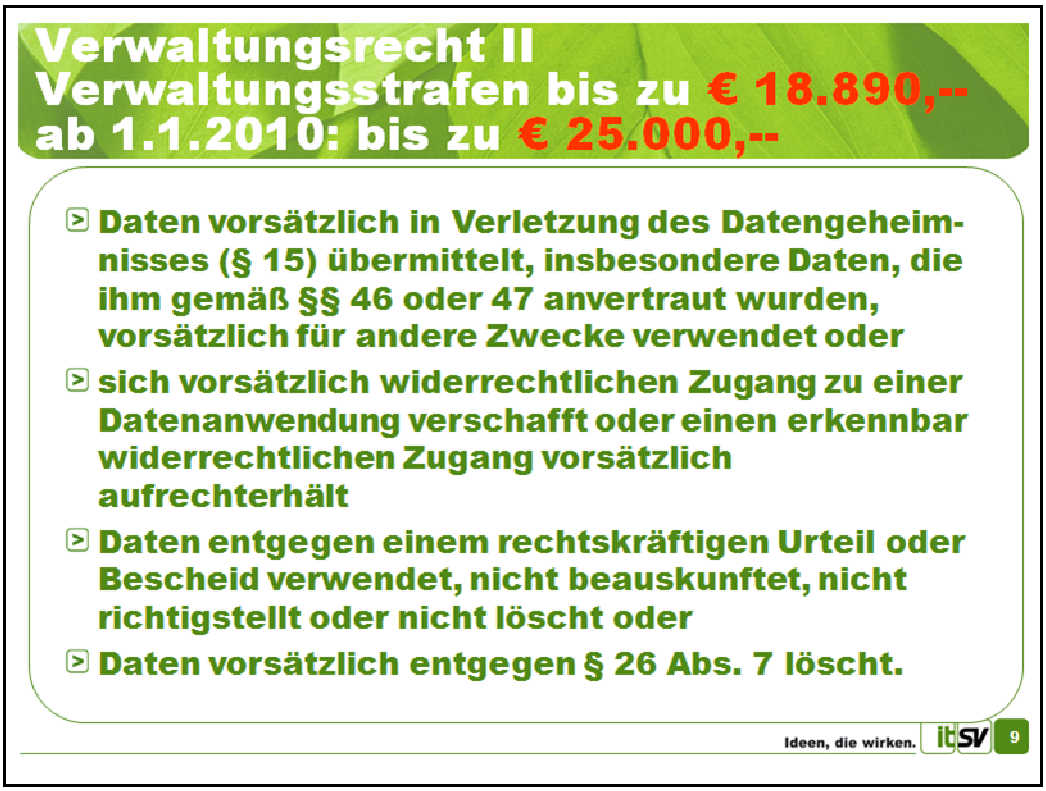
die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht lässt.

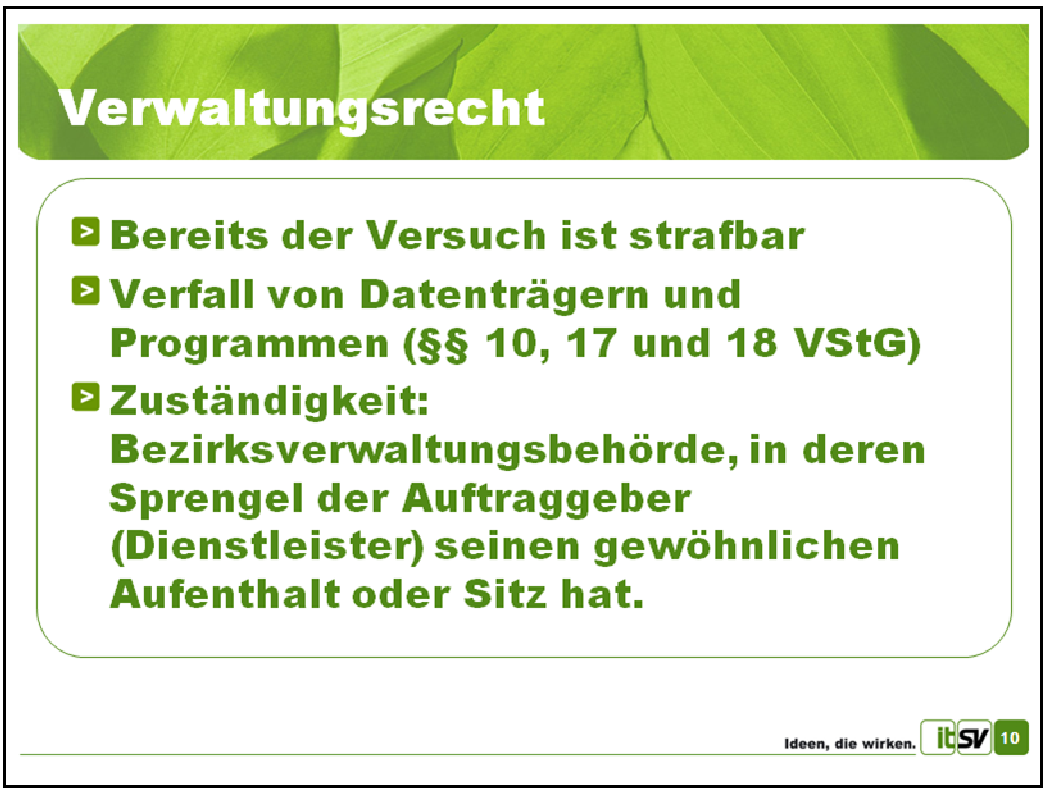
(3) Der Versuch ist strafbar.

(4) Die Strafe des Verfalls von Datenträgern und Programmen („sowie Bildübertragungs- und

Bildaufzeichnungsgeräten“ – ab 1.1.2010) kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.

(5) Zuständig für Entscheidungen nach Abs. 1 bis 4 ist die Bezirksverwaltungsbehörde, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat. Falls ein solcher im Inland nicht gegeben ist, ist die am Sitz der Datenschutzkommission eingerichtete Bezirksverwaltungsbehörde zuständig.


Verwaltungsrecht II
Verwaltungsstrafen bis zu € 18.890,--
ab 1.1.2010: bis zu € 25.000,--
Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder
sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält
Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht oder
Daten vorsätzlich entgegen § 26 Abs. 7 löscht.
Ideen, die wirken.
itSV
9


Verwaltungsrecht
Bereits der Versuch ist strafbar
Verfall von Datenträgern und Programmen (§§ 10, 17 und 18 VStG)
Zuständigkeit: Bezirksverwaltungsbehörde, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat.
Ideen, die wirken.
itSV
10

Strafbestimmung: § 51 DSG

„Wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen."

Ab 1.1.2010: kein Ermächtigungsdelikt mehr!

11

Konsequenzen für Projekte

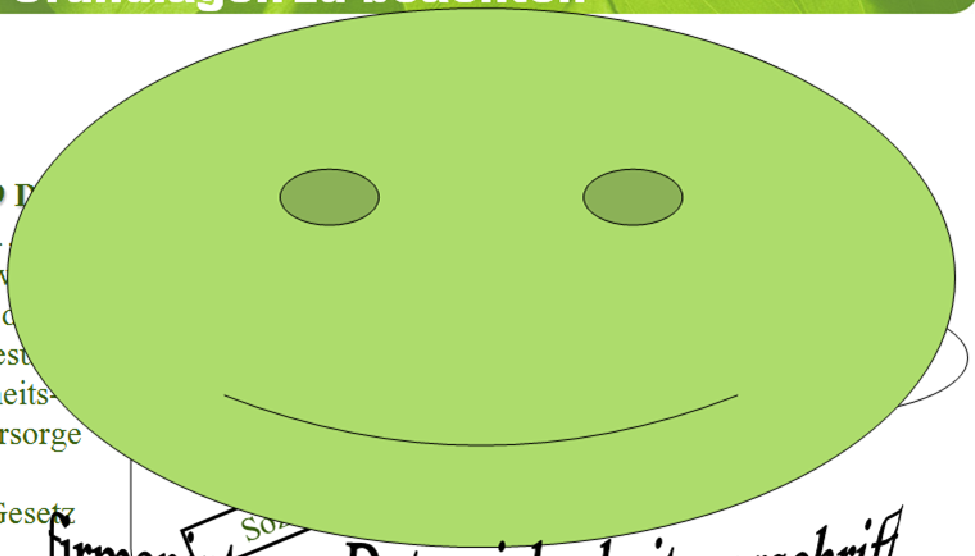
- Verzögerung der Inbetriebnahme (z.B. 2-Monatsfrist)
- Pflichtenheft unvollständig
  - Vergabeverfahren ev. zu wiederholen
  - ungeplante Kostensteigerungen
- nachträgliche Programmanpassungen erforderlich
  - teurer als wenn gleich eingeplant
  - Zeitverzögerung
  - öffentlichkeitswirksame Blamage bzw. Rufschädigung

Ideen, die wirken. itSV 12

… sinnvolle Haltung?

Ideen, die wirken. itSV 13

Das Datenschutz-Recht: Was ist für uns an gesetzlichen Grundlagen zu beachten



§ 9 D
•…
Zv
Gest
heits-
vorsorge

•Gesetz

firmeninterne Datensicherheitsvorschrift

Ideen, die wirken. itSV 14

Das Datenschutzgesetz 2000 als Basis für das Gesundheitstelematikgesetz

§ 6 DSG Grundsätze für die Datenverwendung

§ 7 DSG Zulässigkeit der Verwendung v. Daten

§ 9 DSG Schutz v. Geheimhaltungsinteressen bei sensiblen Daten

- gesetzlichen Vorschriften
- Zustimmung
- lebenswichtige Interessen, Zustimmung nicht rechtzeitig einholbar
- zum Zweck der Gesundheitsvorsorge + Verarbeitung durch Ärzte etc.

§§ 10, 11 DSG Inanspruchnahme von Dienstleistern

§ 14 DSG Datensicherheitsmaßnahmen

- Gesundheitstelematikgesetz (GTelG)
- § 9 SV-DSV

Das Gesundheitstelematikgesetz (als Teil des gesamten „Datenschutzrechtes") spezifiziert die gem. § 14 Datenschutzgesetz zu implementierenden Sicherheitsmaßnahmen gezielt für den Gesundheitsbereich auf einem sehr hohen/strengen Sicherheitsniveau.

Daten dürfen nur verarbeitet und übermittelt werden, wenn:

Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind (§ 7 Abs. 1 DSG 2000) und schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden (§ 7 Abs. 1 DSG 2000).

Da Gesundheitsdaten sensible Daten iSd § 4 Z 2 DSG 2000 sind, gilt § 9 DSG 2000, wonach die Verwendung von Daten nur in bestimmten Fällen zulässig ist; für den Bereich der Gesundheitsdaten sind die wichtigsten dieser Fälle, dass sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen (§ 9 Z. 3 DSG 2000),

oder

der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt (§ 9 Z. 6 DSG 2000),

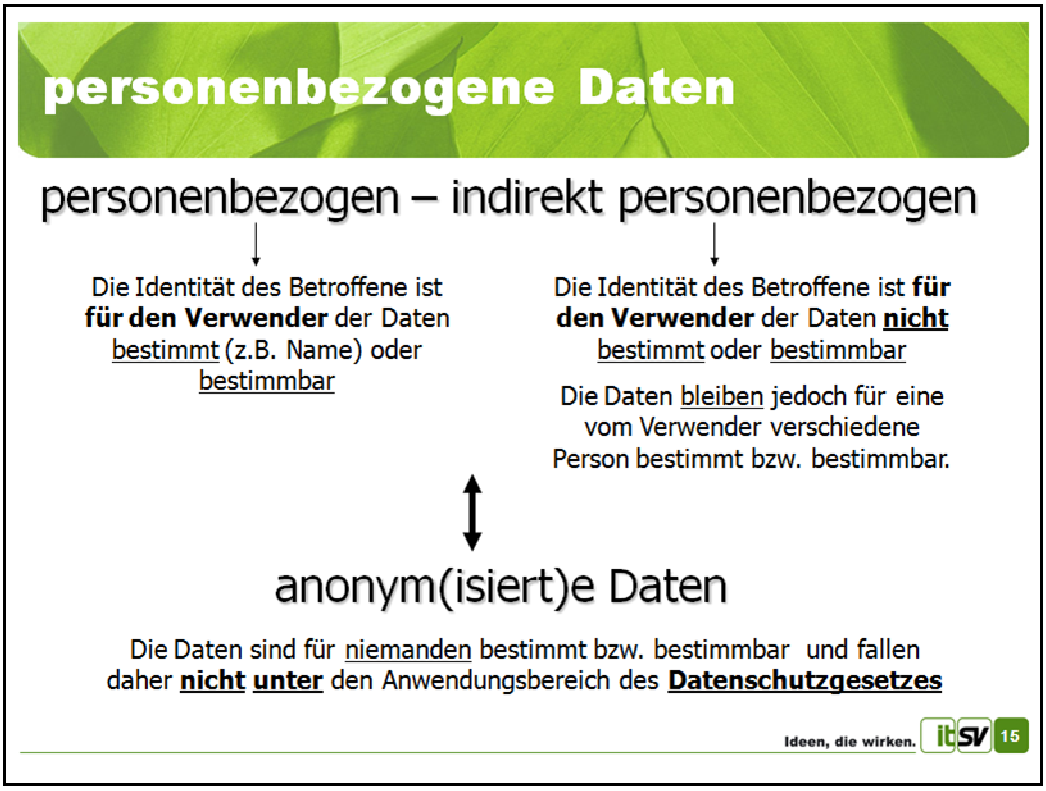
oder

die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann, z.B. Behandlung im Notfall (§ 9 Z. 7 DSG 2000),

oder

die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich sind und die Verwendung dieser Daten durch ärztliches Personal oder sonstiges Personal erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen (§ 9 Z. 12 DSG 2000).

Die Weiterverwendung von personenbezogenen Daten für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 DSG 2000 zulässig.



Indirekt personenbezogene Informationen sind Daten, bei denen der Personenbezug der Daten derart ist, dass die *betroffenen* Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des ***Betroffenen mit rechtlich zulässigen Mitteln*** nicht bestimmen können. (Es existiert allerdings für einen anderen Datenverwender die Möglichkeit diese Daten einer bestimmten Person zuzuordnen. Für diesen Datenverwender sind diese Daten daher "direkt" bezogen und unterliegen zur Gänze dem Datenschutz, während für die Verwender von indirekt personenbezogenen Daten weitreichende Ausnahmen existieren, so sind indirekt personenbezogene Daten nicht nur von der Meldepflicht ausgenommen, sondern auch von der Auskunftspflicht, dem Widerspruchsrecht sowie der Löschungs- und Richtigstellungsverpflichtung.) Unter Bedachtnahme auf Erwägungsgrund 26 der Richtlinie wird diesbezüglich weiter einzuschränken sein auf diejenigen *rechtlich zulässigen Mittel, welche als möglich anzusehen sind*, d.h. also weder seiner Art nach, noch seinem Aufwand nach vollkommen ungewöhnlich ist. Hingegen gibt es bei *anonymisierten Daten* für niemanden einen Personenbezug, daher sind diese auch *nicht* datenschutzrelevant.

§ 4 Z 2 Datenschutzgesetz (DSG)

“sensible Daten”
Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschafts-zugehörigkeit, religiöse oder philo-sophische Überzeugung, Gesundheit oder ihr Sexualleben;

Ideen, die wirken. itSV 16

Gesundheitsdaten werden im Gesundheitstelematikgesetz definiert

§ 2 Z 1 GTelG “Gesundheitsdaten”

direkt personenbezogene Daten über die physische oder psychische Befindlichkeit
- **Diagnose**
- **Medizinische Vorsorge und Versorgung, Pflege**
- **Verrechnung**
- **Versicherung von Gesundheitsrisiken**

Beispiele:
verordneten/bezogenen Arzneimittel, Heilbehelfe, Hilfsmittel,
Diagnose-, Therapie- oder Pflegemethoden
Art, Anzahl, Dauer, Kosten von Gesundheits-/ Versicherungsdienstleistungen

Ideen, die wirken. itSV 17

Ab 1.1.2010 lautet § 4 Abs. 1 Z 4 :

Auftraggeber: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten zu verwenden (Z 8), unabhängig davon, ob sie die Daten selbst verwenden (Z 8) oder damit einen Dienstleister (Z 5) beauftragen. Sie gelten auch dann als Auftraggeber, wenn der mit der Herstellung eines Werkes beauftragte Dienstleister (Z 5) die Entscheidung trifft, zu diesem Zweck Daten zu verwenden

(Z 8), es sei denn dies wurde ihm ausdrücklich untersagt oder der Beauftragte hat auf Grund von Rechtsvorschriften oder Verhaltensregeln über die Verwendung eigenverantwortlich zu entscheiden;

Ab 1.1.2010 lautet § 4 Abs. 1 Z 5 :

Dienstleister: natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten nur zur Herstellung eines ihnen aufgetragenen Werkes verwenden (Z 8);

Erläuterungen zu § 4 Abs. 1 Z. 4:

Durch den vorgeschlagenen § 4 Abs. 1 Z 4 soll der für die Praxis des Datenschutzes zentrale Begriff des Auftraggebers sprachlich gestrafft und leichter verständlich formuliert werden, ohne dass es zu inhaltlichen Änderungen kommt. Klargestellt soll lediglich werden, dass die Auftraggebereigenschaft nicht nur dann erhalten bleibt, wenn der Dienstleister (Z 5) zur Herstellung des ihm aufgetragenen Werkes Daten verwendet, die ihm vom Auftraggeber überlassen werden, sondern auch dann, wenn er für die Zwecke seines Auftrages Daten bei Dritten ermittelt (sog. Ermittlungsdienstleister). Dass es nunmehr „verwenden“ anstatt bisher „verarbeiten“ lautet, soll lediglich eine Zurechnung sowohl von Verarbeitungs- als auch von Übermittlungsschritten zum Auftraggeber verdeutlichen, was dem umfassenden Begriff des Art. 2 lit. d der Richtlinie 95/46/EG entspricht. Unverändert bleibt auch die Auftraggebereigenschaft jener beauftragten Berufsgruppen, die aufgrund von Rechtsvorschriften eigenverantwortlich über die Verwendung von Daten entscheiden (vgl. die beispielhafte Aufzählung

der Rechtsanwälte, Wirtschaftstreuhänder und Ziviltechniker in den Erläuterungen zur Regierungsvorlage 1613 der Beilagen XX. GP, 37, zur Stammfassung).

Erläuterungen zu § 4 Abs. 1 Z. 5:

Der vorgeschlagene § 4 Abs. 1 Z 5 enthält die schon beim Auftraggeberbegriff vorgenommene Klarstellung hinsichtlich der sog. Ermittlungsdienstleister. Nicht als Dienstleister anzusehen werden aber folgende Fälle sein:

- ein mit der Herstellung eines Werkes Betrauter, der für die zu diesem Zweck überlassenen Daten ein Entgelt leistet (anders noch DSK 13. Dezember 2006, GZ K121.217/0021-DSK/2006); oder

- ein mit der Herstellung eines Werkes Betrauter, der Daten verschiedener Aufträge verknüpft; oder

- der Empfänger von Daten, der über die Verwendung von Daten entgegen einer Anordnung dessen entscheiden kann, welcher ihm die Daten weitergegeben hat.

Durch die Einfügung des Wortes „nur“ soll klargestellt werden, dass der mit der Herstellung eines Werkes Beauftragte nur dann als Dienstleister qualifiziert werden kann, wenn er ihm überlassene bzw. von ihm ermittelte Daten ausschließlich für den Zweck der Werkherstellung und nicht (auch) für einen anderen Zweck verwendet (vgl. in diesem Sinn schon DSK 20. Oktober 2006, GZ K121.155/0015-DSK/2006).

§ 50 DSG – Neuerungen ab 1.1.2010

(1) […] Abgesehen von der abweichenden Frist gilt § 26 Abs. 3 bis 10 sinngemäß.

(2) Durch entsprechenden Rechtsakt können auch weitere Auftraggeberpflichten, insbesondere auch die Vornahme der Meldung des Informationsverbundsystems, auf den Betreiber übertragen werden. Allein für die Übertragung der Meldepflicht ist die Vorlage von Vollmachten nach § 10 des Allgemeinen Verwaltungsverfahrensgesetzes 1991, BGBl. Nr. 51, nicht erforderlich. Soweit der Pflichtenübergang nicht durch Gesetz angeordnet ist, ist er gegenüber Dritten nur wirksam, wenn er – auf Grund einer

entsprechenden Meldung an die Datenschutzkommission – aus der Registrierung im Datenverarbeitungsregister ersichtlich ist.

(2a) Wird ein Informationsverbundsystem auf Grund einer Meldung von zumindest zwei Auftraggebern registriert, so können Auftraggeber, die in der Folge die Teilnahme an dem Informationsverbundsystem anstreben, die Meldung im Umfang des § 19 Z 3 bis 8 auf einen Verweis auf den Inhalt der Meldung eines bereits registrierten Auftraggebers beschränken, wenn sie eine Teilnahme im genau gleichen Umfang anstreben. Soweit sich ein solcher weiterer Auftraggeber anlässlich der Meldung ausdrücklich den Auflagen unterwirft, die die Datenschutzkommission anlässlich der Meldung, auf die er verweist, ausgesprochen hat, werden diese für ihn mit der Registrierung in gleicher Weise und mit gleicher Wirkung (§ 52 Abs. 1 Z 3) verbindlich und ist die Erlassung eines gesonderten Auflagenbescheides durch die Datenschutzkommission nicht erforderlich.

Erläuterungen zu § 50 Abs. 1 dritter Satz:

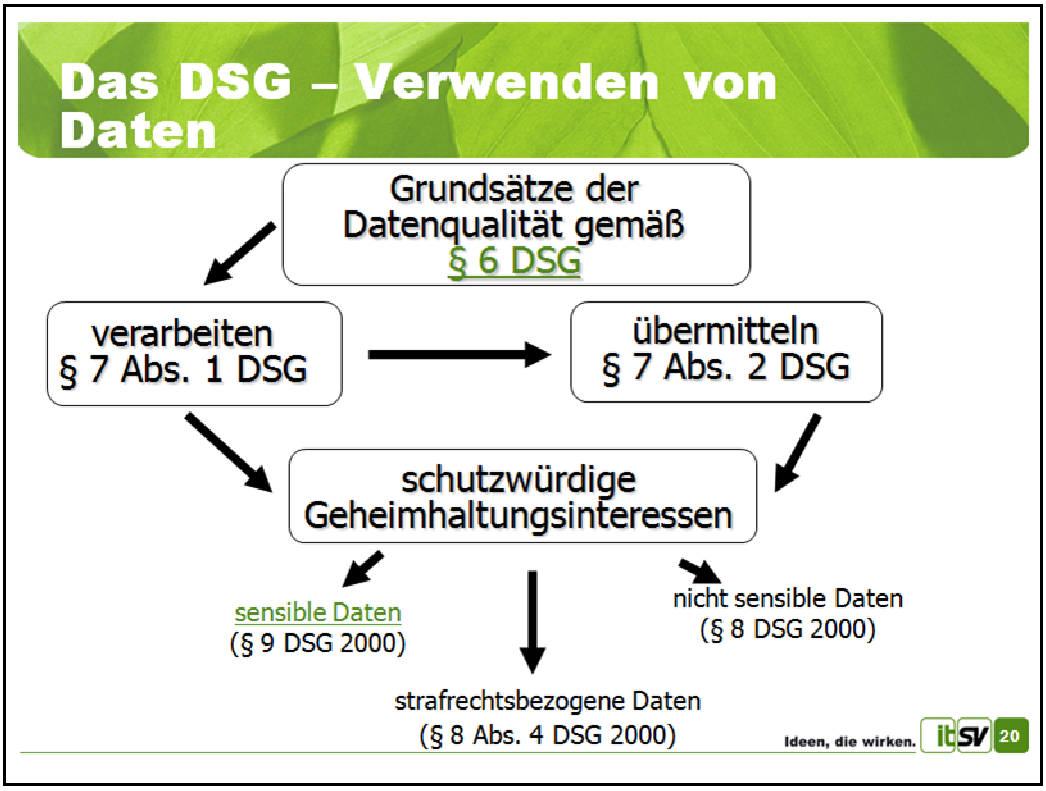
Die Einforderung des Rechts auf Bekanntgabe des Ablaufs einer automationsunterstützten Einzelentscheidung bzw. des verantwortlichen Auftraggebers in einem Informationsverbundsystem soll gleich wie beim Recht auf Auskunft erfolgen.

Erläuterungen zu § 50 Abs. 2 und 2a:

Diese Bestimmungen sollen der Vereinfachung des Registrierungsverfahrens für Informationsverbundsysteme dienen. Zunächst wird in Abs. 2 klargestellt, dass dem Betreiber auch die Vornahme der Meldung (idR durch eine Vollmacht) übertragen werden kann. In diesem Fall scheint es nicht erforderlich, dass die DSK vom Betreiber Vollmachten aller Auftraggeber einfordern muss, wie es § 10 des Allgemeinen Verwaltungsverfahrensgesetzes 1991, BGBl. Nr. 51 (AVG) an sich vorsehen würde. Wenn der Betreiber in der Lage ist, die Meldungen vorzunehmen, so kann das Vorliegen eines Vollmachtsverhältnisses vermutet werden. Im Zweifelsfall hat die DSK selbstverständlich die Möglichkeit, sich dieses auch nachweisen zu lassen. Die Nennung von Behörden im zweiten Satz scheint entbehrlich, sie sind idR „Dritte“. Der Datenschutzkommission als verfahrensführender Behörde wird die Pflichtenübertragung schon vor der Registrierung bekannt, daher kann sie ihr gegenüber schon mit dem Einlangen der Meldung wirksam werden.

Nach dem neuen Abs. 2a kann sich die Meldung eines Teilnehmers an einem Informationsverbundsystem hinsichtlich des Inhalts der Datenanwendung nunmehr auf einen Verweis auf eine bereits registrierte Meldung eines anderen Teilnehmers beschränken, wenn er im exakt gleichen Umfang teilnehmen will.

Damit gelten für solche weiteren Meldungen im Ergebnis ähnliche Vereinfachungen wie für Musteranwendungen. Wenn sich der weitere Teilnehmer anlässlich der vereinfachten Meldung auch noch den anlässlich der „Vorbildmeldung“ bereits erteilten Auflagen unterwirft, so werden diese kraft Gesetzes mit der Registrierung für ihn ebenso wirksam, ein eigener Auflagenbescheid braucht nicht erlassen zu werden. Ein Rechtsschutzdefizit entsteht dadurch nicht, weil jedem Teilnehmer jederzeit auch die Abgabe einer gewöhnlichen Meldung offen steht und dann in der Folge über die Auflagen in Bescheidform zu entscheiden ist.



§ 6 stellt hinsichtlich der Zulässigkeit der Verwendung von Daten **zunächst** allgemeine Grundsätze auf, die den übrigen Voraussetzungen vorangestellt sind; § 7 enthält die Regeln für die Beurteilung der Zulässigkeit einer konkreten Datenverwendung, wobei zwischen Verarbeitung (Abs. 1) und Übermittlung (Abs. 2) unterschieden wird.

Die Zulässigkeit der Verarbeitung einer *konkreten* Datenanwendung hat 2 Voraussetzungen:

1. Die Berechtigung des Auftraggebers (aufgrund seiner gesetzlichen Zuständigkeit (öffentlicher Bereich) oder seiner rechtlichen Befugnissen (privater Bereich)).--> Überprüfung des **Zwecks** der Verarbeitung

2. Die Berücksichtigung der schutzwürdigen Geheimhaltungsinteressen des Betroffenen betreffend die Verarbeitung ihn betreffende Daten.--> (unter Bedachtnahme auf die Unterscheidung zwischen sensiblen, strafrechtsbezogenen und nicht-sensiblen Daten).

Die Zulässigkeit einer *konkreten* Übermittlung, welche nur aus einer - wie o.a. „zulässigen“ - Datenanwendung erfolgen darf, bedarf zusätzlich folgender Voraussetzungen:

3. Der Empfänger hat dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis - sowie diese nicht außer Zweifel steht - im Hinblick auf den Übermittlungs*zweck* **glaubhaft** (z.B. durch den Nachweis der gesetzliche Zuständigkeit oder der rechtlichen Befugnis, z.B. durch einen Gewerbeschein) zu machen.

4. Die Berücksichtigung der schutzwürdigen Geheimhaltungsinteressen des Betroffenen betreffend die Übermittlung ihn betreffende Daten.

„schutzwürdige Geheimhaltungsinteressen“

Bei der Beurteilung, ob schutzwürdige Geheimhaltungsinteressen nicht verletzt werden - und daher die Datenanwendung grundsätzlich zulässig ist - ist zu unterscheiden, ob in der Datenanwendung sensible (§ 9 DSG 2000), nichtsensible (§ 8 Abs. 1-3 DSG 2000) oder strafrechtlich relevante Daten (§ 8 Abs. 4 DSG 2000) verwendet werden:

Schutzwürdige Geheimhaltungsinteressen sind bei der Verwendung von keiner der o.a. Datenqualitäten verletzt, wenn

- sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt (welche bei der Verwendung von sensiblen Daten außerdem noch der Wahrung wichtiger öffentlicher Interessen dienen müssen),*)

- der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt,

- die Daten nur in indirekt personenbezogener Form verwendet werden,

- lebenswichtige Interessen des Betroffenen die Verwendung erfordern (wobei bei der Verwendung sensibler Daten das zusätzliche Erfordernis - nämlich die Unmöglichkeit der Einholung der rechtzeitigen Zustimmung des Betroffen - hinzutreten muss),*)

- die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht,

- die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden,*)

- die Verwendung zur Wahrung lebenswichtiger Interessen eines anderen erforderlich sind, *)

- Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben,

- der Betroffene die Daten offenkundig selbst öffentlich gemacht hat (bei "nichtsensiblen" Daten reicht es, wenn die Daten von irgendjemandem - zulässigerweise - veröffentlicht wurden).

Alle Datenqualitäten können desweiteren für Zwecke iSd §§ 45 (private Zwecke), 46 (wissenschaftliche Forschung oder Statistik), 47 (Benachrichtigung oder Befragung des Betroffenen), sowie für eng umrissene Aufgaben gemäß § 9 Zif. 11 - 13 DSG 2000 auf dem Gebiet des Arbeitsrechts, Gesundheitsrechts und der Religion verwendet werden.

Der o.a. Katalog ist betreffend die Verwendung "sensibler" Daten abschließend. Die Verwendung sensibler Daten ist daher nur unter den o.a. Voraussetzungen zulässig.

*) **In Ausnahmefällen wurde die Richtlinie unrichtig umgesetzt:** bei der Verwendung von Daten zur Wahrung lebenswichtiger Interessen des Betroffenen **oder** eines Dritten setzt die RL voraus, dass die betroffenen Person ihre Einwilligung aus physischen oder rechtlichen Gründen nicht geben kann (Art. 8 Abs. 2 lit.c) und ist damit enger als § 9 Z 7 und 8 DSG. Dort genügt es, wenn die Zustimmung nicht rechtzeitig eingeholt werden kann (Z7) bzw. fehlt das Erfordernis der Zustimmung ganz (Z8). Z 9 ermöglicht eine Ausnahme, wenn die Verwendung der Daten für die Durchsetzung eines Rechtsanspruchs „vor Behörden“ notwendig ist, während die RL von Rechtsansprüchen „vor Gericht“ spricht (lit.e). Problematisch ist schließlich auch noch die Ausnahme nach Z 3, wenn sich die Ermächtigung zur Datenverwendung aus gesetzlichen Vorschriften ergibt, soweit diese zur Wahrung eines wichtigen öffentlichen Interesses dienen. Art. 8 Abs. 4 der RL verlangt für diese Fälle zusätzlich angemessene Garantien des Datenschutzes. **In allen diesen Fällen gelten wegen ihrer unmittelbaren Anwendbarkeit die engeren Bestimmungen der RL.**

Strafrechtsbezogene Daten (Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen, insbesondere auch über den "Verdacht" der Begehung von Straftaten, sowie über strafrechtliche Verurteilungen oder vorbeugende Maßnahmen) bilden grundsätzlich einen Sonderfall der "nichtsensiblen" Daten. Deren Verwendungsbefugnis wird in § 8 Abs. 4 DSG 2000 geregelt und sieht vor, dass dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen verstoßen wird, wenn:

- eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten besteht oder

- die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder

- sich sonst die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergibt, und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach diesem Bundesgesetz gewährleistet

- ab 1.1.2010 (Z. 4): die Datenweitergabe zum Zweck der Erstattung einer Anzeige an eine zur Verfolgung der angezeigten strafbaren Handlungen (Unterlassungen) zuständige Behörde erfolgt. (Erläuterungen zu § 8 Abs. 4 Z. 4: Die bisherige Regelung über die Verwendung von strafrechtsrelevanten Daten scheint insofern ergänzungsbedürftig, als der hier genannte Fall der Anzeigeerstattung (insbesondere im Verwaltungsstrafverfahren) unter keinen der dort genannten Tatbestände eindeutig subsumierbar scheint. Sofern besondere gesetzliche Vorschriften bestehen, die etwa eine bestimmte Vorgangsweise bei der Anzeigenerstattung vorsehen (wie das Suchtmittelgesetz) oder einer Anzeigeerstattung entgegenstehen, gehen diese Bestimmungen dem § 8 Abs. 4 Z 4 vor.)

Im Gegensatz dazu wird bei **ausschließlich nichtsensiblen Daten** in Form einer Generalklausel (§ 8 Abs. 1 DSG 2000) mit einzelnen wichtigen Beispielen (§ 8 Abs. 2-3 DSG 2000) festgelegt, wann keine "schutzwürdigen Geheimhaltungsinteressen" bei der Verwendung ausschließlich "nichtsensibler" Daten verletzt werden und die Verwendung dieser Daten daher zulässig ist. Zu den o.a. angeführten Ziffern 1-9 treten hinsichtlich der Verwendung nichtsensibler Daten folgende Punkte hinzu:

- die Verwendung nichtsensibler Daten ist zulässig, wenn das überwiegende berechtigte Interesse des Auftraggebers oder eines Dritten die Verwendung erfordert (dieser Anwendungsfall wird teilweise durch die oben angeführten Voraussetzungen beispielsweise ausgeführt; aufgrund des demonstrativen Charakters dieser Bestimmung sind die o.a. Voraussetzungen jedoch nicht als abschließend zu betrachten, weshalb auch unter Berücksichtigung einer restriktiven Auslegung des Verhältnismäßigkeitsprinzips ein erweiterbarer Anwendungsbereich bleibt)

- Die Verwendung ausschließlich nichtsensibler Daten ist außerdem zulässig, wenn die Datenverwendung für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist.

Der Unterschied zwischen den beiden Regelungen liegt vor allem darin, dass eine Verwendung von nichtsensiblen Daten durch Auftraggeber des öffentlichen Bereichs gemäß § 8 DSG 2000 erlaubt ist, wenn hiefür eine ausdrückliche gesetzliche Ermächtigung besteht, oder soweit dies für den Auftraggeber zur Wahrnehmung der ihm gesetzlich übertragenen Aufgaben eine wesentliche Voraussetzung bildet, während bei der Verwendung sensibler Daten durch jedweden Auftraggeber (auch den privaten) die Abstellung auf eine "wesentliche Voraussetzung zur Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe" - entsprechend dem abschließenden Katalog des § 9 DSG 2000 - nicht ausreicht.

Datensicherheitsmaßnahmen

§ 7. (1) Auftraggeber und Dienstleister haben die Richtigkeit der Verarbeitungsergebnisse in regelmäßigen Abständen durch Stichproben oder Prüfprogramme zu überprüfen.

(2) Daten und Programme sind vor Entstellung, Zerstörung und Verlust sowie gegen unbefugte Verwendung und Weitergabe zu schützen.

(3) Der Auftraggeber (oder in dessen Auftrag der Dienstleister) hat für die Vernichtung unbrauchbarer oder nicht mehr benötigter Ausdrucke und sonstiger Datenträger Sorge zu tragen.

(4) Wird ein Fehler festgestellt, so haben der Auftraggeber und der Dienstleister alles zu unternehmen, um das Schadensausmaß gering zu halten, den Betroffenen unnötige Mühe zu ersparen, die Fehlerbehebung raschest einzuleiten und Folgefehler zu verhindern.

(5) Für die ordnungsgemäße und sichere Anwendung von Daten sind folgende Datensicherheitsmaßnahmen (§ 14 DSG 2000) zu setzen:

1. Es ist eine Ansprechstelle (Person, Organisationseinheit) für Datensicherheitsmaßnahmen zu benennen, welcher die Unterlagen (Organisationsbeschreibungen, Datensicherheitsmaßnahmen etc.) des Versicherungsträgers und des Hauptverbandes gesammelt zur Verfügung stehen.

2. Für die Programmverwaltung sind Zuständigkeiten und Regeln festzulegen. Zugriffsschutz zu personenbezogenen Daten und Datensicherheitsmaßnahmen sind nach Maßgabe des jeweiligen Standes der Technik zu organisieren; erteilte Zugriffsberechtigungen sind einfach lesbar auf nachvollziehbare Weise (inklusive des Berechtigungszeitraumes) zu dokumentieren. Bestehende Einrichtungen sind regelmäßig auf Verbesserungsmöglichkeiten zu untersuchen.

3. Zugriff auf Datenanwendungen darf nur eingeräumt werden, nachdem die Bestimmungen über das Datengeheimnis (§ 15 DSG 2000), die Datensicherheitsmaßnahmen und diese Verordnung zur Kenntnis gebracht wurden. Sammelzugriffsberechtigungen sind unzulässig.

4. Zugriffsberechtigungen sind möglichst nur befristet einzuräumen und jedenfalls zu beenden, wenn sie

a) zur weiteren Arbeit nicht mehr benötigt werden oder

b) vom Berechtigten Verstösse gegen Datensicherheitsvorschriften gesetzt wurden.

5. Datensichtgeräte (Bildschirme, etc.) sind so aufzustellen, dass der mit ihnen wiedergegebene Inhalt nicht von Unbefugten mitgelesen werden kann.

6. Von einer Einschau der Datenschutzkommission nach § 30 DSG 2000 betreffend das Informationsverbundsystem der österreichischen Sozialversicherung sind vom betroffenen Versicherungsträger jedenfalls der Hauptverband und jene Versicherungsträger zu verständigen (§ 321 ASVG, § 183 GSVG, § 171 BSVG, § 119 B-KUVG, § 87 NVG), welche Daten des Betroffenen verwenden.

7. Es sind alle dem jeweiligen Stand der Technik entsprechenden und wirtschaftlich zumutbaren Maßnahmen zu treffen, um eine Veränderung oder Vernichtung der Daten durch Programmstörungen zu verhindern, wie die Installation von Virenschutzprogrammen, fire-walls, Laufwerksperren, gestaffelte Zugriffsberechtigungen, etc.

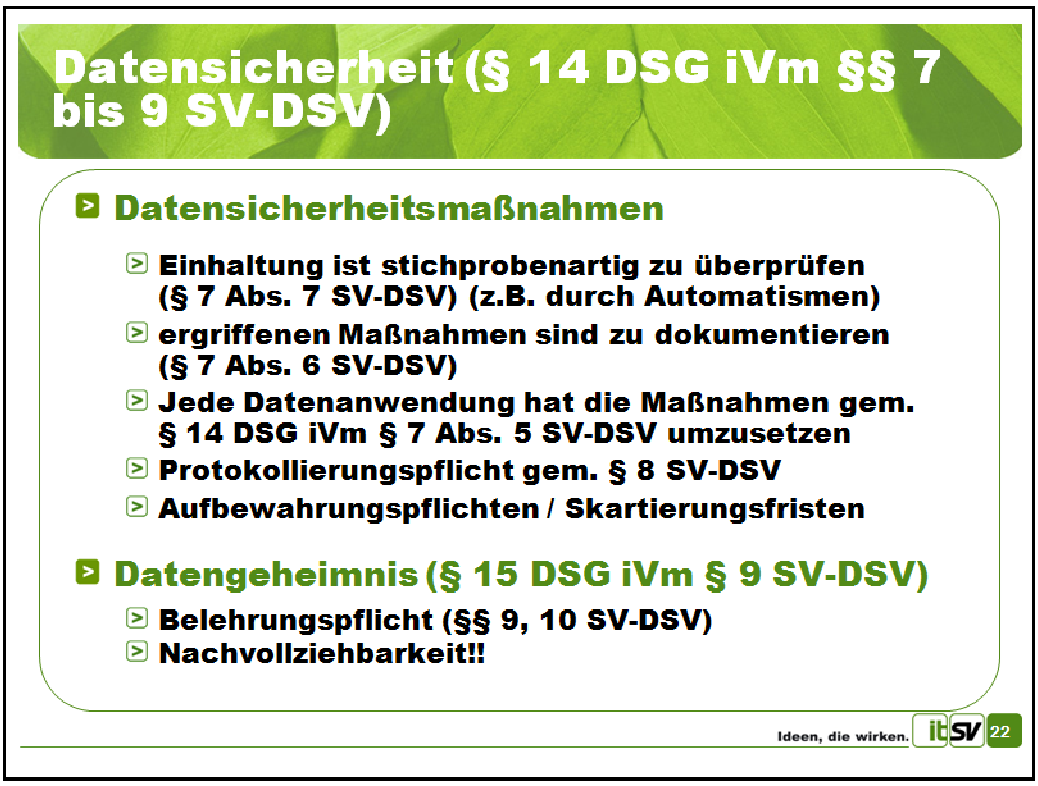
8. Datenträger (Festplatten, Bänder, Disketten etc.) sind vor einer Veräußerung oder Entsorgung zu löschen oder sicher unlesbar zu machen.

9. Zugriff auf Datenverwendungen darf nur auf Grund persönlicher Benützerkennungen und Kennwörter (Passwörter) möglich sein. Die Kennwortvergabe hat vorzusehen, dass Kennwörter aus einer Mindestzahl von Zeichen und (wenn nicht schwer wiegende technische Gründe dagegen sprechen) einer Kombination aus Buchstaben, Ziffern (statt Ziffern auch Sonderzeichen) zu bestehen haben. Kennwörter sind geheim zu halten, ihre Änderung ist dem Zugriffsberechtigten innerhalb periodischer Zeiträume möglich zu machen. Das Kennwort muss von der Benutzerkennung verschieden sein.

(6) Über alle Datensicherheitsmassnahmen ist eine Dokumentation zu führen; diese ist mindestens elf Jahre aufzubewahren.

(7) Der Hauptverband als Betreiber nach § 50 Abs. 1 DSG 2000 hat gemeinsam mit den Versicherungsträgern durch Stichproben zu prüfen, ob die Verwendung der Daten den einschlägigen Bestimmungen entsprechend erfolgt und die erforderlichen Datensicherheitsmaßnahmen ergriffen worden sind.

(8) Bedient sich der Hauptverband oder ein Sozialversicherungsträger für den Datenverkehr eines Dienstleisters, so ist dieser zur Einhaltung aller datenschutzrechtlichen Bestimmungen und Ergreifung der in dieser Verordnung vorgesehenen Datensicherheitsmaßnahmen zu verpflichten.



Gemäß § 14 Abs. 1 iVm Abs. 2 erster sowie letzter Satz ist zu folgern, dass die u.a. Prinzipien nicht durchgehend verwirklicht werden müssen. Es kann daher *beispielsweise* die Protokollierungsverpflichtung entfallen, wenn auf eine Datenanwendung nur ein sehr beschränkter Personenkreis zugreift, sodass die Verantwortung bei allfälligem Missbrauch, bedingt durch organisatorische Maßnahmen, eindeutig erkennbar ist. Es ist jedoch in Summe ein System zu etablieren, welches je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit - sicherstellt, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Diese Einschränkung (der Protokollierungspflicht) ist allerdings **sehr restriktiv** zu beurteilen.

Kompetenztrennungsprinzip (Z1): die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ist ausdrücklich festzulegen. Es muss folglich eine genaue Rollenverteilung (beinhaltend eine genaue Rollenbeschreibung mit Funktionsbeschreibungen, Kommandostrukturen, u.ä.) existieren, was die Existenz einer klaren Aufbauorganisation bedingt.

Auftragsprinzip (Z2): die Verwendung von Daten ist an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden, was unter anderem die Verwirklichung des Kompetenztrennungsprinzips, die nachweisliche Belehrung über - beziehungsweise Bindung an - Geheimhaltungsverpflichtungen, eine Klassifikation von Geheimhaltungsstufen (geheim, streng geheim, u.ä.), sowie die Erstellung verschiedener Vorschriften betreffend den Umgang mit nicht mehr benötigten Datenträgern bedingt (Aktenshredder, Festplattenformatierungen, u.ä.).

Belehrungsverpflichtung (Z3): jeder Mitarbeiter ist über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren. Es ist folglich die Benutzung von Datenverarbeitungsanlagen,

sowie jeweils einzelnen Datenanwendungen an einen Kenntnisnachweis zu binden (z.B: Teachwarekurse, inner und/oder außerbetriebliche Schulungen).

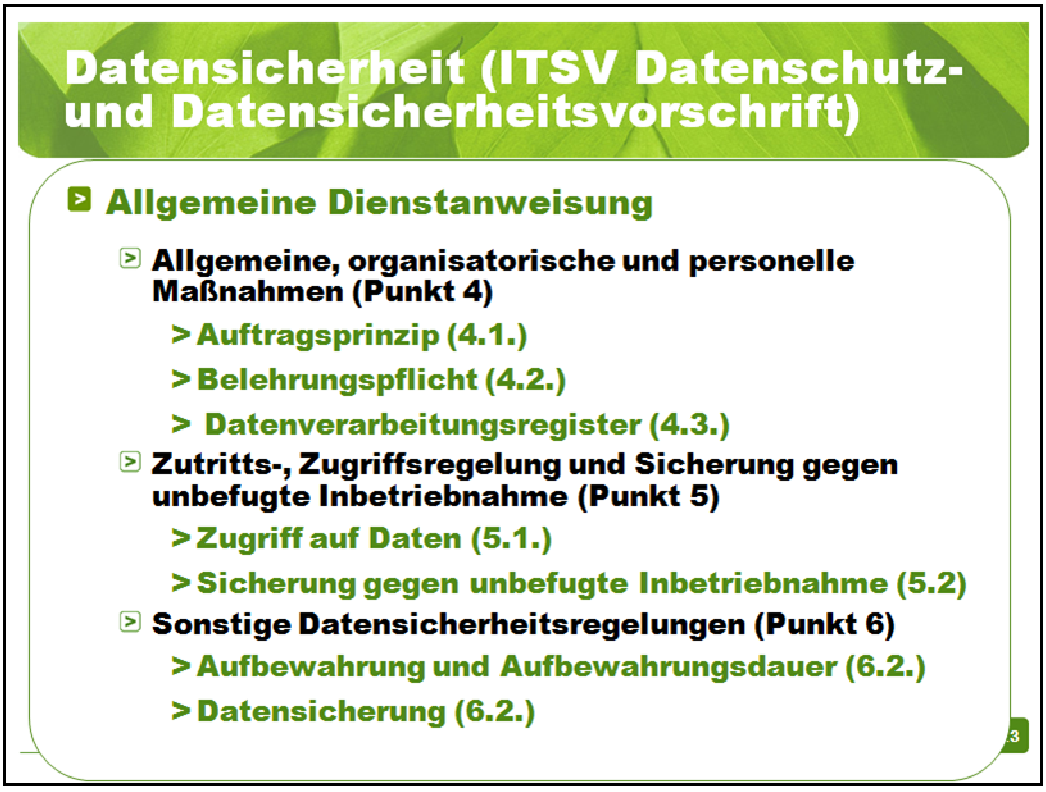
Zutrittsprinzip (Z4): die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters ist zu regeln. Es sind daher Zutrittsschranken (bauliche, technische sowie organisatorische) zu etablieren.

Benutzerverwaltung (Z 5 und 6): die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte ist zu regeln, sowie die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen eine unbefugte Inbetriebnahme abzusichern. Es ist folglich eine nicht zu umgehende (z.B. Einsatz von Passwörter, u.ä.) Benutzerverwaltung zu etablieren.

Protokollierungsverpflichtung (Z7): es ist Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Eine Umgehung dieser Protokollierung, beispielsweise durch Zugriff auf die Datei mittels der Importfunktionen anderer Anwendungen, darf nicht möglich sein. *Übermittlungen* aus beim DVR gemeldeten Datenanwendungen brauchen nicht Protokolliert werden (§ 14 Abs. 3 DSG). Es ist nur eine zweckgebundene Verwendung der Protokolldateien erlaubt (§ 14 Abs. 4 DSG). *Grundsätzlich* beträgt die Aufbewahrungsfrist von Protokolldateien 3 Jahre (§ 14 Abs. 5 DSG). Grundsätzlich dürfen Protokolldateien nur für DS-Zwecke verwendet werden - ausgenommen: § §14 Abs. 4 DSG (org. Krimonal., Strafhöchstausmaß >5Jahre)

Dokumentationsprinzip (Z8): es ist eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern (z.B: Datensicherheitshandbuch, Pflichtenheft).

***Grundvoraussetzung* ist eine ständige effiziente Kontrolle der Einhaltung aller o.a. Prinzipien.**



4.1. Auftragsprinzip

Daten dürfen von den einzelnen Bereichen und von deren Mitarbeitern nur im Rahmen ihrer **Zuständigkeit** verwendet werden und sind immer vertraulich zu behandeln.

Die Verwendung von Daten des HVB sowie der Sozialversicherungsträger (SVT) im Rahmen eines von diesen erteilten Auftrages an die ITSV-GmbH unterliegen zusätzlich den vom HVB und dem jeweiligen SVT für den Einzelfall nachweislich kommunizierten Verwendungsbeschränkungen. Es besteht vor der Bearbeitung dieser Daten für jeden Mitarbeiter die Pflicht, sich über die Existenz und den Inhalt diese Vorschriften durch Nachfrage bei seinem Vorgesetzten zu informieren.

Die Zuständigkeit gründet sich auf gesetzliche Regelungen oder auf Aufträge der Geschäftsleitung. Sie können genereller Natur sein, z.B. sich aus der Geschäftseinteilung ergeben, oder für den Einzelfall erteilt werden. Die Erteilung von Aufträgen hat in der jeweils üblichen Form (z.B. Vordrucke, mündlich, Zuteilung von Schriftstücken, elektronisch) zu erfolgen.

Jeder (generell oder einzelfallbezogen erteilte) Auftrag, welcher auch die Verwendung von **personenbezogenen** Daten (mit)bedingt, muss zum Schutze des Mitarbeiters nachvollziehbar (keinesfalls daher ausschließlich mündlich) erteilt werden. Ein Auftrag hat daher insbesondere die zu verarbeitenden Daten, die zulässigen Verarbeitungsschritte sowie bei Übermittlungen von personenbezogenen Daten die berechtigten Empfängerkreise zu bezeichnen und ist vom Mitarbeiter zum Zwecke seiner Entlastung im Rahmen einer späteren Datenschutzüberprüfung (beispielsweise durch die Datenschutzkommission oder auch im Rahmen von internen Stichprobenüberprüfungen) aufzubewahren. Ein Mitarbeiter darf personenbezogenen Daten ohne nachvollziehbare (einzelfallbezogene oder generelle) Auftragserteilung nicht verwenden. Diese Inhalte können sich beispielsweise auch aus Beschlüssen des Auftraggebers (z.B. Verbandsvorstand, Trägerkonferenz) oder auch generell auf Grundlage der Arbeitsplatzbeschreibung (z.B. Tätigkeit in der Buchhaltungsabteilung impliziert auch generell den Umgang mit Buchhaltungsdaten) ergeben.

Bei Verwendung von personenbezogenen Daten des HVB oder eines SVT (bzw. von diesen verarbeiteten Daten) ist – so der Verwendungsumfang nicht bereits vorab durch entsprechende Beschlüsse der zuständigen Gremien ausrechend klar bestimmt wird – jeweils eine schriftliche Genehmigung des HVB bzw. des SVT (z.B. per e-Mail) durch den Auftragsempfänger (Geschäftsleitung, Bereichsleiter oder im Einzellfall, soweit eine direkte Auftragserteilung zulässig ist, vom Mitarbeiter selbst) einzuholen.

Der schriftliche Nachweis über die Auftragserteilung ist den Auftrags-/Projektunterlagen beizulegen.

Personenbezogene Daten dürfen auch im Rahmen einer erteilten Genehmigung nur so eingeschränkt wie möglich verwendet werden und sind so bald sie nicht mehr benötigt werden, wieder zu löschen oder zu anonymisieren.

Bestehen Zweifel über die Verwendungsgenehmigung bzw. über deren Umfang, ist der zuständige Jurist der ITSV zu befassen.

4.2. Belehrungspflicht

Die ITSV-GmbH und deren Dienstleister haben in ihrem jeweiligen Wirkungsbereich alle involvierten Mitarbeiter in entsprechender Weise über ihre Pflichten gemäß dem Datenschutzgesetz 2000 (DSG 2000) und über ihre sonstigen Verschwiegenheitspflichten nachweislich gem. Anlage B zu belehren. Diese Belehrung ist durch den zuständigen Juristen der ITSV bei der Personalaufnahme bzw. bei externen Mitarbeitern durch den Leiter der (den Auftrag erteilenden) Organisationseinheit im Rahmen der Beauftragung durchzuführen. Die Abhaltung der Belehrung ist von jedem Mitarbeiter durch Unterfertigung des Merkblattes zu bestätigen. Diese Bestätigung ist den jeweiligen Personalunterlagen anzuschließen.

Sollte sich ein Mitarbeiter unsicher sein, ob eine dieser Bestimmungen sich allgemein auf die Verwendung von „Daten“ oder speziell auf die Verwendung von „personenbezogenen Daten“

bezieht, so hat dieser vor der Verwendung der personenbezogenen Daten Rücksprache mit dem zuständigen Juristen der ITSV zu halten. Grundsätzlich ist zu sagen, dass die meist strengeren Bestimmungen nur auf personenbezogene Daten anzuwenden sind und dann „personenbezogen" auch extra im Text angeführt ist. Diese strengeren Bestimmungen brauchen daher nicht auf „einfache" Daten angewendet werden.

Den Mitarbeitern ist es insbesondere untersagt:

- sich Daten unbefugt (d.h. ohne dass hiefür eine ausreichende rechtliche Grundlage für die Verarbeitung bzw. Übermittlung geltend gemacht werden kann) zu beschaffen,
- Daten zu einem anderen Zweck als für ihre eigene Arbeit zu verwenden
- unbefugten Personen oder unzuständigen Stellen Daten mitzuteilen,
- unbefugten Personen oder unzuständigen Stellen Daten zugänglich zu machen.

Die Mitarbeiter sind zur Einhaltung dieser Verbote auch **nach Beendigung** ihrer Mitarbeit bzw. ihrer Funktion verpflichtet.

Insofern Mitarbeiter längerfristig für die ITSV-GmbH tätig werden, haben diese an der jährlich stattfindenden Datenschutzschulung teilzunehmen.

Wenn Mitarbeiter Zweifel betreffend Ihre Berechtigung zur Verwendung von personenbezogenen Daten haben, ist von diesen der zuständige Jurist der ITSV zu befassen.

4.3. Datenverarbeitungsregister

Personenbezogene Daten dürfen im Rahmen von Datenanwendungen nur verwendet werden, wenn diese Datenanwendung bei der Datenschutzkommission (im Datenverarbeitungsregister) gem. § 17 DSG gemeldet wurde oder wenn die verwendeten Datenarten, der Zweck für den diese verarbeitet werden sowie die Übermittlungsempfänger an die diese übermittelt werden können unter eine der von der ITSV betriebenen Standardanwendungen (gem. Standard- und Musterverordnung, BGBl. II Nr. 312/2004) eingereiht werden können.

Die von der ITSV verwendeten Standardanwendungen sind im Anlage A als Bestandteil dieser Sicherheitsbestimmungen angehängt. Es ist zulässig, weniger als die in der Standardanwendung aufgeführten Datenarten bzw. Übermittlungsempfänger etc. zu verarbeiten. Sobald jedoch auch nur eine zusätzliche Datenart (d.h. ein zusätzliches „Datenfeld"; eine zusätzliche „Information") oder ein zusätzlicher Übermittlungsempfänger hinzukommt, bzw. sich der Zweck der Datenverarbeitung nicht mit dem in der Standardverordnung angeführten entspricht, hat vor Aufnahme der Datenverarbeitung eine Meldung der Datenanwendung gem. § 17 DSG durch den zuständigen Juristen der ITSV zu erfolgen.

Die Mitarbeiter sind daher verpflichtet, dem zuständigen Juristen der ITSV die Aufnahme der Verarbeitung personenbezogener Daten (d.h. die Verwendung einer Software (einer Standardsoftware, einer Datenbank, eines selbstgestrickten Programms oder ähnlichem) oder einer manuellen Datenanwendung [z.B. von Karteikästen], die personenbezogene Daten verarbeitet) bereits im Projektstadium (vor der Aufnahme von Softwareentwicklungsarbeiten bzw. der Befüllung einer gekauften Applikation mit personenbezogenen Daten) **durch Übermittlung der in Anlage C angefügten „Applikationsbeschreibung aus datenschutzrechtlicher Sicht" bekannt zu geben. Bei jeder Änderung bzw. falls im Projektstadium noch nicht alle Felder der Applikationsbeschreibung befüllt werden konnten, ist – so rasch wie möglich - erneut eine vollständig ausgefüllte Applikationsbeschreibung an den zuständigen Juristen zu übermitteln. Es ist bei der Projektierung der Einführung einer neuen Datenverarbeitung (und der Änderung einer bestehenden Datenverarbeitung) zu bedenken, dass je nach Art der verarbeiteten Daten bzw. der Datenanwendung VOR Aufnahme der Verarbeitung bis zu 2 Monate dauern kann, bis von der Datenschutzkommission die Software (die Datenverarbeitung/-anwendung) zur Verwendung frei gegeben wird!!!**

5. ZUTRITTS-, ZUGRIFFSREGELUNG UND SICHERUNG GEGEN UNBEFUGTE INBETRIEBNAHME

Die technischen Einrichtungen sind in gesicherten Räumen (d.h. zumindest mit versperrbaren Türen) aufzustellen. Alle Türen dieser Räume müssen grundsätzlich versperrt werden.

Ein Raum, in dem technische Einrichtungen aufgestellt sind, darf während der Betriebszeit grundsätzlich nur von den Bediensteten der ITSV-GmbH betreten werden; andere Personen (z.B. Wartungstechniker, Besucher) dürfen sich nur im Beisein eines Mitarbeiters in solchen Räumen aufhalten. Unbeaufsichtigte Räume, in denen sich technische Einrichtungen befinden, sind stets versperrt zu halten.

Die Mitarbeiter der ITSV-GmbH haben die Pflicht, den Zutritt unbefugter Personen nach Möglichkeit zu verhindern.

Datensichtgeräte (Bildschirme, etc.) sind so aufzustellen, dass der mit ihnen wiedergegebene Inhalt nicht von Unbefugten mitgelesen werden kann.

Durch die Vergabe von Bedienerkennzeichen (Benutzeridentifikation und Passwort) ist sicherzustellen, dass mit dem Zutritt zum Raum noch kein Zugriff zu Datenanwendungen möglich ist.

Den Mitgliedern der Datenschutzkommission (DSK) ist nach Ausweisleistung der Zutritt zu solchen Räumen zu gestatten. Der jeweilige Leiter der überprüften Organisationseinheit, der zuständige Jurist sowie die Geschäftsführung sind davon unverzüglich zu verständigen, damit diese die DSK entsprechend unterstützen können.

5.1. Zugriff auf Daten

Es sind alle dem jeweiligen Stand der Technik entsprechenden und wirtschaftlich zumutbaren Maßnahmen zu treffen, um eine Veränderung oder Vernichtung der Daten durch Programmstörungen zu verhindern, wie die Installation von Virenschutzprogrammen, Firewalls, gestaffelte Zugriffsberechtigungen, etc. Wenn Mitarbeiter auf ihren PCs lokale Administratorenrechte besitzen, ist diese Pflicht auch unmittelbar von diesen einzuhalten. Für Nicht-Techniker bedeutet das, dass Ausfälle dieser Schutzfunktionen (z.B. des Virenscanners) dem zuständigen Systemadministrator unverzüglich zu melden sind.

Der Zugriff auf gespeicherten Daten ist durch programmgesteuerte Zugriffsermächtigungen zu regeln. Die Differenzierung der Zugriffsermächtigung erfolgt über das Bedienerkennzeichen (Benutzeridentifikation) je nach Funktion sowie der Eingabe- und Abfrageberechtigung eines Mitarbeiters.

Nach jeder Änderung der Funktion eines Mitarbeiters sind seine Zugriffsermächtigungen erneut auf deren unbedingte Notwendigkeit zu evaluieren und neu zu vergeben. Erkennt der Mitarbeiter, dass ihm trotz Funktionsänderung nicht mehr unbedingt erforderliche Zugriffsberechtigungen weiterhin erteilt sind, so hat er dies unverzüglich der Systemadministration bekannt zu geben.

Zugriffsberechtigungen dürfen nur an Mitarbeiter erteilt werden, soweit sie diese für die Erfüllung ihrer Aufgaben unbedingt benötigen. Ein nur sehr sporadischer Bedarf an bestimmten Daten rechtfertigt nicht die Erteilung einer jederzeitigen Zugriffsberechtigung. In solchen Fällen sind die Daten von den berechtigten Mitarbeitern im Rahmen der Bestimmungen dieser Datensicherheitsvorschrift einzuholen.

Die Prinzipien zur Festlegung der Personen, die berechtigt sind, über technische Infrastruktur Einsicht in verarbeitete Daten zu nehmen bzw. Veränderungen an Daten vorzunehmen, richten sich nach den in der Punkten 4.1 angeführten Grundsätzen und sind gem. Punkt 5.2 umzusetzen.

Eine Speicherung von Daten hat nur in den jeweils hiefür vorgesehenen Ordnern zu erfolgen. Die Speicherung von personenbezogenen Daten (der Mitarbeiter oder anderer Betroffenen) in allgemein zugänglichen Ordnern ist – mit Ausnahme von Exzerpten aus allgemein zugänglichen Kontakt- bzw. Telefonlisten – ohne die Zustimmung der Betroffenen nicht zulässig.

Erteilte Zugriffsberechtigungen sind von der erteilenden Stelle auf nachvollziehbare Weise (inklusive des Berechtigungszeitraumes) zu dokumentieren.

Nutzen mehrere Personen regelmäßig (z.B. Praktikant(inn)en, studentische Hilfskräfte etc.) einen PC gemeinsam, ist sicherzustellen, dass die personenbezogenen Nutzer- und Anmeldeprofile sowie Datenbeständen ausschließlich den jeweils angemeldeten Nutzern zur Verfügung stehen. Dies gilt auch bei temporärer Nutzung von Mitarbeiter-PCs durch andere Mitarbeiter.

5.2. Sicherung gegen unbefugte Inbetriebnahme

Die Bedienung der Programme hat nur durch jene Mitarbeiter zu erfolgen, denen eine Benutzerkennzeichen/Benutzeridentifikation (BKZ) erteilt wurde.

Die Vergabe von BKZ erfolgt durch den Leiter des Bereichs Hardware bzw. von einem von diesem hiezu ermächtigten Mitarbeiter der ITSV. Dieser hat das zugewiesene BKZ dem jeweiligen Mitarbeiter ausschließlich mündlich mitzuteilen. Er hat dabei dem Mitarbeiter darauf aufmerksam zu machen, dass über das zugewiesene BKZ von ihm keine (d.h. auch keine elektronischen) Aufzeichnungen geführt werden dürfen.

Jeder Mitarbeiter wird bei der ersten Inbetriebnahme eines Endgerätes aufgefordert, ein persönliches Passwort zu vergeben, das dieser geheim zuhalten hat und über das keine Aufzeichnungen geführt werden dürfen. **Jeder Mitarbeiter ist für die unter seinem BKZ getätigten Eingaben und Abfragen verantwortlich**. Er hat daher die Wirksamkeit seines BKZ vor dem Verlassen des PCs oder bei Beendigung des Eingabe- oder Abfragebetriebes aufzuheben (d.h. z.B. den PC zu sperren). Zusätzlich muss der Bildschirmschoner passwortgeschützt eingerichtet werden, sodass die Sperre automatisch nach wenigen Minuten Nicht-Benutzung automatisch aktiviert wird.

Ein Passwort hat aus einer Kombination aus Buchstaben und Ziffern oder Sonderzeichen zu bestehen und zumindest 6 Zeichen aufzuweisen. Zahlen/Buchstabenkombinationen, welche grundsätzlich auch anderen Personen bekannt sein können (z.B. Geburtsdatum, Namen, Wörter laut Wörterbuch) dürfen nicht verwendet werden, da diese leicht mit div. Passwortknackprogrammen herausgefunden werden können. Das Passwort ist von jedem Benutzer periodisch, mindestens jedoch einmal pro Jahr, zu ändern.

Bei Vergessen des Passwortes kann vom Leiter des Bereiches Hardware bzw. von einem von diesem hiezu ermächtigten Angestellten der ITSV ein neues Passwort vergeben werden, welches vom Mitarbeiter unverzüglich zu ändern ist; das Herausfinden des ehemals verwendeten Passwortes ist nicht möglich.

Wurde ein zugewiesenes Benutzerkennzeichen außer dem Mitarbeiter anderen Personen bekannt oder liegt eine diesbezügliche Vermutung vor, wurde ein BKZ missbräuchlich verwendet oder besteht dahingehend ein Verdacht, so ist der Widerruf/die Änderung dieses BKZ umgehend zu veranlassen.

BKZ und Passwörter, welche für den technischen Systembetrieb erforderlich sind, sind für Zwecke der Vertretung im Rahmen der Systemadministration aufzuzeichnen und von der Geschäftsführung in einem Safe zu hinterlegen. Nach Gebrauch der Unterlagen sind diese BKZ und Passwörter zu ändern und erneut im Safe zu hinterlegen.

6. SONSTIGE DATENSICHERHEITSREGELUNGEN

6.1. Aufbewahrung und Aufbewahrungsdauer

Es kann immer wieder beobachtet werden, dass die Altpapiercontainer von Firmen durchsucht werden (sicherlich nicht um Briefmarken zu sammeln). Umso wichtiger ist es jegliche Informationen vertraulich zu behandeln und gegen Einsichtnahme durch Unbefugte zu sichern. Dabei sind personenbezogene Daten und sensible Firmeninformationen mit einem besonders hohen Schutzniveau zu versehen. Um das zu erreichen ist insbesondere folgendes zu beachten:

Die Aufbewahrung von Datenträger (auch Papier) hat nach Maßgabe deren Sensibilität und der technischen und organisatorischen Möglichkeiten versperrt durch die jeweiligen Bereiche zu erfolgen, z.B. versperrbare Schränke, Fächer, Karteikästen, Zimmer.

Protokoll- und Dokumentationsdaten von personenbezogenen Daten sind gemäß § 14 Abs. 5 DSG 2000 maximal drei Jahre aufzubewahren, sofern gesetzlich nicht ausdrücklich anderes angeordnet ist.

Ausdrucken von Dokumenten: Dokumente, welche personenbezogene Daten beinhalten oder sensible Firmeninformationen enthalten (z.B. Unterlagen von Bewerbern, jegliche Emails, diverse Vorstandsberichte, Listen mit Informationen von und über Personen, Zähllisten, Aufstellungen mit Geldwerten, Projektinformationen die alle Träger angehen usw.) sind – soweit sie nicht auf einen Drucker, der sich im selben Raum wie der Benutzer befindet, ausgedruckt werden - **ausschließlich** an einen der vorhandenen Netzwerkdrucker unter Aktivierung der Vertraulichkeitsfunktion zu schicken (Netzwerkdrucker auswählen - Eigenschaften – Papier – Druck an: „Druck vertraulich"). Dokumente, welche nicht unter diesen erhöhten Sorgfaltsmaßstab fallen (und daher deren Abruf durch die Vertraulichkeitsfunktion nicht möglich ist), sind nach deren Ausdruck sofort vom Drucker abzuholen, sodass Dritte diese nicht einsehen können. Die Nichtabholung der Ausdrucke stellt eine Dienstpflichtverletzung dar!

Vernichtung von Ausdrucken: Dokumente, welche personenbezogene Daten beinhalten oder sensible Firmeninformationen enthalten sind **ausschließlich unter Verwendung des Aktenvernichters oder durch eine gesicherte Altpapierentsorgung zu vernichten.**

Die Ablage von Daten ist grundsätzlich nur auf den Fileservern in den jeweils richtigen (und entsprechend geschützten) Ordnern gestattet. Durch die Offlinedateien (auf den Notebooks) können Daten, auch wenn diese in geschützten Bereichen gespeichert werden, leicht ausgelesen werden (Man kann durch das Booten mit alternativen Betriebssystemen (via CD oder Stick) das Windowsdateisystem leicht auslesen). Daher sind auf einem Notebook Daten nur solange zu speichern, wie diese benötigt werden. Gespeicherte sensible Firmeninformationen und personenbezogene Daten sind, sobald diese nicht mehr benötigt werden, umgehend nach Überspielung auf den Fileserver (zwecks zentraler Sicherung) wieder zu löschen. Der Sicherungsablauf ist so einzustellen, dass dieser weitgehend automatisch abläuft.

Bei der Verarbeitung von vertraulichen Daten sind regelmäßig auch alle temporären Dateien zu löschen (z.B. beim Scannen entstehende Dateien).

Auf die Einhaltung der arbeitsverfassungsrechtlichenrechtlichen Vorschriften (insbesondere bestehender Betriebsvereinbarungen und Dienstanweisungen) ist zu achten.

6.2. Datensicherung

Nur durch konsequente Datensicherung ist es möglich, verloren gegangene bzw. zerstörte Datenbestände zu rekonstruieren. Datenverluste können durch Fehler in der Hardware (z.B. eine defekte Festplatte), fehlerhafte Software, Bedienungsfehler oder Stromausfälle verursacht werden. Manuelle Rekonstruktion von nicht gesicherten Daten ist nur selten oder nur unter hohem Kosten- und Zeitaufwand möglich. Der dadurch verursachte Schaden kann daher sehr hoch sein und kann auch von dem Mitarbeiter eingehoben werden, der den Schaden verursacht hat.

Um zerstörte Datenbestände wieder rekonstruieren zu können, sind daher in regelmäßigen Abständen im Generationsverfahren Sicherungskopien zu erzeugen und diese möglichst gesichert aufzubewahren (insbesondere an verschiedenen Orten). Dies wird, soweit die Daten auf den Servern der ITSV-GmbH gespeichert werden, im Rahmen der allgemeinen Sicherungsroutinen von den Systemadminstratoren der ITSV-GmbH durchgeführt.

Daten sind daher dauerhaft nicht auf der Festplatte des eigenen PCs/Notebooks sondern nur auf einem der Netzlaufwerke in dem korrekten Ordner zu speichern/zu verarbeiten.

Wenn länger als 2 Wochen keine Speicherung im entsprechenden Netzwerkordner erfolgen kann, sind unternehmenswichtige Daten auf externen Speichermedien zu sichern (Diskette, CD, DVD, Speicherkarte etc.) und sofort nach neuerlicher Anbindung an das ITSV-Netzwerk in die entsprechenden Netzwerkordner zu speichern. Die verwendeten Speichermedien sind danach zu löschen/zu vernichten.

Den Weisungen der Systemadministratoren in Bezug auf Datensicherung und Datensicherheit ist unmittelbar im selben Umfang wie einer Anweisung des eigenen Bereichsleiters Folge zu leisten!!

6.3. Verwenden von Daten zu Testzwecken

Für Testzwecke sind nach Möglichkeit synthetische Daten ohne Bezug zu einer realen Person zu verwenden. Die Verwendung von Echtdaten (Produktivdaten) zu Testzwecken ist vorab durch den zuständigen Juristen zu genehmigen.

6.4. Datenlöschung und Datenvernichtung

Richtigstellungen und Löschungen von personenbezogenen Daten gemäß § 27 DSG 2000 hat der jeweilige Auftraggeber (HVB, SVT, GF der ITSV) unter Anwendung des für das Aufgabengebiet vorgesehenen Änderungsdienstes (Regelungswerk für die Änderungen wie beispielsweise gesetzlich vorgesehene Löschungsfristen etc.) durchzuführen oder zu veranlassen.

Nicht mehr benötigte Daten, insbesondere abgelaufene Datenbestände, Fehlausdrucke oder Erfassungsformulare sowie nicht anonymisierte Testdaten, sind zu löschen bzw. so zu vernichten, dass eine Rekonstruktion nicht möglich ist. Wenn aus Gründen der Wirtschaftlichkeit die physische Löschung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind diese Daten bis dahin logisch und sodann physisch zu löschen. Die entsprechenden Datenträger sind bis zur physischen Löschung versperrt aufzubewahren.

Laufend auszuscheidende Belege (Verarbeitungsaufträge, Aufzeichnungen über aufgezeichnete Daten, Ausdrucke) sind, sofern sie nicht zur ständigen Aufbewahrung bestimmt sind, einer gesicherten Vernichtung zuzuführen oder derart unkenntlich zu machen, dass eine Beziehung zu einer (natürlichen oder juristischen) Person mit höchstmöglicher Wahrscheinlichkeit nicht mehr hergestellt werden kann.

Für den Fall, dass technische Einrichtungen zu Servicezwecken aus dem Sicherheitsbereich entfernt (oder Altgeräte entsorgt) werden müssen, ist dafür Sorge zu tragen, dass eine unautorisierte

Verwendung nicht stattfinden kann (z.B. dass nicht mit durch am Gerät noch vorhandene Voreinstellungen automatisiert in das SV-Netz eingedrungen werden kann oder auf der technischen Einrichtung verarbeitete Daten eingesehen bzw. rekonstruiert werden können).

Bei einer Überführung eines Servers, PCs oder von einzelnen Datenträgern (z.B. Festplatten) zu einer Fremdfirma, sind auf der technischen Einrichtung verarbeitete Daten vom zuständigen Systemadministrator jedenfalls mit einem sicheren Verfahren (z.B. Mehrfachüberschreiben der Daten) zu löschen. Die Durchführung dieser Sicherheitsmaßnahmen ist nachvollziehbar zu dokumentieren. Nicht mehr benötigte Datenträger (CDs, Disketten, DVDs, Festplatten etc.) müssen ebenfalls an die Systemadministration zurückgegeben werden, von der sie fachgerecht zu entsorgen sind.

Die Entsorgung kann auch von dem o.a. Prozedere abweichen, wenn sie durch ein entsprechend zertifiziertes Fachunternehmen durchgeführt wird.

6.5. Transport von Daten

Beim Transport von Datenträgern sind diese gegen unbefugten Einblick bzw. Zugriff ausreichend zu sichern. Bei Versendung außer Haus ist grundsätzlich die Form der eingeschriebenen Sendung, allenfalls auch als Wertpaket, zu wählen.

Dateien mit vertraulichem Inhalt oder mit personenbezogenen Daten Dritter **dürfen, sobald eine bestimmte Methode von der ITSV als Service ermöglicht wird** (z.B. eine bestimmte Verschlüsselungsmethode, eine Web-Zugangsmöglichkeit mit Benutzeridentifikation und Passwort etc.), **an externe Stellen nur mit dieser zur Verfügung gestellten Methode** oder anderen sicheren Verschlüsselungsmethoden oder über sichere Netze **versendet werden**. Sichere Netze sind Netze, die eine Zugriffsmöglichkeit von Externen auf die übermittelten Daten auf Grund der verwendeten Technik soweit wie möglich ausschließt.

Bis dahin, ist eine Versendung von personenbezogenen Daten über nicht sichere Netze nur mit Zustimmung der Betroffenen zulässig (z.B. Verschlüsselung, VPN).).

Vor der Übermittlung von personenbezogenen Daten ist der zuständige Jurist der ITSV zu befassen, welcher zu bestätigen hat, dass die Übermittlung zulässig ist.

Der Versand von Dateien via Email stellt eine Übermittlungsform dar, welche der einer Postkarte gleichkommt. Jedes Analyseprogramm im Datenstrom (z.B. Proxy, Emailserver, Firewall und auch diverse andere Geräte) ist in der Lage, diese Informationen (inkl. der Anhänge) zu lesen. Die Inhalte (inkl. aller Anhänge) werden oftmals zwischengespeichert und sind teilweise einer langjährigen Archivierung unterworfen. Oftmals enthalten die Office Dateien (Word, Excel, Powerpoint) auch Reste von vorherigen Entwurfstadien, sodass es ein Leichtes ist, die verschiedenen Versionen eines Dokumentes nachzuvollziehen. Ist die Versendung derartiger Dokumente (zwecks Weiterbearbeitung im Originalformat) daher nicht unbedingt erforderlich, ist die Umwandlung in ein PDF Dokument vorzunehmen, wobei in jedem Fall die Sicherheitsfeatures (zumindest ein Passwort zum Öffnen und eine Verschlüsselung) zu setzen sind. Informationen hiezu können von der Systemadministration erfragt werden. Werden die **Dateien über ein sicheres Netz** (verschlüsselte Dateiübertragung) versendet, ist eine **Umwandlung in PDF jedoch nicht erforderlich**.

6.6. Kategorisierung von Daten und Aufgabengebieten

Aus Gründen der Zweckmäßigkeit, Wirtschaftlichkeit und Sparsamkeit ist es sinnvoll, nicht für alle Daten- und Aufgabengebiete einen gleich hohen Aufwand (für die Datensicherheit) zu betreiben.

Insofern die Verarbeitung von personenbezogenen Daten betroffen ist, müssen diese Maßnahmen jedoch unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Unterstützung bei der Entscheidungsfindung kann jederzeit vom zuständigen Juristen der ITSV angefordert werden.

6.7. Auskunftserteilung gem. § 26 DSG (an den Betroffenen betreffend die über ihn verarbeiteten Daten)

Zur Auskunftserteilung an den Betroffenen gemäß § 26 DSG 2000 ist der jeweils zuständige Auftraggeber verpflichtet. Ein Auskunftsersuchen kann an die ITSV-GmbH hinsichtlich von „eigenen" Daten der ITSV oder Daten von Auftraggebern der ITSV-GmbH (wie beispielsweise des Hauptverbandes der VAEB und/oder anderer SVT, deren Daten für die die ITSV als Dienstleister Daten pflegt) betreffen.

Ein an die ITSV gestelltes Auskunftsbegehren gem. § 26 DSG über personenbezogene Daten des antragstellenden Betroffenen, welche durch die ITSV als Dienstleister für den HVB oder einen SVT verarbeitet werden, ist unverzüglich, möglichst noch am selben Tag **– über den zuständigen Juristen der ITSV-GmbH -** an die vom zuständigen Auftraggeber (HVB, SVT) namhaft gemachte Dienststelle, unter Beifügung der über den Antragsteller verarbeiteten Daten, weiterzuleiten.

Eine Auskunft gem. § 26 DSG über personenbezogene Daten des antragstellenden Betroffenen, welche durch die ITSV als Auftraggeber verarbeitet werden, ist - nach Auftragserteilung durch die Geschäftsführung - so rasch als möglich, jedenfalls jedoch innerhalb von 8 Wochen nach Einlangen des Auskunftsbegehrens (oder falls erforderlich nach Einzahlung des Kostenersatzes bzw. Konkretisierung des Auskunftsbegehrens) ausschließlich durch den zuständigen Juristen der ITSV nach folgenden Grundsätzen zu erteilen:

Eine Auskunft darf nur erteilt werden, wenn die Identität des Betroffenen in unbedenklicher Form festgestellt werden konnte. Auskünfte über Telefon, Telefax oder e-mail sind nur dann zulässig, wenn hiefür Sicherheitsvorkehrungen (Standleitungen, Rückruf, Verschlüsselungsverfahren, elektronische Signatur etc.) genützt werden. Die Auskunftserteilung ist hinsichtlich Form und Inhalt zu dokumentieren.

Auskünfte dürfen nur in folgenden Fällen gegeben werden:

- an den Betroffenen über die eigenen Daten
- an behördlich bestellte Vertreter auf Grund ausdrücklicher Bestellungsurkunden, Beschlüsse oder Aufträge,
- an gesetzliche Vertreter (Erziehungsberechtigte), jedoch in den Fällen, in denen ein Kind das 14. Lebensjahr bereits vollendet hat, nur dann, wenn vor der Auskunftserteilung bescheinigt ist, dass die Auskunftserteilung nicht gegen dessen Interessen verstößt. Diese Bescheinigung hat der Art der angeforderten Daten zu entsprechen und ist bei sensiblen Daten nachvollziehbar festzuhalten.

Die Auskunft ist so zu erteilen, dass bei durchschnittlichem Verständnis vom Betroffenen erwartet werden kann, er werde Inhalt und Aussage der Auskunft zweifelsfrei verstehen. Abkürzungen dürfen in der Auskunft verwendet werden, wenn erwartet werden kann, dass der Betroffene sie versteht oder wenn ihre Bedeutung dem Auskunftsschreiben zu entnehmen ist.

Wenn personenbezogene Daten auf Grund einer

- Standardanwendung (§ 17 Abs. 2 Z 6 DSG) oder
- Musterverordnung (§ 19 Abs. 2 DSG)

verwendet werden ist dem Betroffenen bei einer Anfrage nach § 26 DSG mitzuteilen, dass bestimmte Datenarten des Betroffenenkreises, zu dem auch der Betroffene gehört, an einen bestimmten Empfängerkreis planmäßig übermittelt werden. Die hievon betroffenen Datenarten, Betroffenenkreise und Empfängerkreise sind in der Auskunft zu nennen.

Das Auskunftsrecht umfasst auch Auskünfte aus Protokolldaten über Zugriffe auf Daten des Betroffenen, es sei denn es werden dadurch überwiegende Interessen des Auftraggebers oder eines Dritten bzw. öffentliche Interessen verletzt.

Eine Auskunft schließt auch Daten des Auskunftswerbers ein, die unter einem Ordnungsmerkmal eines Dritten (z. B. eines Dienstgebers, behandelnden Arztes) bzw. unter einem anderen Sachverhalt/Ordner gespeichert sind, soweit der Auskunftswerber einen geeigneten Hinweis zur Feststellung dieses Ordnungsmerkmales/Sachverhaltes gibt.

Von der Bearbeitung eines Auskunftsersuchens ist abzusehen, wenn der Betroffene nicht am Verfahren mitwirkt (d.h. beispielsweise die Datenverarbeitung nennt, in welcher möglicherweise Daten über ihn verarbeitet werden oder zumindest einen Sachverhalt schildert, aus dem geschlossen werden kann, in welcher Datenverarbeitung mit hoher Wahrscheinlichkeit Daten über den betroffenen Antragsteller verarbeitet werden). Auf diesen Umstand ist der Betroffene in einer Aufforderung zur Mitwirkung (Abs. 7, § 26 Abs. 4 DSG 2000) hinzuweisen. Als „Datenverarbeitung" sind in diesem Zusammenhang auch bloße Ordner zu verstehen in denen - sachbezogen – personenbezogene Daten verarbeitet werden.

Kostenersatz:
Auskünfte nach § 26 DSG 2000 sind unentgeltlich zu erteilen, wenn sie den aktuellen und direkt abfragbaren Datenbestand einer Datenanwendung betreffen und wenn der Auskunftswerber im laufenden Kalenderjahr zum selben Aufgabengebiet noch kein Auskunftsersuchen an den Auftraggeber gestellt hat. In allen anderen Fällen kann ein pauschalierter Kostenersatz von 19 € verlangt werden. Ein höherer Kostenersatz darf nur dann verlangt werden, wenn tatsächlich höhere Kosten entstanden sind. Diese tatsächlichen Kosten sind an Hand der vollständigen Kosten der verbrauchten Arbeitszeit und konkreten Bezüge der hiefür eingesetzten Personen sowie des sonstigen Aufwandes (Material- und Sachaufwand etc.) zu errechnen (Vollkostenrechnung). Die Kosten sind vor Auskunftserteilung an den Betroffenen diesem durch das F/C der ITSV vorzuschreiben. Eine Barzahlung der Kosten ist nicht zulässig.

6.8. Übermittlungen / Auskunftserteilungen an Dritte

Eine Auskunftserteilung über personenbezogene Daten an Dritte außerhalb der ITSV-GmbH ist nur zulässig, wenn eindeutig die Berechtigung des Datenempfängers zum Empfang der Daten geklärt ist. Der Empfänger der Daten (eine natürliche Person) ist eindeutig zu identifizieren. Telefonische Auskünfte sind nur im Wege eines Rückrufes zu erteilen. Ausnahmsweise, wenn keine Bedenken hinsichtlich der Person des Anrufers und dessen Berechtigung, Auskünfte zu erhalten, bestehen, kann die Auskunft unmittelbar erfolgen. Die erfolgte Datenübermittlung (was, wann, warum und an wen) ist schriftlich oder automationsunterstützt festzuhalten und innerhalb der Löschungsfristen (=Skartierungsfristen) jederzeit abrufbar zu halten.

Officedokumente, welche personenbezogenen Daten enthalten, dürfen nur in Ausnahmefällen per eMail verschickt werden, wenn es die weitere Bearbeitung durch den Empfänger erforderlich macht. Sie sind in diesem Fall verschlüsselt zu übermitteln. Im Regelfall ist das Dokument vor dem Versand in Adobe PDF zu konvertieren, wobei in jedem Fall die Sicherheitsfeatures (zumindest ein Passwort zum Öffnen und eine Verschlüsselung) zu setzen ist. Werden die Dateien über ein sicheres Netz (verschlüsselte Dateiübertragung) versendet, ist eine Umwandlung in PDF jedoch nicht erforderlich. Müssen die Daten vom Empfänger weiterverarbeitet werden können, sind diese mit dem jeweiligen Programm (z.B. MS-Word) dokumentbezogen zu verschlüsseln.

6.9. Protokollierung von personenbezogenen Daten

Soweit dies unter Bedachtnahme auf § 14 Abs. 2 Schlusssatz erforderlich ist (Wirtschaftlichkeitsabwägung), sind gem. § 14 Abs. 2 Z 7 DSG 2000 vom Auftraggeber der Datenverwaltung (selbst oder über den beauftragten Dienstleister) Protokolle zu führen, um die tatsächlich durchgeführten Verwendungsvorgänge - wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollziehen zu können. Die Protokollierung ist so zu gestalten, dass auch Zugriffe der eigenen Mitarbeiter nachvollzogen werden können.

Eine Protokollierung von Übermittlungen solcher Daten, die im System verarbeitet werden, hat gem. § 14 Abs. 3 DSG so zu erfolgen, dass Anträge auf Auskunftserteilung gem. § 26 DSG entsprochen werden kann. Eine Protokollierung kann entfallen, wenn

- Daten auf Grund einer Standardanwendung (§ 17 Abs. 2 Z 6 DSG) oder Musterverordnung (§ 19 Abs. 2 DSG) verwendet werden (wie bei den Datenanwendungen, bei denen die ITSV-GmbH Auftraggeber ist (siehe Anlage A),

- Daten nach § 46 DSG für wissenschaftliche Forschung und Statistik verwendet werden oder

- Daten gesammelt als Grundlage gesetzlich vorgesehener konkreter weiterer Verwendungen (z.B. zur Vorbereitung von Wahlen nach § 45 Arbeiterkammergesetz) übermittelt werden.

Protokolle betreffend Datenanwendungen, deren Hauptzweck die Verarbeitung von personenbezogenen Daten darstellt, sind mindestens 11 Jahre und höchstens 31 Jahre in automationsunterstützt lesbaren Form aufzubewahren.

Protokoll- und Dokumentationsdaten dürfen nicht für Zwecke verwendet werden, die mit ihrem Ermittlungszweck – das ist die Kontrolle der Zulässigkeit der Verwendung des protokollierten oder dokumentierten Datenbestandes – unvereinbar sind. Unvereinbar ist insbesondere die Weiterverwendung zum Zweck der Kontrolle von Betroffenen, deren Daten im protokollierten Datenbestand enthalten sind, oder zum Zweck der Kontrolle jener Personen, die auf den protokollierten Datenbestand zugegriffen haben, aus einem anderen Grund als jenem der Prüfung ihrer Zugriffsberechtigung.

6.10. Benutzung von Endgeräten (PC, Notebooks, PDA, Mobiltelefone und ähnliches)

6.10.1 firmeneigene Endgeräte

Die Benutzung von Endgeräten für private Zwecke ist – ausgenommen es bestehen Einzelvereinbarungen (z.B. Dienstvertrag - Handynutzung) oder das Recht wird in gesonderten Dienstanweisungen erteilt, nicht gestattet. Insbesondere dürfen keine von dem Bereich Hardware nicht freigegebenen Anwendungen oder Programme installiert und betrieben werden.

Eine Ausnahme besteht nur für die private Nutzung der gemäß dieser Dienstanweisung (korrekt bzw. entsprechend dieser Dienstanweisung) installierten Software auf den zur Verfügung gestellten Laptops für **rechtmäßige** Zwecke in der Freizeit. Dies allerdings nur unter der Voraussetzung, dass der Mitarbeiter den in dieser Dienstanweisung und allfälligen weiteren Dienstanweisungen und Betriebsvereinbarungen (bzgl. die Laptopverwendung) vorgesehenen Kontrollmaßnahmen ebenfalls akzeptiert. Die ITSV-GmbH hat jederzeit das Recht und die Pflicht den Laptop darauf zu überprüfen, ob dieser nur für rechtmäßige Zwecke benutzt wird. Nutzt der Mitarbeiter den Laptop daher auch für private Zwecke, nimmt er zu Kenntnis, dass er eine Überprüfung (auch allfällig angelegter privater Ordner/Dateien) nicht mit der Berufung auf das Datenschutzgesetz oder andere Persönlichkeitsrechte verweigern darf. Ist der Dienstnehmer mit der Überprüfung der privat genutzten Bereiche des Laptops nicht einverstanden, darf er den Laptop ausschließlich für berufliche und keinesfalls für private Zwecke nutzen.

Ausgenommen von den Einschränkungen dieser DA ist die Nutzung von Terminkalendersoftware im Rahmen der Büroautomatisierung (→Handy- SynchronisierungsSW).

Die Umgehung von Sicherheitseinstellungen (Virenschutz, Firewall usw.) ist (auch im Rahmen der erlaubten privaten Laptop Benutzung) keinesfalls gestattet und stellt eine grobe Dienstpflichtverletzung dar, welche auch ohne Abmahnung eine Entlassung rechtfertigt. Es wird auch ausdrücklich darauf hingewiesen, dass auf den Client-PCs im Netzwerk keine Serverdienste zu installieren und zu betreiben sind (z.B. Telnet-, FTP- oder WEB-Server).

Ein Handy darf nicht als Modem zum Zwecke der Umgehung der firmeneigenen Schutzeinrichtungen (z.B. Firewall) benutzt werden. Die Verwendung der firmeneigenen UMTS-Karte hat ausschließlich für dienstliche Zwecke zu erfolgen.

6.10.2. private Endgeräte

Die berufliche Verwendung von privaten Endgeräten (PC, Laptops) für Zwecke der ITSV-GmbH ist nicht gestattet.

6.11. Verwendung von nicht von der ITSV-GmbH zur Verfügung gestellter Software

Alle Programme auf den PCs unterliegen urheberrechtlichen Lizenzbestimmungen. Jedes Programm darf daher in der Regel mit einer Lizenz nur auf einem PC zur selben Zeit eingesetzt werden. Die Nutzung (d.h. auch das Kopieren bzw. die Vervielfältigung) von Programmen ohne zusätzliche Lizenz wird daher von Gesetzes wegen mit hohen Geld und mit Gefängnisstrafen geahndet.

Die widerrechtliche Verwendung (Kopieren, aber auch bloßes Ablaufen lassen etc.) von Programmen kann der ITSV nicht nur einen nicht einzuschätzenden finanziellen sowie Image-Schaden zufügen, sondern seit in Kraft treten des Verbandsverantwortlichkeitsgesetzes mit 01.01.2006 auch zu einer strafrechtlichen Verurteilung der ITSV als juristischer Person führen. Eine **strafrechtliche Verurteilung der ITSV** kann wiederum zu einem Verbot an der Teilnahme von bestimmten Vergabeverfahren und auch – gerade wenn man den Aufgabenbereich der ITSV bedenkt - einen nicht wieder gutzumachenden Image-Schaden herbeiführen.

Neben der ITSV wird immer auch derjenige **Mitarbeiter** strafrechtlich (Freiheitsstrafe bis zu sechs Monaten oder mit Geldstrafe bis zu 360 Tagessätzen) und auch zivilrechtlich (Abschöpfung von Bereicherungen, Lizenzzahlungen, Schadenersatz) verfolgt, der den Gesetzesverstoß verübt hat. Ebenso werden die verantwortlichen **leitenden Angestellten** der ITSV strafrechtlich verfolgt, wenn sie nicht ausreichende Maßnahmen ergriffen haben, um einen Verstoß von einem Bediensteten oder Beauftragten gegen immaterialgüterrechtliche Bestimmungen (d.h. „im Vorhinein“) zu verhindern („Unterlassungsdelikt“).

Das wissentliche Verwenden - das ist jede Art der Handhabung von Daten in einer Datenanwendung, also sowohl das Verarbeiten als auch das externe und interne Übermitteln von Daten - sowie das Installieren von Computerspielen und anderer nicht ausreichend lizenzierter bzw. technisch überprüfter Fremdsoftware, über E-Mail, Internet (WWW), Diskette, CD-ROM etc. ist daher ausdrücklich verboten.

Zur Vermeidung strafrechtlicher Konsequenzen werden daher stichprobenartig Überprüfungen der auf der firmeneigenen Hardware verwendeten Software/Lizenzen durchgeführt werden. Das Prüfungsergebnis ist mit der vom Systemadministrator zu führenden Liste (welcher Benutzer hat welche Lizenzberechtigungen) zu vergleichen.

Falls die dienstliche Notwendigkeit zur Installation von zusätzlicher Software besteht, so hat dies ausnahmslos nur über hiezu befugte Mitarbeiter der ITSV (oder mit deren ausdrücklicher Genehmigung) nach folgenden Richtlinien zu erfolgen.

Vor Installation ist die Software sowohl von rechtlicher (vom zuständigen Jurist) wie auch von technischer Seite (vom zuständigen Systemadministrator) freizugeben. Hiezu ist vom zuständigen Systemadministrator eine Liste der für die Verwendung auf den einzelnen Laptops genehmigten Softwarelizenzen zu führen. Auf dieser Liste ist auch die Genehmigung durch den zuständigen Juristen (samt dessen rechtlicher Begründung für die zulässige Verwendung der Lizenz) festzuhalten. Von der Systemadministration ist hiezu eine Aufstellung der auf der firmeneigenen Hardware (PCs der einzelnen Mitarbeiter und Server) installierten Software zu führen bzw. aktuell zu halten. Einzelne SW-Komponenten, wie z.B. Treiber, sind hievon nicht umfasst

Der Austausch von Lizenzen untereinander ist - ohne Genehmigung der Systemadministration (welche die entsprechenden Listen zu aktualisieren hat) - verboten.

Die Systemadministration ist berechtigt - generell oder einzelfallbezogen - technische Vorkehrungen zu treffen, die die Installation von nicht genehmigter Software verhindern.

Dem Benutzer ist nicht erlaubt, Geräte zu öffnen oder zu manipulieren. Das Öffnen des PC-Gehäuses und das Durchführen von Veränderungen an der PC-Hardware (z.B. Ein- bzw. Ausbau von Festplatten, Speicherbausteinen etc.) ist nur der Systemadministration erlaubt.

7. Intra-/Internetauftritt der ITSV und Informationsserver/-foren

Die ITSV betreibt einen zentralen Informations-Server bzw. diverse Foren, Gästebucher u.ä. und bietet die Möglichkeit, sich daran zu beteiligen und Form und Inhalt des Informationsraums eigenständig und eigenverantwortlich zu gestalten. Bei Etablierung eines derartigen Dienstes ist vom Leiter der inhaltlich zuständigen Organisationseinheit ein Foren/Gästebuch- Verantwortlicher zu ernennen.

Die Inhalte des zentralen Informations-Servers haben mit dem gesetzlichen Aufgabenbereich der ITSV zu tun. Unzulässig ist jede Dateneinbringung, welche die öffentliche Ordnung und Sicherheit oder die Sittlichkeit gefährdet und daher geeignet ist, den Interessen der ITSV oder ihrem Ansehen in der Öffentlichkeit zu schaden oder die gegen geltende Gesetze oder Verordnungen verstößt. Insbesondere betrifft dies auch die Beschimpfung und die Vernaderung/Verunglimpfung von anderen Personen. Im Fall von Verstößen hat der zuständige Foren/Gästebuch-Verantwortliche der ITSV den Zugriff auf die betreffenden Inhalte mit sofortiger Wirkung sperren oder zu löschen. Hierüber ist auch der zuständige Jurist der ITSV zu informieren.

8. BEAUFTRAGTER FÜR DATENSCHUTZ UND DATENSICHERHEIT

Die Überwachung der Einhaltung dieser Sicherheitsvorschrift obliegt dem zuständigen Juristen der ITSV GmbH (als Datenschutzbeauftragtem), **der berechtigt ist, bei Gefahr im Verzug Abweichungen von dieser Sicherheitsvorschrift anzuordnen.** Diesen Anordnungen ist unverzüglich nachzukommen. Über die angeordneten Abweichungen ist von diesem unverzüglich der Geschäftsleitung Bericht zu erstatten. Die Anordnungen sind schriftlich festzuhalten. Bestehende Betriebsvereinbarungen sind zu befolgen.

Dem Datenschutzbeauftragten obliegen insbesondere die Sammlung und Aktualisierung sämtlicher Sicherheitsregelungen, Risikoanalyse, Vorschläge für die Sicherheitsmaßnahmen, Auskunftserteilung für alle Mitarbeiter sowie die Kontrolle der Einhaltung der Sicherheitsanordnungen durch Stichproben

im Rahmen der bestehenden Betriebsvereinbarungen. Die Dokumentation über alle Datensicherheitsmaßnahmen ist mindestens 11 Jahre aufzubewahren.

Er hat dafür Sorge zu tragen, dass in die aktuelle Fassung dieser Datensicherheitsvorschrift jederzeit Einsicht genommen werden kann.

Auf Anforderung durch die Datenschutzkommission sind ihr diese Unterlagen zur Kenntnis zu bringen.

Die Mitarbeiter aller Bereiche sind verpflichtet, sich untereinander sowie den zuständigen Organisationsleiter auf allfällige Sicherheitsmängel aufmerksam zu machen und Verstöße gegen die Sicherheitsbestimmungen zu melden. Der Organisationsleiter leitet diese Informationen an den zuständigen Juristen der ITSV weiter.

9. SYSTEMADMINISTRATION

Die für die Systemadministration/Systembetreuung tätigen Mitarbeiter haben Ihre Aufgaben unter größtmöglicher Schonung der Privatsphäre der Mitarbeiter sowie Dritter durchzuführen.

Die Einschau auf zulässigerweise privat verarbeitete Dateien ist unzulässig. Inhaltliche Überprüfungen (darunter ist auch die Einschau in private Ordner zu verstehen, ohne dass Dateien geöffnet werden) sind ausschließlich auf Grundlage und im Rahmen dieser Dienstanweisung sowie der allenfalls bestehenden Betriebsvereinbarungen zulässig.

Aufgrund des Umfanges der Zugriffsmöglichkeiten der Mitarbeiter der Systemadministration ist in diesem Zusammenhang nochmals auf die bestehenden arbeitsrechtlichen und gesetzlichen Geheimhaltungsverpflichtungen (insbesondere bestehende Betriebsvereinbarungen sowie § 15 Datenschutzgesetz) zu verweisen, denen die Systemadministratoren unterliegen. Die Einsicht in personenbezogene Daten ohne Auftrag oder die Weitergabe von im Rahmen ihrer Tätigkeit gesammelten Daten/Informationen durch Systemadministratoren an andere Mitarbeiter (auch an ihre Vorgesetzten außerhalb deren im (unten angeführt) zu erstellenden Berechtigungskonzept festgelegten Zuständigkeiten) oder externe Personen außerhalb ihrer Dienstpflichten und unter Umgehung der oben angeführten Zulässigkeitsvoraussetzungen, stellt eine **schwere Dienstpflichtverletzung** dar, die – ausgenommen es lag ein besonderer technischer Notfall vor – je nach schwere des Falles zur fristlosen Entlassung des Systemadministrators führen kann.

Neben personenbezogenen Daten ist in diesem Zusammenhang insbesondere auch zu betonen, dass Zugriffsberechtigungen auf Berichte der Gremien der ITSV und der Sozialversicherung (HVB, SV-Träger) besonders sensibel zu gestalten sind und daher nur im unbedingt nötigem Ausmaß weitergeben bzw. Dritten (auch innerhalb der ITSV und der Sozialversicherung) zugänglich gemacht werden dürfen (Aufsichtsratsberichte, Berichte des Verbandsvorstandes, der Trägerkonferenz, PLAs, Informationen über Interna der Träger etc.)

Erstellung und Überwachung von Berechtigungskonzepten: Jeder Systemadministrator hat, soweit auf von ihm verwaltete Daten/Fileordner/Applikationen Zugriffe auch von Dritten möglich sind, für die von ihm verwalteten Zugriffsmöglichkeiten ein Berechtigungskonzept zu erstellen und diese Zugriffsberechtigungen – auf nachweisliche Art und Weise - zu verwalten. Dazu gehört insbesondere auch - im Rahmen des wirtschaftlich sinnvollen - die Einführung von Überwachungsmechanismen, die gewährleisten, dass bei einem Wechsel von Aufgaben eines im Rahmen des Berechtigungskonzeptes zugriffsberechtigten Mitarbeiters die von diesem nicht mehr benötigten Zugriffsberechtigungen **unverzüglich gelöscht werden**.

Ist der Systemadministrator nur für die technische Durchführung, nicht aber für die inhaltliche Festlegung der Zugriffsverantwortlichkeiten zuständig **(„technischer Systemadministrator“)**, hat der inhaltlich Verantwortliche **(„inhaltliche Systemadministrator“)** das Berechtigungskonzept zu erstellen. Der technische Systemadministrator hat die Zugriffsberechtigungen - ausschließlich wie im Berechtigungskonzept durch den inhaltlich Verantwortlichen festgelegt - zu verwalten. Im Zweifelsfall hält er vor Vergabe von Berechtigungen Rücksprache mit dem inhaltlichen Systemadministrator. Auch ein Zugriff des Vorgesetzten eines (technischen und/oder inhaltlichen) Systemadministrators ist nur im Rahmen des Berechtigungskonzeptes zulässig. Der technische Systemadministrator ist nur im Rahmen seiner technischen Zuständigkeiten dafür verantwortlich, dass Zugriffe im Rahmen der im

Berechtigungskonzept festgelegten Regeln erfolgen und für das Aufzeigen von bestehenden Zugriffsmöglichkeiten an seinen Vorgesetzten, der hiefür den inhaltlichen verantwortlichen Systemadministrator bestimmt. Für die Einhaltung der übrigen Bestimmungen ist ausschließlich der inhaltliche Systemverantwortliche verantwortlich.

Das Berechtigungskonzept und dessen Überwachungsmechanismen sind vom inhaltlichen Systemadministrator mit dem für Datenschutz zuständigen Juristen abzustimmen, da dieser als Datenschutzbeauftragter die von ihm zu führende Liste der Datensicherheitsmaßnahmen zu erstellen und laufend zu ergänzen hat.

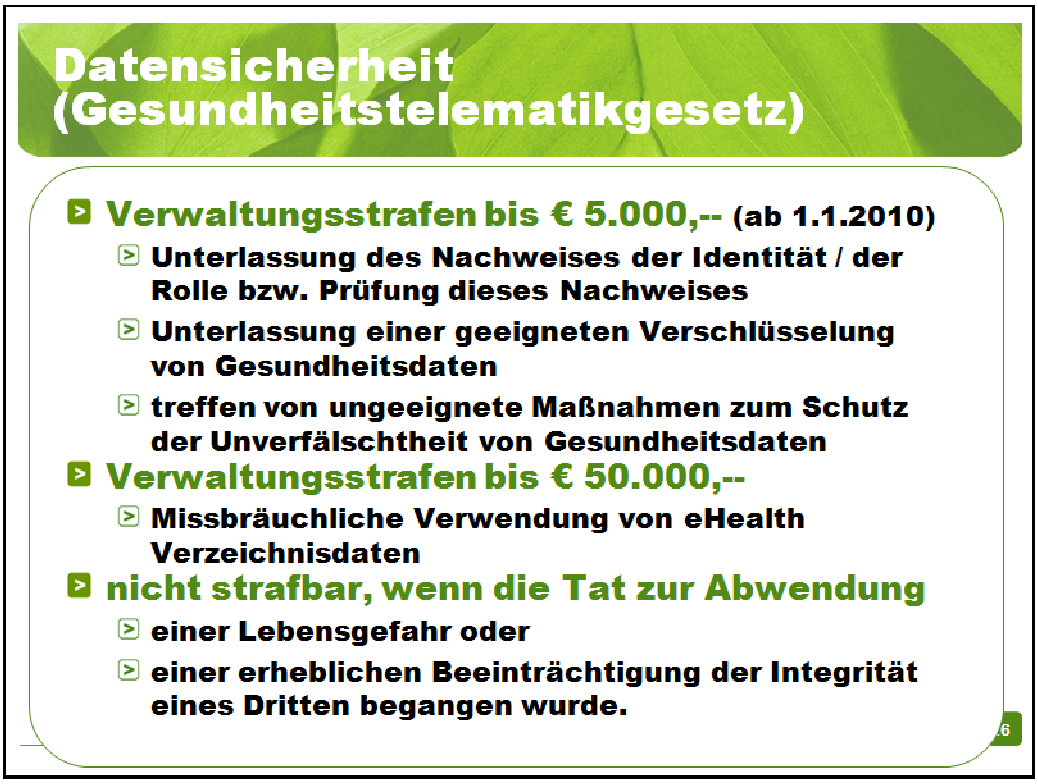
Diese Bestimmungen richten sich unmittelbar an den inhaltlichen und den technischen Systemadministrator (kann auch nur eine Person sein) und nicht an deren Vorgesetzte. Der zuständige Jurist hat jedoch diese Berechtigungskonzepte – nach Absprache mit dem zuständigen Bereichsleiter und Einholung der Stellungnahmen der übrigen betroffenen Bereichsleiter im Management-JF - zur Genehmigung der Geschäftsführung vorzulegen. In Folge hat er die unter Punkt 12 geführte Liste der Systemadministratoren laufend zu ergänzen und an alle Mitarbeiter zu kommunizieren. In dieser Liste ist zwischen dem inhaltlich verantwortlichen und dem bloß technisch verantwortlichen (durchführenden) Systemadministrator zu unterscheiden.

10. EXTERNE DIENSTLEISTUNGEN

Sollten technische Einrichtungen von Fremdfirmen implementiert, gewartet oder bei Anwenderschulungen benützt werden, und Personal dieser Firmen hierbei Zugriff auf personenbezogene Daten erlangen, so ist darauf zu achten, dass bereits vor Tätigkeitsaufnahme für den jeweiligen Zweck der Dienstleistung mit der Fremdfirma ein Dienstleistervertrag gemäß den §§ 10ff DSG abgeschlossen worden ist (Muster siehe Anlage D) und die konkret eingesetzten Dienstnehmer jeweils Geheimhaltungsverpflichtungserklärungen unterschrieben haben.

11. Auslegung

Bei Fragen betreffend die Auslegung der Bestimmung dieser Dienstanweisung ist von den Mitarbeitern – insbesondere bei Fragen betreffend die Handhabung von personenbezogenen Daten - der zuständige Jurist der ITSV vor Ergreifung der jeweiligen Maßnahme zu befassen.



Verwaltungsstrafbestimmungen

§ 17. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu € 5.000,-- zu ahnden ist, wer beim elektronischen Gesundheitsdatenaustausch nach dem 31.12.2009

1. es entgegen der Bestimmungen der §§ 3 bis 5 unterlässt, die Nachweise der Identität und der Rolle zu erbringen oder diese Nachweise zu prüfen oder

2. entgegen der Bestimmungen des § 6 die Verschlüsselung von Gesundheitsdaten unterlässt oder hiezu Methoden und Verfahren verwendet, die den qualitativen Anforderungen gemäß § 7 Abs. 5 nicht entsprechen oder

3. entgegen der Bestimmungen des § 7 keine elektronische Signatur verwendet oder eine elektronische Signatur verwendet, die den qualitativen Anforderungen nicht entspricht oder Gesundheitsdaten trotz fehlgeschlagener Signaturprüfung weitergibt oder verwendet.

(2) Eine Verwaltungsübertretung gemäß Abs. 1 ist nicht strafbar, wenn die Tat zur Abwendung einer gegenwärtigen oder unmittelbar drohenden Gefahr für das Leben einer/eines Dritten oder zur Abwendung einer gegenwärtigen oder unmittelbar drohenden Gefahr einer erheblichen Beeinträchtigung der physischen oder psychischen Integrität einer/eines Dritten begangen wurde.

(3) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu € 50.000,-- zu ahnden ist, wer entgegen der Bestimmung des § 9 Abs. 5 Daten oder Teile dieser Daten für andere Zwecke verwendet.

(4) Zuständig für Entscheidungen nach Abs. 1 bis 3 ist jene Behörde, in deren Sprengel die Verwaltungsübertretung begangen wurde.

Ausnahmen von der Meldepflicht:

Die Forderung nach höchstmöglicher **Publizität von Datenverarbeitungen** wurde in dem von der Richtlinie erforderlichen Ausmaß erweitert. Der Einführung neuer Informationspflichten (**Ausweitung der Registrierungspflicht auf manuelle Dateien – ABER: ab 1.1.2010: Registrierungspflicht manueller Dateien nur noch bei Vorliegen sensibler oder strafrechtlich relevanter Daten oder Zweck der Auskunftserteilung über Kreditwürdigkeit oder Durchführung in Form eines Informationsverbundsystems**) steht eine **Verminderung des Registrierungsaufwandes** gegenüber, die dadurch bewirkt wird, dass im Vergleich zur derzeitigen Gesetzeslage mehrere Registrierungsverpflichtungen wegfallen werden. So ist im derzeit aktuellen Gesetzestext (§ 17 Abs. 2 u. Abs. 3) vorgesehen:

Nicht meldepflichtig sind Datenanwendungen, die

1. **ausschließlich** veröffentlichte Daten enthalten (Diese Ausnahme ist nicht anwendbar, wenn neben veröffentlichten Daten auch andere personenbezogene Daten in einer Datenanwendung verarbeitet werden, insbesondere Bewertungen, Analysen, Verknüpfungen, etc. von veröffentlichten Daten. Diese Ausnahme ist angesichts ihrer Grundrechtsrelevanz restriktiv zu interpretieren) oder

2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses (vgl. Art. 21 Abs. 3, 2. Unterabsatz, RL)oder

3. nur indirekt personenbezogene Daten enthalten oder

(4. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§ 45) (vgl. Art. 3 Abs. 2, 2. Anstrich, RL) oder)

(5. für publizistische Tätigkeit gemäß § 48 vorgenommen werden (vgl. Art. 9 RL) oder)

6. Standardanwendungen darstellen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der zu verwendenden Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen. (vgl. Art. 18 Abs. 2, 1. Anstrich RL)

Weiters sind Datenanwendungen für Zwecke (betreffen sämtlich Regelungsbereiche außerhalb des Geltungsbereiches der Richtlinie (vgl. Art. 3 Abs. 2, 1. Anstrich RL))

1. des **Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich** oder

2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder

3. der Sicherstellung der Interessen der umfassenden Landesverteidigung oder

4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder

5. der **Vorbeugung, Verhinderung oder Verfolgung von Straftaten**

von der Meldepflicht ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist (Im Gegensatz zur bisherigen Regelung in §4 Abs. 3 DSG sind nicht mehr alle Datenanwendungen der in Z1-5 genannten Bereiche von der Meldepflicht ausgenommen, sondern nur mehr jene, bei welchen die Nichtmeldung **aufgrund der konkreten Zweckbestimmung** der einzelnen Datenanwendung notwendig ist).

§ 17 DSG - ab 1.1.2010:

(1) Jeder Auftraggeber hat, soweit in den Abs. 2 und 3 nicht anderes bestimmt ist, vor Aufnahme einer Datenanwendung eine Meldung an die Datenschutzkommission mit dem in § 19 festgelegten Inhalt zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Diese Meldepflicht gilt auch für

Umstände, die nachträglich die Unrichtigkeit und Unvollständigkeit einer Meldung bewirken (Änderungsmeldung). Für manuelle Dateien besteht eine Meldepflicht nur, soweit die Inhalte zumindest einen der Tatbestände des § 18 Abs. 2 Z 1 bis 4 erfüllen.

(1a) Die Meldung ist in elektronischer Form im Wege der vom Bundeskanzler bereit zu stellenden Internetanwendung einzubringen. Die Identifizierung und Authentifizierung kann insbesondere durch die Bürgerkarte (§ 2 Z 10 des E-Government-Gesetzes, BGBl. I Nr. 10/2004) erfolgen. Nähere Bestimmungen über die Identifizierung und Authentifizierung sind in die gemäß § 16 Abs. 3 zu erlassende Verordnung aufzunehmen. Eine Meldung in nicht-elektronischer Form ist für manuelle

Dateien sowie bei einem längeren technischen Ausfall der Internetanwendung zulässig.

(2) Nicht meldepflichtig sind Datenanwendungen, die

1. ausschließlich veröffentlichte Daten enthalten oder
2. die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind, sei es auch nur bei Nachweis eines berechtigten Interesses oder
3. nur indirekt personenbezogene Daten enthalten oder
4. von natürlichen Personen ausschließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (§ 45) oder
5. für publizistische Tätigkeit gemäß § 48 vorgenommen werden oder
6. einer Standardanwendung entsprechen: Der Bundeskanzler kann durch Verordnung Typen von Datenanwendungen und Übermittlungen aus diesen zu Standardanwendungen erklären, wenn sie von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszwecks und der verarbeiteten Datenarten die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist. In der Verordnung sind für jede Standardanwendung die zulässigen Datenarten, die Betroffenen- und Empfängerkreise und die Höchstdauer der zulässigen Datenaufbewahrung festzulegen.

(3) Weiters sind Datenanwendungen für Zwecke

1. des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich oder
2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder
3. der Sicherstellung der Interessen der umfassenden Landesverteidigung oder
4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder
5. der Vorbeugung, Verhinderung oder Verfolgung von Straftaten

von der Meldepflicht ausgenommen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist.

(4) Weiters sind Datenanwendungen von der Meldepflicht ausgenommen, für die der Zweck, die betroffenen Personengruppen, Datenarten, Übermittlungen und Übermittlungsempfänger in einem Gesetz oder in einer Verordnung abschließend geregelt sind.

Erläuterungen zu § 17 Abs. 1:

Mit der Einführung des Terminus „Änderungsmeldung“ soll die Verpflichtung, den Stand des Datenverarbeitungsregisters durch Meldung jeder relevanten Änderung stets aktuell zu halten, verdeutlicht werden. Der dritte Satz übernimmt den Inhalt des bisherigen § 58 zweiter Satz.

Erläuterungen zu § 17 Abs. 1a:

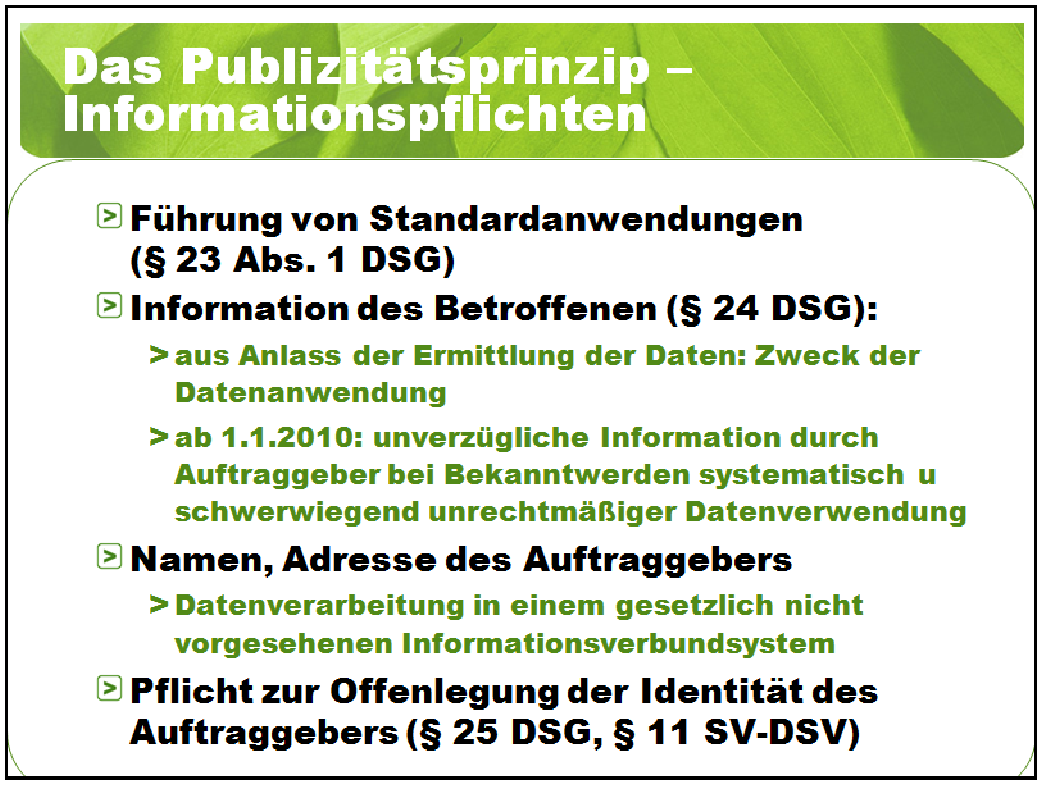
Das Datenverarbeitungsregister soll künftig in Form einer Datenbank geführt und Meldungen primär in automationsunterstützter Form über eine Internetanwendung (also online) erstattet werden, damit die Verwaltungsabläufe vereinfacht und beschleunigt werden können. Die Identifizierung und Authentifizierung der Meldepflichtigen kann insbesondere auch durch die Bürgerkarte erfolgen.

Ausnahmen von der elektronischen Meldung sind für manuelle Dateien und für Fälle eines längeren technischen Ausfalls der Internetanwendung vorgesehen. Eine nähere Ausgestaltung hat in der Verordnung nach § 16 Abs. 3 zu erfolgen.

Erläuterungen zu § 17 Abs. 4:

Die gegenständliche Ausnahme von der Meldepflicht soll zu einer weiteren Entlastung des bei der Datenschutzkommission eingerichteten Datenverarbeitungsregisters dienen. Die Transparenz ist für den Rechtsunterworfenen dadurch gegeben, dass der Zweck der Datenverwendung, die betroffenen Personengruppen, Datenarten, Übermittlungen und Übermittlungsempfänger in einem Gesetz oder einer

Verordnung abschließend geregelt sind. Damit bedarf es auch keiner Duplizierung solcher abschließend geregelten Fälle in der Standard- und Musterverordnung.



§ 24 DSG - ab 1.1.2010:

(2a) Wird dem Auftraggeber bekannt, dass Daten aus einer seiner Datenanwendungen systematisch und schwerwiegend unrechtmäßig verwendet wurden, hat er darüber unverzüglich die Betroffenen zu informieren.

Erläuterungen zu § 24 Abs. 2a:

Hier wird eine besondere Informationsverpflichtung jener Auftraggeber geschaffen, die Kenntnis von einer systematischen und schwerwiegenden unrechtmäßigen Verwendung (Datenmissbrauch) ihrer Datenbestände erlangen. Dies soll vor allem der Vermeidung von Vermögensschäden der Betroffenen dienen.

Die Informationspflicht des Auftraggebers macht dem Betroffenen bewusst, dass seine Geheimhaltungsinteressen berührt sind. In den Artikeln 10 und 11 der Richtlinie wird die zwingende Information des Betroffenen - falls ihn betreffende personenbezogener Daten erhoben werden - normiert, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen (§ 24 Abs. 1 DSG 2000). Diese Informationspflicht kann folglich nicht so verstanden werden, dass sich daraus ein Zwang zur Verdoppelung der Meldepflicht (an das Register) in Form einer zusätzlichen Pflicht zur "Meldung an den Betroffenen" ergibt. Diesen Rechten wird durch die §§ 24 bis 26 DSG 2000 entsprochen. Dies ist eine der wesentlichsten Neuerungen der Richtlinie gegenüber der bisherigen österreichischen Rechtslage. Sie soll es dem Betroffenen zusätzlich erleichtern, seine Rechte zu wahren. **Sie bezieht sich allerdings nur auf meldepflichtigen Fälle**. Gem. § 24 Abs. 4 besteht keine Informationspflicht bei jenen Datenanwendungen, die gemäß § 17 Abs. 2 u. 3 nicht meldepflichtig sind. Damit sind Anwendungen der Sicherheitsbehörden im großen Maße von der Informationspflicht gem. § 24 DSG 2000 ausgenommen.

- (Für Verarbeitungen zu persönlichen und familiären Zwecken gilt die Richtlinie nicht und daher auch nicht die Informationspflicht;)

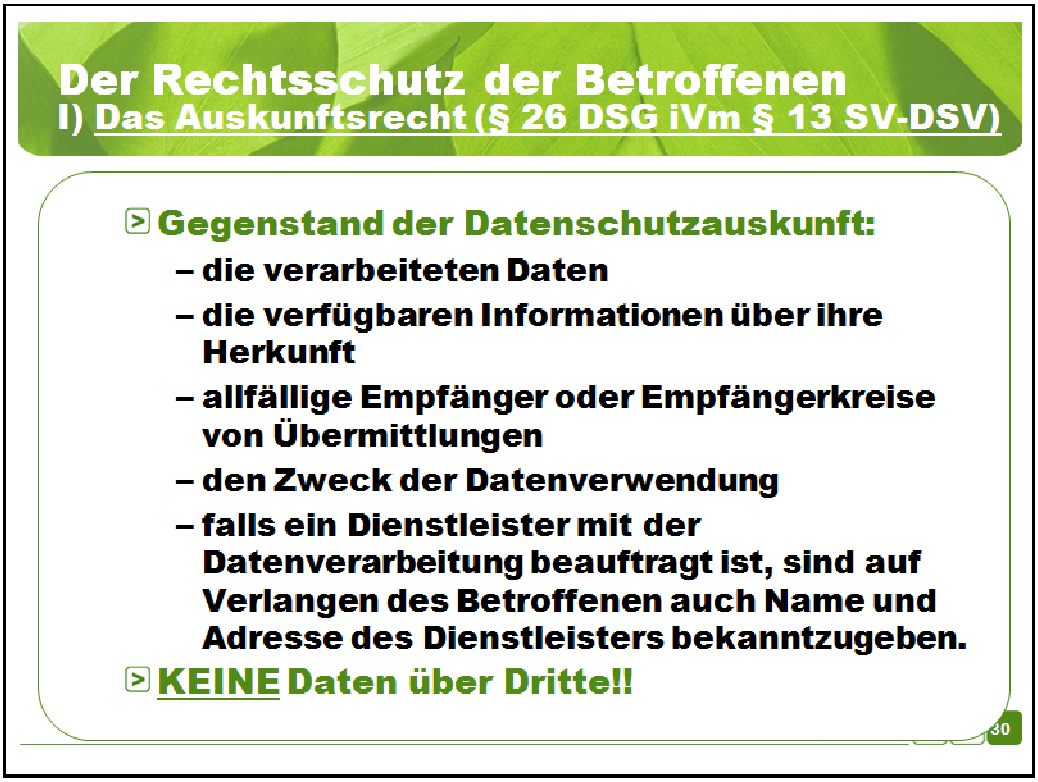
- die Führung von durch Gesetz eingerichteten öffentlichen Registern muss als bekannt vorausgesetzt werden (- "die Information liegt vor" -);

- die Durchführung von Standardverarbeitungen geschieht jeweils in einem Kontext, der für den Betroffenen klar erkennbar ist und umfasst die aus einer - im BGBl. veröffentlichten - Verordnung ersichtlichen Daten, so dass auch in diesem Fall davon auszugehen ist, dass "die Information dem Betroffenen vorliegt";(vgl. auch § 54 DSG 2000)

- Musteranwendungen dagegen sind Meldepflichtig, unterliegen daher auch der Informationspflicht.

- was die bloße Abfrage aus öffentlichen Datensammlungen betrifft, ist aus der "Öffentlichkeit" des Zugangs zu diesen Daten abzuleiten, dass der Betroffene mit der Kenntnisnahme dieser Daten durch jedermann rechnen muss, so dass eine besondere Informationspflicht unverhältnismäßig wäre.

Der Auftraggeber hat seine Identität auch in jenen Fällen, in welchen keine Registernummer geführt wird, offenzulegen. Ebenso besteht einen Offenlegungspflicht, falls Daten aus einer Datenanwendung für Zwecke einer vom Auftraggeber verschiedenen Person verwendet werden. Dann ist bei Mitteilungen an den Betroffenen neben der Identität der Person, für deren Zwecke die Daten verwendet wer-den, auch die Identität des Auftraggebers beizufügen (§ 25 DSG 2000).



Auskunftsrecht:

§ 26. (1) Der Auftraggeber hat dem Betroffenen Auskunft über die zu seiner Person verarbeiteten Daten zu geben, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich **gestellt** werden. **Die Auskunft hat** die verarbeiteten Daten, die verfügbaren Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form **anzuführen**. Auf Verlangen des Betroffenen sind auch Namen und Adresse von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Mit Zustimmung des Betroffenen kann anstelle der schriftlichen Auskunft auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(2) **Die Auskunft ist nicht zu erteilen, soweit** dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist oder soweit überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten, insbesondere auch überwiegende öffentliche Interessen, der Auskunftserteilung entgegenstehen. Überwiegende öffentliche Interessen können sich hiebei aus der Notwendigkeit

1. des **Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich** oder

2. der Sicherung der Einsatzbereitschaft des Bundesheeres oder

3. der Sicherung der Interessen der umfassenden Landesverteidigung oder

4. des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union oder

5. der **Vorbeugung, Verhinderung oder Verfolgung von Straftaten**

ergeben. Die Zulässigkeit der Auskunftsverweigerung aus den Gründen der Z 1 bis 5 unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission gemäß § 31 Abs. 4.

(3) Der Betroffene hat am Auskunftsverfahren über Befragung in dem ihm zumutbaren Ausmaß **mitzuwirken**, um ungerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.

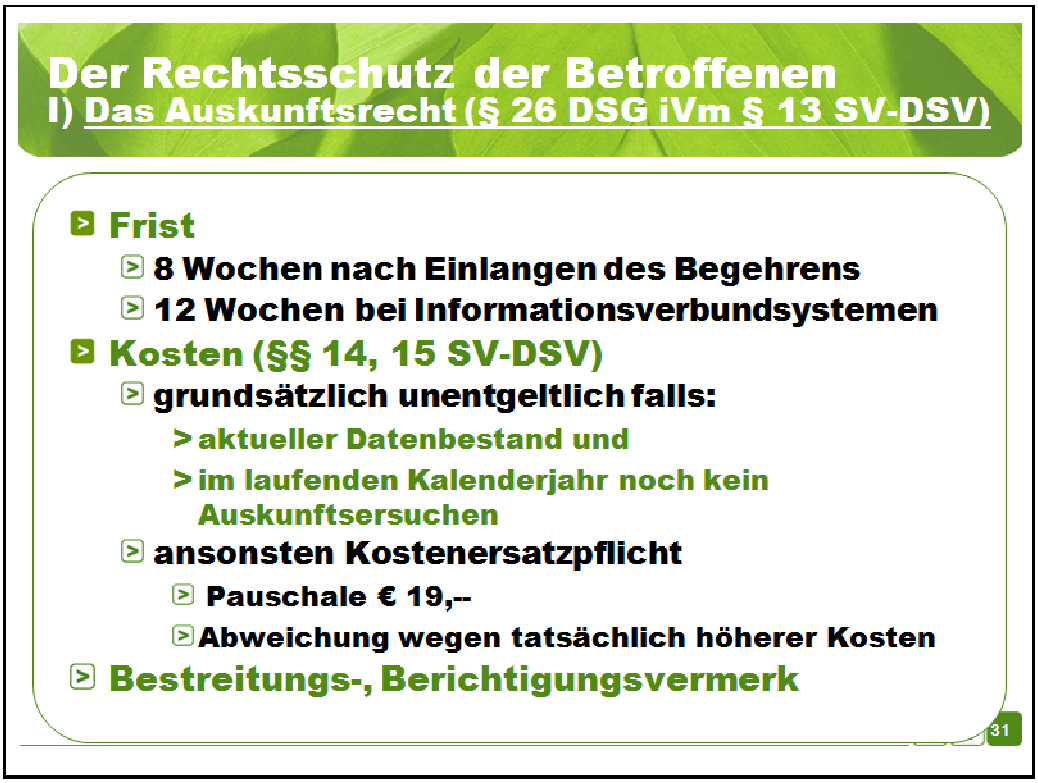
§ 26 DSG – ab 1.1.2010

(1) Ein Auftraggeber hat jeder Person oder Personengemeinschaft, die dies schriftlich verlangt und ihre Identität in geeigneter Form nachweist, Auskunft über die zu dieser Person oder Personengemeinschaft verarbeiteten Daten zu geben. Mit Zustimmung des Auftraggebers kann das Auskunftsbegehren auch mündlich gestellt werden. Die Auskunft hat die verarbeiteten Daten, die verfügbare Informationen über ihre Herkunft, allfällige Empfänger oder Empfängerkreise von Übermittlungen, den

Zweck der Datenverwendung sowie die Rechtsgrundlagen hiefür in allgemein verständlicher Form anzuführen. Auf Verlangen eines Betroffenen sind auch Namen und Adressen von Dienstleistern bekannt zu geben, falls sie mit der Verarbeitung seiner Daten beauftragt sind. Wenn zur Person des Auskunftswerbers keine Daten vorhanden sind, genügt die Bekanntgabe dieses Umstandes (Negativauskunft). Mit Zustimmung des Auskunftswerbers kann anstelle der schriftlichen Auskunft auch

eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme und der Abschrift oder Ablichtung gegeben werden.

(2) bis (7): *das Wort „Betroffener“ ist durch das Wort „Auskunftswerber“ zu ersetzen.*



(4) Innerhalb von **acht Wochen** nach Einlangen des Begehrens ist die Auskunft zu erteilen oder schriftlich zu begründen, warum sie nicht oder nicht vollständig erteilt wird. Von der Erteilung der Auskunft kann auch deshalb abgesehen werden, weil der Betroffene am Verfahren nicht gemäß Abs. 3 mitgewirkt oder weil er den Kostenersatz nicht geleistet hat.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Auskunftsverweigerung erfordert, folgendermaßen vorzugehen: Es ist in allen Fällen, in welchen keine Auskunft erteilt wird - also auch weil tatsächlich keine Daten verwendet werden -, anstelle einer inhaltlichen Begründung der Hinweis zu geben, dass keine der Auskunftspflicht unterliegenden Daten über den Betroffenen verwendet werden. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und wenn der Betroffene im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein pauschalierter **Kostenersatz von € 18,89** verlangt werden, von dem wegen tatsächlich erwachsender höherer Kosten abgewichen werden darf. Ein etwa geleisteter Kostenersatz ist ungeachtet allfälliger Schadenersatzansprüche zurückzuerstatten, wenn Daten rechtswidrig verwendet wurden oder wenn die Auskunft sonst zu einer Richtigstellung geführt hat.

(7) Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraums von vier Monaten und im Falle der Erhebung einer Beschwerde gemäß § 31 an die Datenschutzkommission bis zum rechtskräftigen Abschluss des Verfahrens **nicht vernichten**.

§ 26 Abs. 2 bis 10 DSG – ab 1.1.2010

(2) bis (7) *an die Stelle des „Betroffenen" tritt der „Auskunftswerber"*

(8) In dem Umfang, in dem eine Datenanwendung für eine Person oder Personengemeinschaft hinsichtlich der zu ihr verarbeiteten Daten von Gesetzes wegen einsehbar ist, hat diese das Recht auf Auskunft nach Maßgabe der das Einsichtsrecht vorsehenden Bestimmungen. Für das Verfahren der

Einsichtnahme (einschließlich deren Verweigerung) gelten die näheren Regelungen des Gesetzes, das das Einsichtsrecht vorsieht. In Abs. 1 genannte Bestandteile einer Auskunft, die vom Einsichtsrecht nicht umfasst sind, können dennoch nach diesem Bundesgesetz geltend gemacht werden."

(9) [keine Änderung]

(10) Ergibt sich eine Auftraggeberstellung auf Grund von Rechtsvorschriften, obwohl die Datenverarbeitung für Zwecke der Auftragserfüllung für einen Dritten erfolgt (§ 4 Z 4 letzter Satz), kann der Auskunftswerber sein Auskunftsbegehren zunächst auch an denjenigen richten, der die Herstellung des Werkes aufgetragen hat. Dieser hat dem Auskunftswerber, soweit ihm dies nicht ohnehin bekannt ist, binnen zwei Wochen unentgeltlich Namen und Adresse des tatsächlichen Auftraggebers mitzuteilen, damit der Auskunftswerber sein Auskunftsrecht gemäß Abs. 1 gegen diesen geltend machen kann. Das gilt auch für einen Dienstleister, wenn ein an ihn gerichtetes Auskunftsbegehren erkennen lässt, dass der Auskunftswerber ihn irrtümlich für den Auftraggeber der von ihm betriebenen Datenanwendung hält.

Stattdessen kann er auch innerhalb derselben Frist das Auskunftsbegehren an den Auftraggeber weiterleiten und den Auskunftswerber davon verständigen. Für Betreiber von Informationsverbundsystemen gilt jedoch ausschließlich § 50 Abs. 1.

Erläuterungen zu § 26 Abs. 1 bis 7:

Hier erfolgt lediglich eine der Rechtsprechung der Datenschutzkommission (zB Bescheid vom 2. Februar 2007, GZ K121.220/0001-DSK/2007) entsprechende Klarstellung, dass auch in dem Fall, dass ein Auftraggeber zu einer Person keine Daten verarbeitet, eine sog. Negativauskunft zu erteilen

ist. Dementsprechend wird in § 26 nunmehr im Allgemeinen von „Auskunftswerbern“ gesprochen, der Begriff des Betroffenen wird nur noch im strengen Sinn des § 4 Z 3 gebraucht, dh wenn zur Person des Auskunftswerbers tatsächlich Daten vorhanden sein müssen (zB Anspruch auf Bekanntgabe von Dienstleistern in Abs. 1).

Erläuterungen zu § 26 Abs. 8:

In dieser Bestimmung entfällt die sinnwidrige Einschränkung auf *öffentliche* Einsehbarkeit. Nunmehr soll es darauf ankommen, dass ein Auskunftswerber ein Recht auf Einsicht in die zu seiner Person verarbeiteten Daten hat („zumindest“ bedeutet dabei bloß, dass manchmal, zB im Grundbuch, auch darüber hinaus gehende Einsichtsrechte gewährt werden). Damit wird insbesondere auch die immer

häufiger werdende Führung elektronischer Verfahrensakten durch Behörden jedenfalls hinsichtlich der Verfahrensparteien umfasst (zB § 17 AVG, §§ 90 f BAO). Wenn durch das Einsichtsrecht nicht alle Bestandteile einer Auskunft nach § 26 Abs. 1 erlangt werden können, besteht darüber hinaus – soweit Informationen vorhanden sind – das Auskunftsrecht nach dem DSG 2000. Bei (teil-)öffentlichen

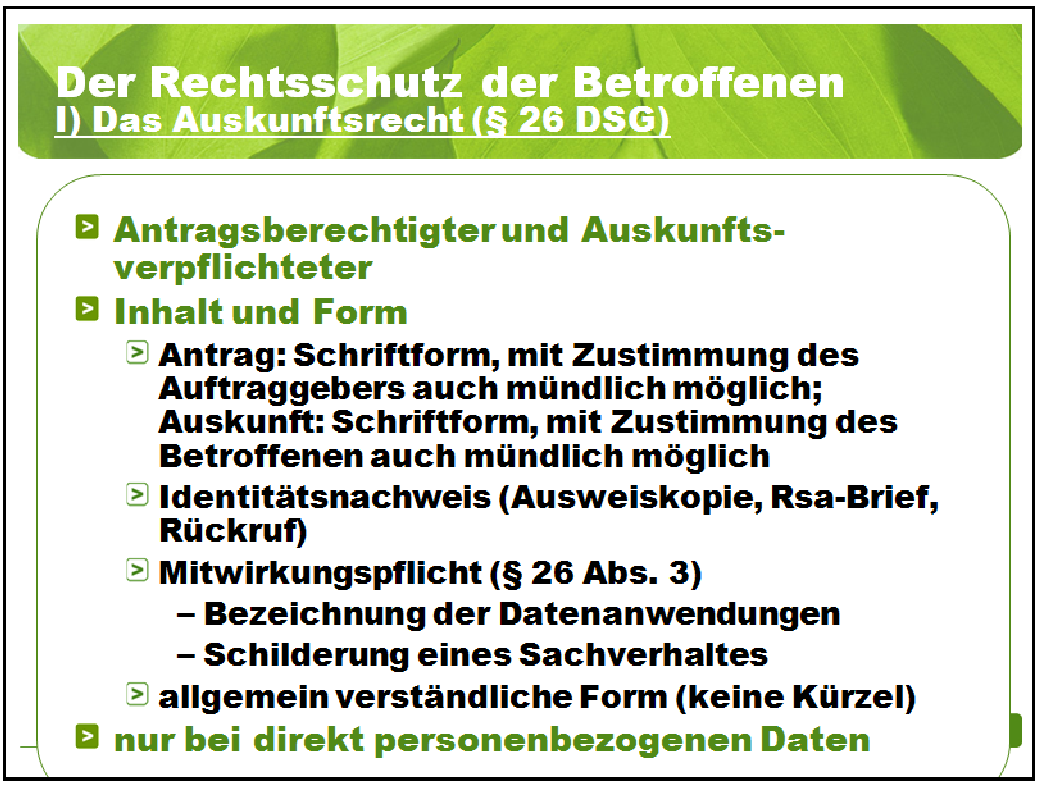
Registern ist freilich die Bekanntgabe von Empfängerkreisen – mehr wird im Hinblick auf fehlendes Rechtsschutzbedürfnis im Regelfall nicht erforderlich sein (vgl. das Erkenntnis des VwGH vom 19. Dezember 2006, Zl. 2005/06/0111) – schon durch den dem Auskunftswerber bekannten Umstand der (teil-)öffentlichen Einsehbarkeit verwirklicht. Weiterhin nicht möglich sein soll freilich die Umgehung von Beschränkungen von Einsichtsrechten durch das Auskunftsrecht: Die für die Beschränkung maßgeblichen Gründe werden idR auch nach § 26 Abs. 2 eine Ablehnung der Auskunft ermöglichen.

Im Hinblick auf die Richtlinie 95/46/EG ist diese Ausnahme unproblematisch, weil dort die näheren Modalitäten der Auskunftserteilung nicht geregelt sind. Eine geringe Kostenpflicht ist nicht ausgeschlossen. Die Anrufbarkeit der Datenschutzkommission nach § 30 ist trotz Ausschluss des förmlichen Beschwerderechts gegeben, sodass auch die Umsetzung von Art. 28 der Richtlinie gewahrt bleibt.

Erläuterungen zu § 26 Abs. 10:

Die ersten beiden Sätze wurden nur sprachlich geringfügig angepasst und bleiben inhaltlich unverändert. In den beiden neuen Sätzen erfolgt der Schluss einer Lücke im System des Auskunftsrechts: Wenn der Auskunftswerber ein Auskunftsbegehren irrtümlich an einen Dienstleister richtet, so hat ihm dieser nunmehr den Auftraggeber zu benennen. Stattdessen kann er das Auskunftsbegehren auch gleich an den

Auftraggeber weiterleiten, für den mit dem Einlangen die achtwöchige Frist nach Abs. 4 zu laufen beginnt. Für Betreiber von Informationsverbundsystemen gilt weiterhin § 50 Abs. 1.



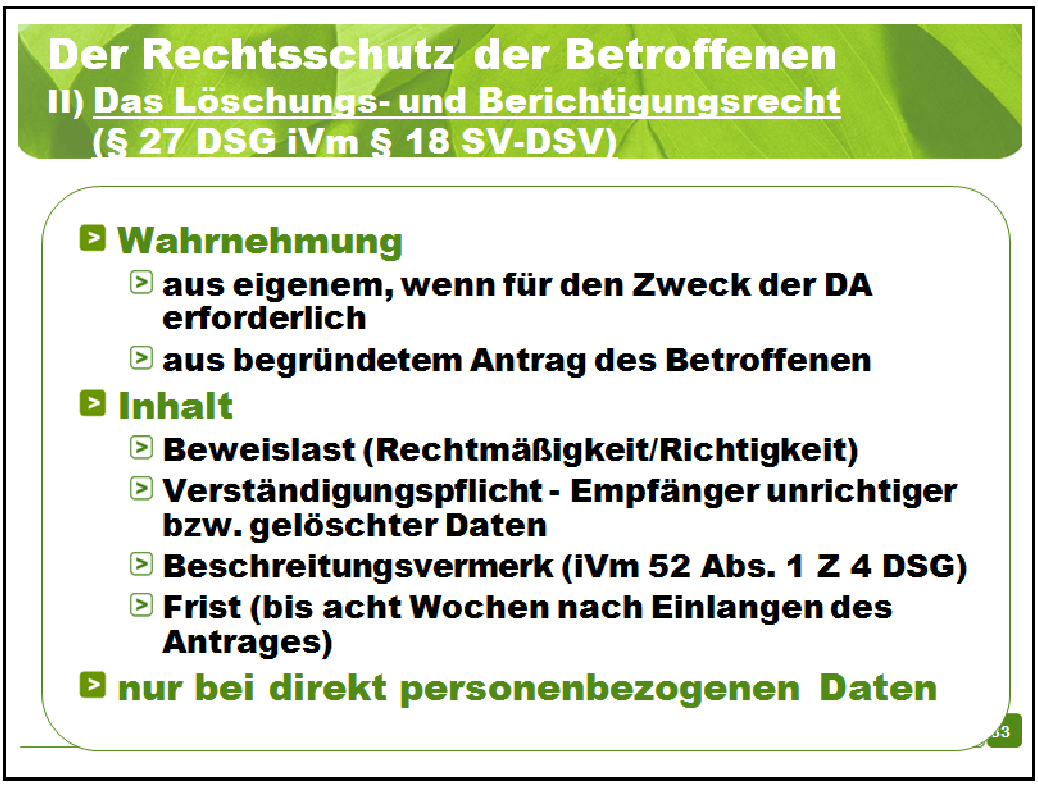
Das Auskunftsrecht, das als Angelpunkt für die Verwirklichung von Betroffeneninteressen anzusehen ist, ist in Hinkunft leichter durchsetzbar, da hiefür nunmehr immer die Datenschutzkommission (auch im privaten Bereich) zuständig ist (Kostenrisiko sinkt - § 53 DSG 2000), ansonsten bleibt jedoch die Trennung des Rechtsweges für die Durchsetzung der Interessen der Betroffenen aufrecht: Für die Entscheidung über Verletzungen des Datenschutzes durch einen Auftraggeber des öffentlichen Bereichs ist nach wie vor die Datenschutzkommission zuständig, zu Entscheidungen über Verletzungen des Datenschutzes im privaten Bereich sind die ordentlichen Gerichte berufen. § 5 Abs. 2 DSG 2000 nimmt die Teilung des Rechtsschutzinstrumentariums zwischen ordentlichen Gerichten und Datenschutzkommission in einer Weise vor, indem sie - grundsätzlich - nicht auf den Inhalt der Tätigkeit abstellt, sondern auf die rechtliche Organisationsform des Auftraggebers:

In § 26 Abs. 5 DSG 2000 wird nunmehr - dem ehemaligen § 62 SPG (Außerkrafttretensdatum: 30.9.2002) nachgebildet - das Auskunftsrecht in grundsätzlich der Geheimhaltung unterliegenden Bereichen (§ 26 Abs. 2 Z 1 - 5) geregelt (Kontrolle durch die DSK).

Die Pflicht zur Auskunftserteilung gem. § 26 DSG besteht **nicht bei Protokolldaten**, die nur durch sequentielle Suche aufgefunden werden können.

Antragsberechtigt ist jeder Betroffene Auskunftswerber (Personen oder Personengemeinschaften), der seine Identität ausreichend nachweist, hinsichtlich der über ihn verarbeiteten Daten. Sind über einen Auskunftswerber keine Daten vorhanden, so ist eine Negativauskunft zu erteilen.

Auskunftsverpflichtet ist der Auftraggeber bzw. der eigenverantwortliche Auftragnehmer. Neu ab 1.1.2010: Dienstleister hat, wenn Auskunftswerber ihn irrtümlich für den Auftraggeber hält, Auftraggeber zu benennen oder Auskunftsbegehren direkt an Auftraggeber weiterzuleiten (8-wöchige Frist beginnt mit einlangen neu zu laufen).



Hinsichtlich der **Pflicht zur Löschung bzw. Richtigstellung** von Daten (§ 27 DSG 2000) wird klargestellt, dass diese Pflichten den Auftraggeber auch dann trifft, wenn der Betroffene dies nicht eigens beantragt hat. Die Frist, in der der Auftraggeber dem Antrag zu entsprechen hat, wird von vier auf acht Wochen erhöht. § 27 Abs. 2 normiert, dass die Beweispflicht für die Richtigkeit der Daten grundsätzlich beim Auftraggeber liegt. § 27 Abs. 5 eröffnet der DSK eine Kontrollbefugnis, ob dem Richtigstellungs- bzw. Löschungsantrag des Betroffenen rechtmäßig durch den Auftraggeber nachgekommen wurde. § 27 Abs. 8 normiert, dass der Auftraggeber, falls dieser richtiggestellte oder gelöschte Daten vor Richtigstellung oder Löschung übermittelt hat, die Empfänger dieser Daten grundsätzlich hievon zu informieren hat.

Die Pflicht zur **Richtigstellung** ***aus eigenem*** ist insoweit eingeschränkt, als sie nur solche Daten betrifft, deren Richtigkeit für den Zweck der DA von Bedeutung ist. Die Unvollständigkeit von Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit die Unrichtigkeit der Gesamtinformation ergibt.

Sobald Daten für den Zweck der DA nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, dass ihre Archivierung rechtlich zulässig ist und dass der Zugang zu diesen Daten besonders geschützt ist.

Beweislastumkehr: Der Beweis der Richtigkeit der Daten obliegt dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen ermittelt wurden.

Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, soweit der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zulässt (z.B. Krankengeschichte, ?Vereinsregister?). Die erforderlichen Richtigstellungen sind diesfalls durch entsprechende zusätzliche Anmerkungen zu bewirken.

Recht auf Richtigstellung oder Löschung

§ 27. (1) Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen dieses Bundesgesetzes verarbeitete Daten richtigzustellen oder zu löschen, und zwar

1. aus eigenem, sobald ihm die Unrichtigkeit von Daten oder die Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder

2. auf begründeten Antrag des Betroffenen.

Der Pflicht zur Richtigstellung nach Z 1 unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist. Die Unvollständigkeit verwendeter Daten bewirkt nur dann einen Berichtigungsanspruch, wenn sich aus der Unvollständigkeit im Hinblick auf den Zweck der Datenanwendung die Unrichtigkeit der Gesamtinformation ergibt. Sobald Daten für den Zweck der Datenanwendung nicht mehr benötigt werden, gelten sie als unzulässig verarbeitete Daten und sind zu löschen, es sei denn, dass ihre Archivierung rechtlich zulässig ist und dass der Zugang zu diesen Daten besonders geschützt ist. Die Weiterverwendung von Daten für einen anderen Zweck ist nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist; die Zulässigkeit der Weiterverwendung für wissenschaftliche oder statistische Zwecke ergibt sich aus den §§ 46 und 47.

(2) Der Beweis der Richtigkeit der Daten obliegt - sofern gesetzlich nicht ausdrücklich anderes angeordnet ist - dem Auftraggeber, soweit die Daten nicht ausschließlich auf Grund von Angaben des Betroffenen ermittelt wurden.

(3) Eine Richtigstellung oder Löschung von Daten ist ausgeschlossen, soweit der Dokumentationszweck einer Datenanwendung nachträgliche Änderungen nicht zulässt. Die erforderlichen Richtigstellungen sind diesfalls durch entsprechende zusätzliche Anmerkungen zu bewirken.

(4) Innerhalb von acht Wochen nach Einlangen eines Antrags auf Richtigstellung oder Löschung ist dem Antrag zu entsprechen und dem Betroffenen davon Mitteilung zu machen oder schriftlich zu begründen, warum die verlangte Löschung oder Richtigstellung nicht vorgenommen wird.

(5) In jenen Bereichen der Vollziehung, die mit der Wahrnehmung der in § 26 Abs. 2 Z 1 bis 5 bezeichneten Aufgaben betraut sind, ist, soweit dies zum Schutz jener öffentlichen Interessen notwendig ist, die eine Geheimhaltung erfordern, mit einem Richtigstellungs- oder Löschungsantrag folgendermaßen zu verfahren: Die Richtigstellung oder Löschung ist vorzunehmen, wenn das Begehren des Betroffenen nach Auffassung des Auftraggebers berechtigt ist. Die gemäß Abs. 4 erforderliche Mitteilung an den Betroffenen hat in allen Fällen dahingehend zu lauten, dass die Überprüfung der Datenbestände des Auftraggebers im Hinblick auf das Richtigstellungs- oder Löschungsbegehren durchgeführt wurde. Die Zulässigkeit dieser Vorgangsweise unterliegt der Kontrolle durch die Datenschutzkommission nach § 30 Abs. 3 und dem besonderen Beschwerdeverfahren vor der Datenschutzkommission nach § 31 Abs. 4.

(6) Wenn die Löschung oder Richtigstellung von Daten auf ausschließlich automationsunterstützt lesbaren Datenträgern aus Gründen der Wirtschaftlichkeit nur zu bestimmten Zeitpunkten vorgenommen werden kann, sind bis dahin die zu löschenden Daten für den Zugriff zu sperren und die zu berichtigenden Daten mit einer berichtigenden Anmerkung zu versehen.

(7) Werden Daten verwendet, deren Richtigkeit der Betroffene bestreitet, und lässt sich weder ihre Richtigkeit noch ihre Unrichtigkeit feststellen, so ist auf Verlangen des Betroffenen ein Vermerk über die Bestreitung beizufügen. Der Bestreitungsvermerk darf nur mit Zustimmung des Betroffenen oder auf Grund einer Entscheidung des zuständigen Gerichtes oder der Datenschutzkommission gelöscht werden.

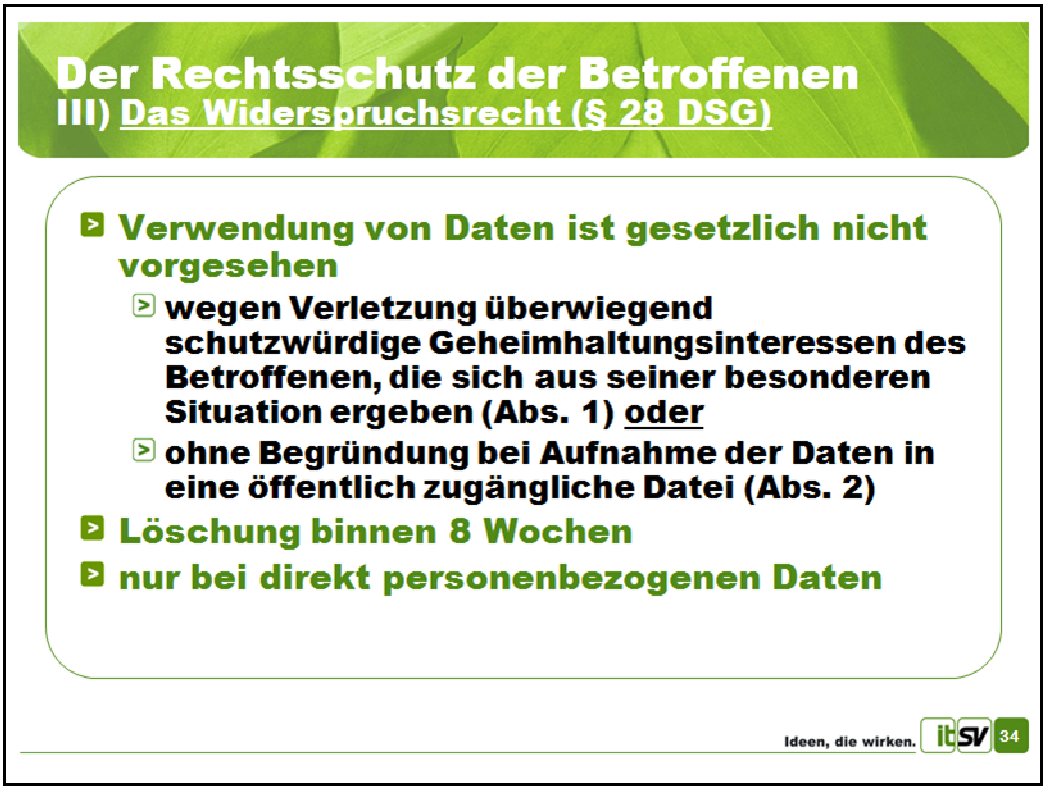
(8) Wurden im Sinne des Abs. 1 richtiggestellte oder gelöschte Daten vor der Richtigstellung oder Löschung übermittelt, so hat der Auftraggeber die Empfänger dieser Daten hievon in geeigneter Weise zu verständigen, sofern dies keinen unverhältnismäßigen Aufwand, insbesondere im Hinblick auf das Vorhandensein eines berechtigten Interesses an der Verständigung, bedeutet und die Empfänger noch feststellbar sind.

(9) Die Regelungen der Abs. 1 bis 8 gelten für das gemäß Strafregistergesetz 1968 geführte Strafregister sowie für öffentliche (ab 1.1.2010) Bücher und Register, die von Auftraggebern des öffentlichen Bereichs geführt werden, nur insoweit als für

1. die Verpflichtung zur Richtigstellung und Löschung von Amts wegen oder

2. das Verfahren der Durchsetzung und die Zuständigkeit zur Entscheidung über Berichtigungs- und Löschungsanträge von Betroffenen

durch Bundesgesetz nicht anderes bestimmt ist.



Das Widerspruchsrecht: § 28 DSG 2000 führt in Umsetzung des Art. 14 RL - sofern die Verwendung der Daten nicht gesetzlich vorgesehen ist - ein Widerspruchsrecht gegen deren Verwendung ein. Im Gegensatz zur Beschwerde (Klage) wegen unzulässiger Verarbeitung von Daten nach den §§ 31 oder 32 DSG 2000 hat das Widerspruchsrecht keinen Einfluss auf die rechtliche Zulässigkeit der Datenanwendung an sich. Sie bewirkt nur eine individuell auf den (erfolgreich) Widersprechenden begrenzte Löschungspflicht, bedeutet aber nicht, dass die gesamte Datenanwendung wegen Rechtswidrigkeit einzustellen wäre. Die erfolgreiche Ausübung des Widerspruchsrechts wird daher - zumindest grundsätzlich - auch keinen Schadenersatzanspruch begründen können.

Im Gegensatz zum Löschungsrecht, welches nur zur Anwendung kommt, falls Daten des Betroffenen unzulässigerweise verarbeitet wurden, gibt das Widerspruchsrecht dem Betroffenen - aufgrund seiner besonderen Situation - auch bei - rechtmäßig - verarbeiteten Daten die Möglichkeit, diese Löschen zu lassen.

Anwendungsfälle sind beispielsweise die Verwendung von Daten, welche gem. § 8 Abs. 1 Zif. 4 DSG aufgrund "überwiegend berechtigter Interessen des Auftraggebers oder eines Dritten" erfolgen. Die Datenanwendung ist zwar grundsätzlich zulässig, in bestimmten Einzelfällen überwiegen jedoch möglicherweise die Interessen des Betroffenen jenen des Auftraggebers oder des Dritten (Äquivalenzprinzip!).

Das Widerspruchsrecht nach Abs. 2 ist leichter auszuüben, da es nicht begründet werden muss.

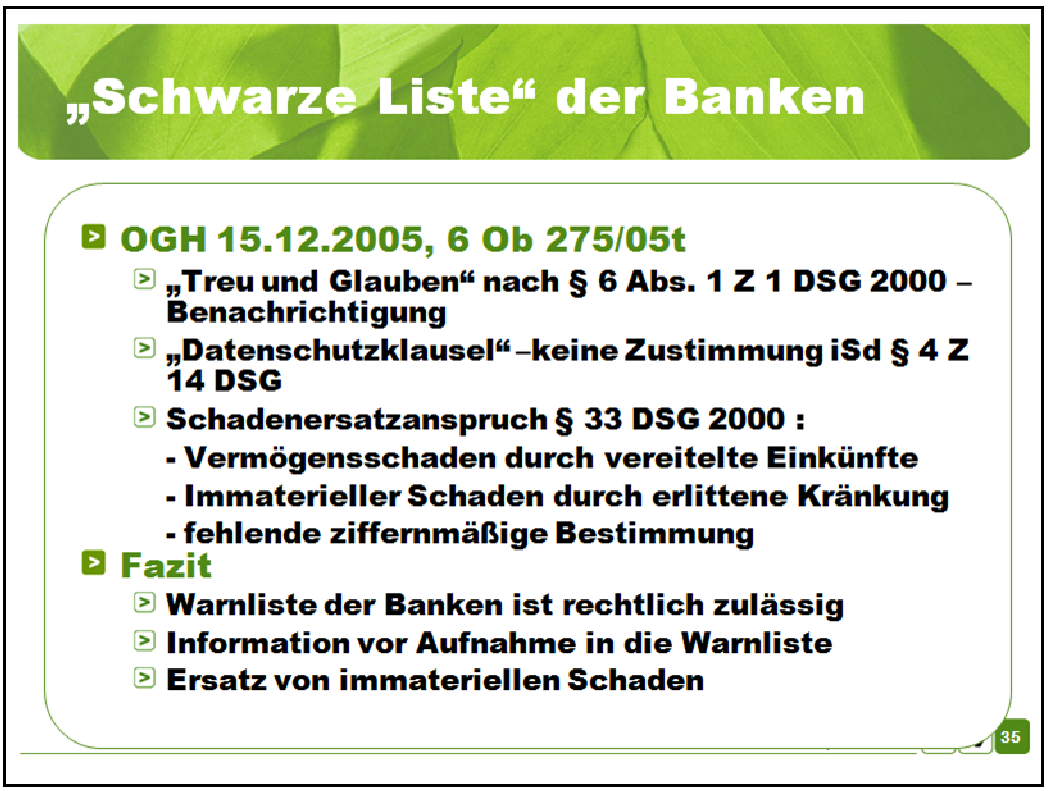
§ 28. (1) Sofern die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, die sich aus seiner besonderen Situation ergeben, beim Auftraggeber der Datenanwendung Widerspruch zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen acht Wochen aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen.

(2) Gegen eine nicht gesetzlich angeordnete Aufnahme in eine öffentlich zugängliche Datei kann der Betroffene jederzeit auch ohne Begründung seines Begehrens Widerspruch erheben. Die Daten sind binnen acht Wochen zu löschen.

(3) § 27 Abs. 4 bis 6 gelten auch in den Fällen der Abs. 1 und 2. (ab 1.1.2010)

Erläuterungen zu § 28 Abs. 3:

Hier wird lediglich klargestellt, dass die Bestimmungen über die Durchsetzung des Richtigstellungs- und Löschungsrechts auch für das als Sonderfall des Löschungsrechts anzusehende Widerspruchsrecht gelten.



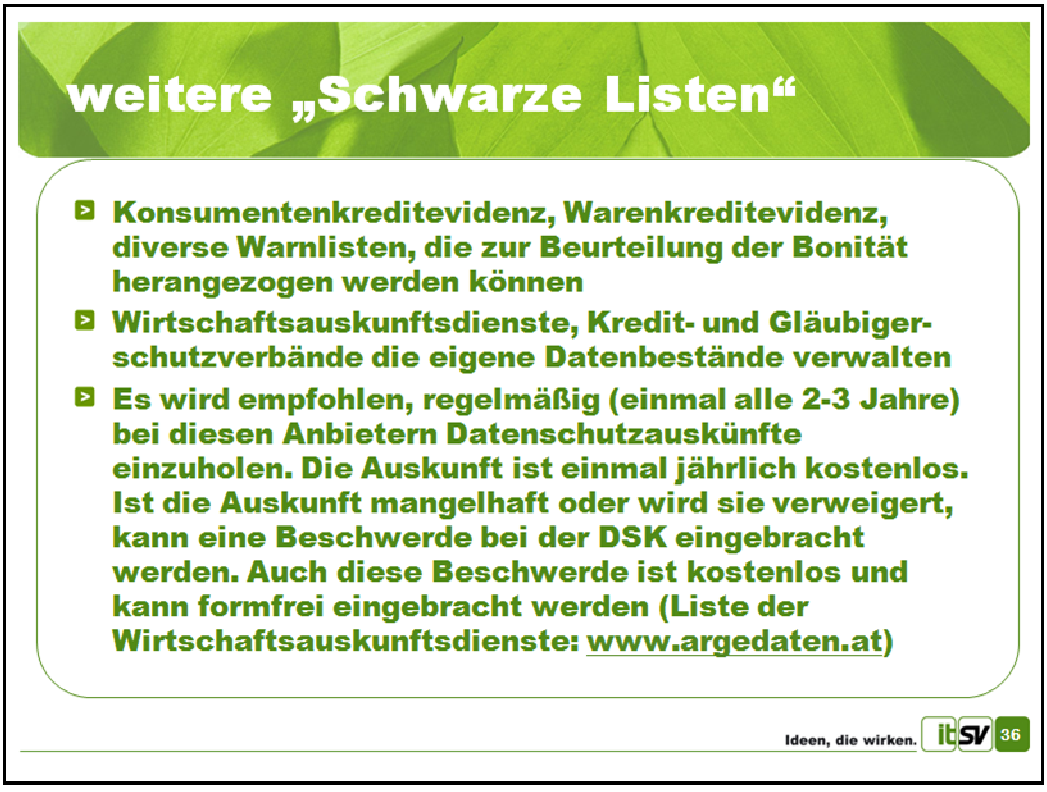
Wirtschaftsauskunftsdienste, Kredit- und Gläubigerschutzverbände, sonstige Dienste die eigene Datenbestände ("Schwarze Listen", Bonitätsinformationen, Inkasso) verwalten
Es wird empfohlen, regelmäßig (einmal alle 2-3 Jahre) bei diesen Anbietern (Wirtschaftsauskunftsdienste, Inkassodienst, ...) Datenschutzauskünfte einzuholen. Die Auskunft ist einmal jährlich kostenlos, ist die Auskunft mangelhaft oder wird sie verweigert, kann eine Beschwerde bei der Datenschutzkommission eingebracht werden. Auch diese Beschwerde ist kostenlos und kann formfrei eingebracht werden. Mit **VIP** wurden jene Unternehmen bezeichnet, die als Branchenführer anzusehen sind. Beachten Sie die Anmerkungen zu jedem Auskunftsdienst, manche haben sich auf bestimmte Bereiche, wie Unternehmen oder Privatkunden spezialisiert.
Alpenländischer Kreditorenverband für Kreditschutz und Betriebswirtschaft (AKV)
A-1040 Wien, Schleifmühlgasse 2/2
fon: +43.1.5861771.0 fax: +43.1.5870821 mail: office@akveuropa.at
VIP UID ATU 28661409 DVR 2109678 Wirtschaftskammer registrierter Verein ZVR 586673624
http://www.akv.at/
Schwerpunkt sind Unternehmen. Bevorrechteter Gläubigerschutzverbands gemäß § 11 Insolvenzrechtseinführungsgesetz **Creditreform Wirtschaftsauskunftei Kubicki KG**
A-1190 Wien, Muthgasse 36 - 40 (Bauteil 4)
fon: +43.1.21862200 fax: +43.1.21862204 mail: creditreform.service@wien.creditreform.at
VIP HG Wien FN 9948f UID ATU 11828806 Wirtschaftskammer http://www.creditreform.at/
Diese Einrichtung ist auch Betreiber des Informationsverbundsystems "Warnliste der österreichischen Versicherungsunternehmen" und für Auskünfte nach dem Datenschutzgesetz verantwortlich.

Bevorrechteter Gläubigerschutzverbands gemäß § 11 Insolvenzrechtseinführungsgesetz **Deltavista GmbH**
A-1150 Wien, Diefenbachgasse 35
fon: +43.1.8974244 fax: +43.1.8974244.31 mail: info.at@deltavista.com
VIP FG Wien FN 200570g UID ATU 50804704 DVR 1062107 Wirtschaftskammer
https://www.deltavista.at
Schwerpunkt sind Privatpersonen mit besonders umfangreichen Verbindungen zu anderen Inkassobüros und Wirtschaftsauskunftsdiensten. Hauptkundengruppe dürften Telekom-Unternehmen und Versandhäuser sein. **Dun & Bradstreet Information Services GmbH**
A-1110 Wien, Geiselbergstraße 17-19
fon: +43.1.588610 fax: +43.1.5863359 mail: office@dnbaustria.at
VIP HG Wien FN 148453p DVR 0869376 Wirtschaftskammer http://dbaustria.dnb.com/
Schwerpunkt sind Unternehmen **FirmenABC Marketing GmbH**
A-5301 Eugendorf, Pebering-Straße 1
fon: +43.6225.208100 fax: +43.6225.2081020 mail: office@firmenabc.at
http://www.firmenabc.at
Schwerpunkt sind Firmendaten - im Internet zumindest teilweise frei abrufbar **GBI-Genios Deutsche Wirtschaftsdatenbank GmbH**
D-81927 München, Freischützstraße 96
fon: 089.9928790 fax: 089.99287999 mail: info@genios.de
HRB München FN 54889 UID DE 129354131 www.genios.de
Deutscher Anbieter für Firmeninformationen, der auch Bonitätsdaten österreichischer Firmen verbreitet und angeblich mit Dun & Bradstreet und dem KSV von 1870 zusammen arbeitet. Ein Teil der Daten ist frei im Internet abrufbar. **infoscore austria gmbh**
A-1040 WIEN, Weyringergasse 1/5
fon: +43.1.5036490 fax: +43.1.5036490.968 mail: info@infoscore.at
HG Wien FN 148689k DVR 0865176, 0898422 Wirtschaftskammer http://www.bfs-finance.at/
Rechtsnachfolger von BFS risk & collection Austria GmbH. Nach eigenen Angaben nur Inkassobüro, die keine Daten im Sinne eines Auskunftsdienstes weitergeben. Laut WKO (Stand 23.4.2009) Gewerbeberechtigung für "Inkassodienste" und "Immobilien- und Vermögenstreuhänder". **Intrum Creditcontrol Auskunftsgesellschaft m.b.H.**
A-5020 Salzburg, Karolingerstraße 36
fon: +43.662.8350770 fax: +43.662.835080
VIP http://firmen.wko.at/Web/DetailsKontakt.aspx?FirmaID=d9abdfbb... **Intrum Justitia Inkasso Gesellschaft m.b.H.**
A-5071 Wals-Siezenheim, Franz-Brötzner-Straße 11
fon: +43.662.835077 fax: +43.662.835080 mail: info@at.intrum.com
VIP DVR 0769444 http://www.intrum.at **Kreditinform - Josef Hirnschall**
A-1090 WIEN, Rossauer Lände 25/8
fon: +43.1.3197822 fax: +43.1.3104295
DVR 0478784 http://www.scan.verbraucherrecht.at/2008/OGH_1.10.2008_6_Ob_1...
Schwerpunkt sind Privatpersonen und deren Exekutionsdaten **Kreditschutzverband von 1870 (KSV 1870)**
A-1120 Wien, Wagenseilgasse 7
fon: +43.050.1870 fax: +43.50.1870.991000 mail: ksv@ksv.at
VIP UID ATU16357706 DVR 0431591 http://www.ksv.at
Auf Grund der undurchsichtigen Firmenkonstruktion des KSV 1870 empfehlen wir Löschungsbegehren auch an die "KSV1870 Information Gmbh" (Adresse ident) zu richten. Der KSV 1870 ist auch Betreiber der Informationsverbundsysteme "KKE (Konsumentenkreditevidenz)" und "Warnliste der Banken", beide werden im Auftrag der österreichischen kreditgebenden Einrichtungen (inkl. Banken und Leasingfirmen) betrieben. Der KSV 1870 ist für Auskünfte nach dem Datenschutzgesetz aus diesen Beständen verantwortlich. Löschungen aus KKE und Warnliste sind direkt bei den entsprechenden Einrichtungen vorzubringen, die die Einträge zu verantworten haben.
Bevorrechteter Gläubigerschutzverbands gemäß § 11 Insolvenzrechtseinführungsgesetz **SLC Europe s.r.o.**
SK-81106 Bratis Bratislava, Stefanikova 7
fon: +421.2.33006510
www.slc-europe.com
Slowakische "Community" über österreichische Firmen die sich in Konkurs befinden. Zur Zeit offline

(29.04.09). **Wiener Zeitung Digitale Publikationen GmbH**
A-1040 Wien, Wiedner Gürtel 10
fon: +43.1.20699.0 fax: +43.1.20699.461 mail: digipub@wienerzeitung.at
HG Wien FN 196865h UID ATU49871704 http://www.digipub.at
Wirtschaftsauskünfte beschränken sich auf Firmen/Unternehmer, Schwerpunkt sind Angaben aus dem Firmenbuch

Die angezeigten Informationen und Artikel werden im Rahmen des ARGE DATEN Informationsdienstes kostenlos zur Verfügung gestellt. Alle Angaben sind sorgfältig recherchiert, es wird jedoch für die Richtigkeit keine Gewähr übernommen. Alle Angaben, Aussagen und Daten beziehen sich auf das Datum der Veröffentlichung des Artikels. Es wird ausdrücklich darauf hingewiesen, dass insbesondere Links, auf Websites gemachte Beobachtungen und zu einem Sachverhalt gemachte Aussagen zum Zeitpunkt der Anzeige eines Artikels nicht mehr stimmen müssen. Der Artikel wird ausschließlich aus historischem und/oder archivarischen Interesse angezeigt. Die Nutzung der Informationen ist nur zum persönlichen Gebrauch bestimmt. Dieser Informationsdienst kann professionelle fachliche Beratung nicht ersetzen. Diese wird von der ARGE DATEN im Rahmen ihres Beratungs- und Seminarservice angeboten und vermittelt. Verwendete Logos dienen ausschließlich zur Kennzeichnung der entsprechenden Einrichtung. Die verwendeten Bilder der Website stammen, soweit nicht anders vermerkt von der ARGE DATEN selbst, den in den Artikeln erwähnten Unternehmen, Pixelio, Aboutpixel oder Flickr.

LINK: http://www2.argedaten.at/php/cms_monitor.php?q=LIST-BONITAET

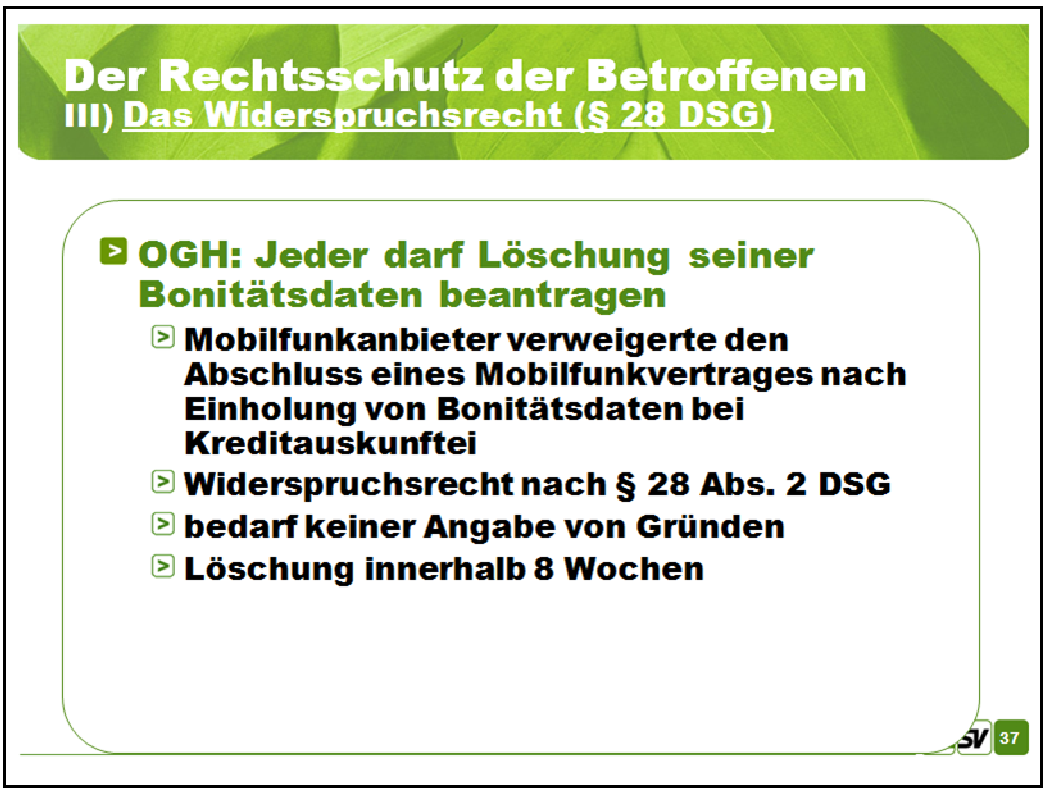


Wirtschaftsauskunftsdienste, Kredit- und Gläubigerschutzverbände, sonstige Dienste die eigene Datenbestände ("Schwarze Listen", Bonitätsinformationen, Inkasso) verwalten
Es wird empfohlen, regelmäßig (einmal alle 2-3 Jahre) bei diesen Anbietern (Wirtschaftsauskunftsdienste, Inkassodienst, ...) Datenschutzauskünfte einzuholen. Die Auskunft ist einmal jährlich kostenlos, ist die Auskunft mangelhaft oder wird sie verweigert, kann eine Beschwerde bei der Datenschutzkommission eingebracht werden. Auch diese Beschwerde ist kostenlos und kann formfrei eingebracht werden. Mit **VIP** wurden jene Unternehmen bezeichnet, die als Branchenführer anzusehen sind. Beachten Sie die Anmerkungen zu jedem Auskunftsdienst, manche haben sich auf bestimmte Bereiche, wie Unternehmen oder Privatkunden spezialisiert.
Alpenländischer Kreditorenverband für Kreditschutz und Betriebswirtschaft (AKV)

A-1040 Wien, Schleifmühlgasse 2/2
fon: +43.1.5861771.0 fax: +43.1.5870821 mail: office@akveuropa.at
VIP UID ATU 28661409 DVR 2109678 Wirtschaftskammer registrierter Verein ZVR 586673624
http://www.akv.at/
Schwerpunkt sind Unternehmen. Bevorrechteter Gläubigerschutzverbands gemäß § 11 Insolvenzrechtseinführungsgesetz **Creditreform Wirtschaftsauskunftei Kubicki KG**
A-1190 Wien, Muthgasse 36 - 40 (Bauteil 4)
fon: +43.1.21862200 fax: +43.1.21862204 mail: creditreform.service@wien.creditreform.at
VIP HG Wien FN 9948f UID ATU 11828806 Wirtschaftskammer http://www.creditreform.at/
Diese Einrichtung ist auch Betreiber des Informationsverbundsystems "Warnliste der österreichischen Versicherungsunternehmen" und für Auskünfte nach dem Datenschutzgesetz verantwortlich. Bevorrechteter Gläubigerschutzverbands gemäß § 11 Insolvenzrechtseinführungsgesetz **Deltavista GmbH**
A-1150 Wien, Diefenbachgasse 35
fon: +43.1.8974244 fax: +43.1.8974244.31 mail: info.at@deltavista.com
VIP FG Wien FN 200570g UID ATU 50804704 DVR 1062107 Wirtschaftskammer
https://www.deltavista.at
Schwerpunkt sind Privatpersonen mit besonders umfangreichen Verbindungen zu anderen Inkassobüros und Wirtschaftsauskunftsdiensten. Hauptkundengruppe dürften Telekom-Unternehmen und Versandhäuser sein. **Dun & Bradstreet Information Services GmbH**
A-1110 Wien, Geiselbergstraße 17-19
fon: +43.1.588610 fax: +43.1.5863359 mail: office@dnbaustria.at
VIP HG Wien FN 148453p DVR 0869376 Wirtschaftskammer http://dbaustria.dnb.com/
Schwerpunkt sind Unternehmen **FirmenABC Marketing GmbH**
A-5301 Eugendorf, Pebering-Straße 1
fon: +43.6225.208100 fax: +43.6225.2081020 mail: office@firmenabc.at
http://www.firmenabc.at
Schwerpunkt sind Firmendaten - im Internet zumindest teilweise frei abrufbar **GBI-Genios Deutsche Wirtschaftsdatenbank GmbH**
D-81927 München, Freischützstraße 96
fon: 089.9928790 fax: 089.99287999 mail: info@genios.de
HRB München FN 54889 UID DE 129354131 www.genios.de
Deutscher Anbieter für Firmeninformationen, der auch Bonitätsdaten österreichischer Firmen verbreitet und angeblich mit Dun & Bradstreet und dem KSV von 1870 zusammen arbeitet. Ein Teil der Daten ist frei im Internet abrufbar. **infoscore austria gmbh**
A-1040 WIEN, Weyringergasse 1/5
fon: +43.1.5036490 fax: +43.1.5036490.968 mail: info@infoscore.at
HG Wien FN 148689k DVR 0865176, 0898422 Wirtschaftskammer http://www.bfs-finance.at/
Rechtsnachfolger von BFS risk & collection Austria GmbH. Nach eigenen Angaben nur Inkassobüro, die keine Daten im Sinne eines Auskunftsdienstes weitergeben. Laut WKO (Stand 23.4.2009) Gewerbeberechtigung für "Inkassodienste" und "Immobilien- und Vermögenstreuhänder". **Intrum Creditcontrol Auskunftsgesellschaft m.b.H.**
A-5020 Salzburg, Karolingerstraße 36
fon: +43.662.8350770 fax: +43.662.835080
VIP http://firmen.wko.at/Web/DetailsKontakt.aspx?FirmaID=d9abdfbb... **Intrum Justitia Inkasso Gesellschaft m.b.H.**
A-5071 Wals-Siezenheim, Franz-Brötzner-Straße 11
fon: +43.662.835077 fax: +43.662.835080 mail: info@at.intrum.com
VIP DVR 0769444 http://www.intrum.at **Kreditinform - Josef Hirnschall**
A-1090 WIEN, Rossauer Lände 25/8
fon: +43.1.3197822 fax: +43.1.3104295
DVR 0478784 http://www.scan.verbraucherrecht.at/2008/OGH_1.10.2008_6_Ob_1...
Schwerpunkt sind Privatpersonen und deren Exekutionsdaten **Kreditschutzverband von 1870 (KSV 1870)**
A-1120 Wien, Wagenseilgasse 7
fon: +43.050.1870 fax: +43.50.1870.991000 mail: ksv@ksv.at
VIP UID ATU16357706 DVR 0431591 http://www.ksv.at
Auf Grund der undurchsichtigen Firmenkonstruktion des KSV 1870 empfehlen wir Löschungsbegehren auch an die "KSV1870 Information Gmbh" (Adresse ident) zu richten. Der KSV

1870 ist auch Betreiber der Informationsverbundsysteme "KKE (Konsumentenkreditevidenz)" und "Warnliste der Banken", beide werden im Auftrag der österreichischen kreditgebenden Einrichtungen (inkl. Banken und Leasingfirmen) betrieben. Der KSV 1870 ist für Auskünfte nach dem Datenschutzgesetz aus diesen Beständen verantwortlich. Löschungen aus KKE und Warnliste sind direkt bei den entsprechenden Einrichtungen vorzubringen, die die Einträge zu verantworten haben. Bevorrechteter Gläubigerschutzverbands gemäß § 11 Insolvenzrechtseinführungsgesetz **SLC Europe s.r.o.**
SK-81106 Bratis Bratislava, Stefanikova 7
fon: +421.2.33006510
www.slc-europe.com
Slowakische "Community" über österreichische Firmen die sich in Konkurs befinden. Zur Zeit offline (29.04.09). **Wiener Zeitung Digitale Publikationen GmbH**
A-1040 Wien, Wiedner Gürtel 10
fon: +43.1.20699.0 fax: +43.1.20699.461 mail: digipub@wienerzeitung.at
HG Wien FN 196865h UID ATU49871704 http://www.digipub.at
Wirtschaftsauskünfte beschränken sich auf Firmen/Unternehmer, Schwerpunkt sind Angaben aus dem Firmenbuch

LINK: http://www2.argedaten.at/php/cms_monitor.php?q=LIST-BONITAET



OGH E. 1.10.2008, 6 Ob 195/08g: Jeder darf Löschung seiner Bonitätsdaten beantragen

In einem Musterprozess fällten die Höchstrichter ein rasches Urteil: Demnach darf jeder die Löschung seiner Bonitätsdaten verlangen. Beklagter im Prozess war eine Kreditauskunftei gewesen: Sie sammelt alle öffentlich zugänglichen Bonitätsdaten (auch solche über Exekutionsverfahren). Diese Daten gibt die Kreditauskunftei an ein Partnerunternehmen weiter. Das war einem Mann, dem wegen der Datenweitergabe der Abschluss eines Vertrages mit einem Mobilfunkanbieter verwehrt wurde, ein Dorn im Auge: Er klagte mit Unterstützung von VKI (Verein für Konsumenteninformation) und Sozialministerium.

Bereits die Vorinstanzen hatten einen Anspruch auf Löschung der Daten festgehalten, der Oberste Gerichtshof bestätigte nun diese Ansicht: Es gelte das Widerspruchsrecht nach § 28 Abs 2 DSG. Der Betroffene könne ohne Angabe von Gründen die Löschung der Daten verlangen. Die Daten müssen dann innerhalb von acht Wochen gelöscht werden.

Die Befugnisse der DSK

Sie darf eine Menge....

Ideen, die wirken. itSV 38

Die Befugnisse der DSK (§§ 30ff DSG)

- **Unabhängige Kontrollstelle**
  - **Kollegialorgan mit richterl. Einschlag**
  - **oberste Instanz in DS-Angelegenheiten**
- **Klagebefugnisse**
  - **Feststellungsklage (§ 32 Abs. 5)**
  - **Nebenintervention (§ 32 Abs. 6)**
- **Überprüfungsbefugnis**
  - **auch ohne Vorliegen eines Verdachtes**
  - **Auskunftsrecht: öffentlicher und privater Bereich**

39

unabhängige Kontrollstelle iSd Art. 28 der Richtlinie wird die Datenschutzkommission eingesetzt (§ 30 DSG 2000), der die Kontrolle über sämtliche Auftraggeber einer Datenverarbeitung - soweit sie nicht der Gerichtsbarkeit oder der Gesetzgebung zuzurechnen ist - als zusätzliche, neue Kompetenz übertragen wird. Im Gegensatz zum bisherigen System (§ 41 DSG 1978) werden die Kontrollbefugnisse der DSK, die hinsichtlich laufender Datenverarbeitungen bisher nur auf den öffentlichen Bereich beschränkt waren, auch auf den privaten Bereich ausgedehnt (§ 31 DSG 2000).

Rechtsförmliche Entscheidungen über behauptete Datenschutzverletzungen werden hingegen so wie bisher von der Datenschutzkommission zu erlassen sein, wenn sie Auftraggeber der öffentlichen Bereichs betreffen, und von den ordentlichen Gerichten, wenn sie Auftraggeber des privaten Bereichs betreffen. (Kontrollbefugnis der DSK bezüglich des Auskunftsrechtes jedoch für den öffentlichen und privaten Bereich). § 31 Abs. 4 enthält besondere Regelungen für solche Beschwerdeverfahren, die in Konsequenz von §§ 26 Abs. 5 und 27 Abs. 5 vor der DSK geführt werden. Diese Regelung derogiert teilweise § 62 Abs. 4 und 5 SPG. Ab 1.1.2010: § 31 DSG enthält Regelungen über Beschwerdeverfahren, die in Konsequenz von § 26 oder §§ 27 und 28 vor der DSK geführt werden.

Wenn der Verdacht einer schwerwiegenden Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs vorliegt, kann die Datenschutzkommission anstelle des Betroffenen Feststellungsklage bei dem zuständigen Gericht erheben. Auf der Grundlage des gerichtlichen Feststellungsurteils kann der Betroffene sodann entscheiden, ob er seine Unterlassungs- und Schadenersatzansprüche selbst weiterverfolgen will. Die Möglichkeit einer Nebenintervention wurde beibehalten (§ 32 Abs. 6 DSG2000).

Wirkung von Bescheiden - Parteistellung (§ 40 DSG 2000): Hinsichtlich der bescheidmäßigen Erledigungen der Datenschutzkommission besteht die generelle Möglichkeit, den Verwaltungsgerichtshof anzurufen, nicht nur für die Parteien des Verfahrens, sonder neuerdings auch für die belangte Behörde. Besondere gesetzliche Vorschriften über das Recht der Amtsbeschwerde, wie etwa § 91 SPG, bleiben daneben aufrecht (Spezialnorm für SPG-Anwendungen). In jenen Konstellationen, in welchen jedoch im Datenschutzgesetz bei Auftraggebern des öffentlichen Bereichs die Eigenschaft als "belangte Behörde" nicht im Vordergrund steht, wie im Registrierungsverfahren und im Genehmigungsverfahren im internationalen Datenverkehr, wird den in Vollziehung der Gesetze tätigen Auftraggebern des öffentlichen Bereichs weiterhin Parteistellung und, daran anknüpfend, das Beschwerderecht an den VwGH eingeräumt.

Erläuterungen zu § 31 (DSG Novelle 2010):

Die Vollzugspraxis hat zahlreiche Probleme bei der Auslegung der bisherigen spärlichen Regelungen des § 31 Abs. 1 und 2 gezeigt. Zunächst war lange nicht klar, welchen Charakter die Bescheide der Datenschutzkommission haben. Durch Rechtsprechung des VwGH ist dies nunmehr weitgehend klargestellt (vgl. vor allem die beiden Erkenntnisse vom 28. März 2006, Zl. 2004/06/0125, und vom

27. Juni 2006, Zl. 2005/06/0366). An dieser orientiert sich auch der nunmehrige § 31 Abs. 7. Demnach ist eine Rechtsverletzung jedenfalls festzustellen. Nur bei Auftraggebern des privaten Bereich ist darüber hinaus ein – vollstreckbarer – Leistungsauftrag zu erteilen, der so zu formulieren ist, dass die festgestellte Rechtsverletzung beseitigt wird. Der Leistungsauftrag ist je nach dem Beschwerdebegehren bzw. den die Feststellung der Rechtswidrigkeit tragenden Gründen im Einzelfall zu formulieren. Es wird sich im Regelfall nicht auf ein konkret verarbeitetes Datum beziehen, weil die Datenschutzkommission die Rechtmäßigkeit der Auskunftserteilung nur ex post prüft und sie nicht an Stelle des Auftraggebers Auskunft zu erteilen hat. Somit wird der Leistungsauftrag in der Regel allgemeiner formuliert sein (zB „Der Beschwerdegegner hat innerhalb von zwei Wochen (neuerlich) Auskunft über die zur Person des Beschwerdeführers verarbeiteten Daten aus der Datenbank xy zu erteilen oder zu begründen, warum Auskunft nicht erteilt wird.“).

§ 31 vermeidet nunmehr insbesondere in den Abs. 1 und 2 die Verwendung des materiellrechtlichen Begriffs „Auftraggeber“ (ob jemandem diese Rolle zukommt, wird oft erst im Verfahren entschieden) und orientiert sich an der Formulierung von § 1 Abs. 5). Der lückenlosen Umsetzung dieser verfassungsrechtlichen Rechtsschutzbestimmung dient auch die „negative“ Abgrenzung der Beschwerdelegitimation nach Abs. 2, bezogen auf § 32 Abs. 1. Der Organbegriff ist weiterhin funktional zu verstehen, was durch die Formulierung „im Dienste“ nunmehr auch im Text verdeutlicht werden soll.

Weiters wird nun auch eine Beschwerdemöglichkeit im Hinblick auf die Rechte auf Bekanntgabe des Ablaufs einer automatisierten Einzelentscheidung (§ 49 Abs. 3) bzw. des verantwortlichen Auftraggebers in einem Informationsverbundsystem (§ 50 Abs. 1 dritter Satz) vorgesehen. Diesbezüglich bestand bisher (jedenfalls dem Wortlaut nach) eine Rechtsschutzlücke. **Weiters kann nunmehr auch gegen Dienstleister zur Durchsetzung des § 26 Abs. 10 vorgegangen werden.**

Eine gewisse Formalisierung des Beschwerdeverfahrens erfolgt nach dem Vorbild des § 67c Abs. 2 AVG durch die neuen Abs. 3 und 4 des § 31. Dadurch soll es der Datenschutzkommission ermöglicht werden, Beschwerden, die nicht einmal die genannten Minimalanforderungen aufweisen, nicht inhaltlich behandeln zu müssen. Wenn diese fehlen, kann nach § 13 Abs. 3 AVG vorgegangen werden. Eine Behandlung von Anbringen, die Abs. 3 und 4 nicht genügen, kann allenfalls im Verfahren nach § 30 erfolgen. Der VwGH hat in seinem Erkenntnis vom 6. Juni 2007, Zl. 2001/12/0004, ausgesprochen, dass ein Anspruch auf Löschung stets ein entsprechendes Begehren nach § 27 Abs. 1 Z 2 voraussetzt, was wohl sinngemäß auf das Auskunftsrecht zu übertragen ist. Daher müssen Auskunfts- bzw. Löschungsverlangen ohnehin stets vorliegen, um die Rechte erfolgreich geltend zu machen.

§ 31 Abs. 5 enthält lediglich eine Klarstellung, die bisher geübter Praxis entspricht.

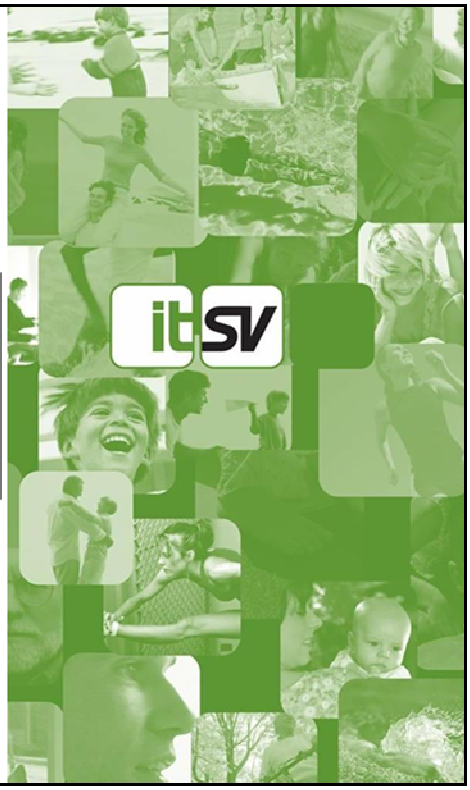
§ 31 Abs. 6 sieht aus Gründen der Verfahrensökonomie vor, dass ein Kontrollverfahren nach § 30 Abs. 1 nicht parallel zu einem Beschwerdeverfahren über denselben Gegenstand geführt werden soll. Freilich können über den Beschwerdegegenstand hinausgehende Verdachtsmomente (insbesondere im Hinblick auf Verpflichtungen, die nicht mit subjektiven Betroffenenrechten korrespondieren) von der Datenschutzkommission nach § 30 weiterverfolgt werden.

§ 31 Abs. 8 sieht eine besondere verfahrensrechtliche Regelung für den in der Praxis regelmäßig auftretenden Fall vor, dass ein Beschwerdeführer während des Auskunfts-, Richtigstellungs- oder Löschungsbeschwerdeverfahrens klaglos gestellt wird, dh die mit der Beschwerde verfolgte Auskunft erteilt oder die Löschung/Richtigstellung durchgeführt wird. Wurde die Beschwerde in einem solchen Fall nicht ausdrücklich zurückgezogen (§ 13 Abs. 7 AVG), so musste dennoch ein abweisender Bescheid erlassen werden, auch wenn auf Grund des Unterbleibens einer Stellungnahme des Beschwerdeführers im Parteiengehör zu vermuten war, dass dieser kein Interesse an der Weiterverfolgung seines Anspruches hat. Nunmehr soll es der Datenschutzkommission ermöglicht werden, in derartigen Fällen das Verfahren formlos (dh ohne Bescheiderlassung, wohl aber unter Verständigung des Beschwerdeführers) einzustellen, wenn der Beschwerdeführer nicht ausdrücklich auf einer Fortsetzung beharrt. Diese § 33 Abs. 1 VwGG nachgebildete Ergänzung des verfahrensrechtlichen Instrumentariums des AVG scheint im Hinblick auf das kontradiktorisch ausgestaltete Beschwerdeverfahren vor der Datenschutzkommission zweckmäßig. Die formlose Einstellung ist auch nicht präjudiziell, eine neue Beschwerdeerhebung innerhalb der Frist des § 34 Abs. 1 daher jederzeit möglich.

Besonders Bedacht genommen wird in der Bestimmung auch auf die immer wieder vorkommende wesentliche Änderung des Verfahrensgegenstandes (§ 13 Abs. 8 AVG) in einer derartigen Konstellation. Wenn etwa zunächst Beschwerde erhoben wurde, weil auf ein Auskunftsbegehren überhaupt nicht reagiert worden ist und während des Verfahrens eine Auskunft erteilt wird, die der Beschwerdeführer aber als unvollständig oder falsch ansieht, so ändert er bei einem entsprechenden Vorbringen den Verfahrensgegenstand wesentlich ab (s. zB den Bescheid der Datenschutzkommission vom 20. Juli 2007, GZ K121.289/0006-DSK/2007). Solche Fälle werden nunmehr entsprechend der bei *Thienel,* Verwaltungsverfahren, 3. Aufl., 112, wiedergegebenen herrschenden Ansicht, der die Datenschutzkommission in der Praxis schon bisher folgte, als (konkludente) Zurückziehung der ursprünglichen Beschwerde und gleichzeitige Einbringung einer weiteren Beschwerde mit dem geänderten Gegenstand gewertet. Damit beginnt auch die Entscheidungsfrist neu zu laufen. Zu verspäteten Äußerungen gilt das zum vorgeschlagenen § 20 Abs. 5 Gesagte sinngemäß. Die nach Abs. 3 erforderlichen Inhalte müssen sich in einem derartigen Fall schlüssig aus einer Zusammenschau von alter und neuer Beschwerde ergeben, ansonsten ist die neue Beschwerde mangelhaft.

Fragen?

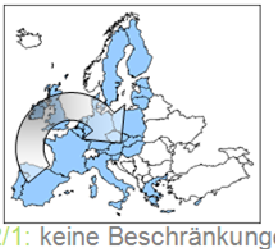
Danke für eure Aufmerksamkeit



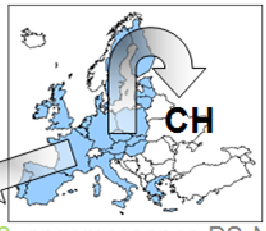
Spam § 107 TKG

- **Spam-Infoblatt der RTR GmbH:**
  www.rtr.at/de/tk/E_Commerce_Gesetz/Spam_Infoblatt.pdf
- **Robinsonliste:** **eintragen@ecg.rtr.at**
- **Spam wird überwiegend von Personen versandt, denen die rechtlichen Vorschriften egal sind. Diese Personen werden auch diese Liste nicht beachten.**

.datentransfer

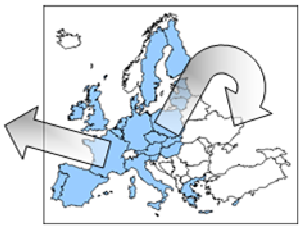


§ 12/1: keine Beschränkungen



§ 12/2: angemessenes DS-Niveau

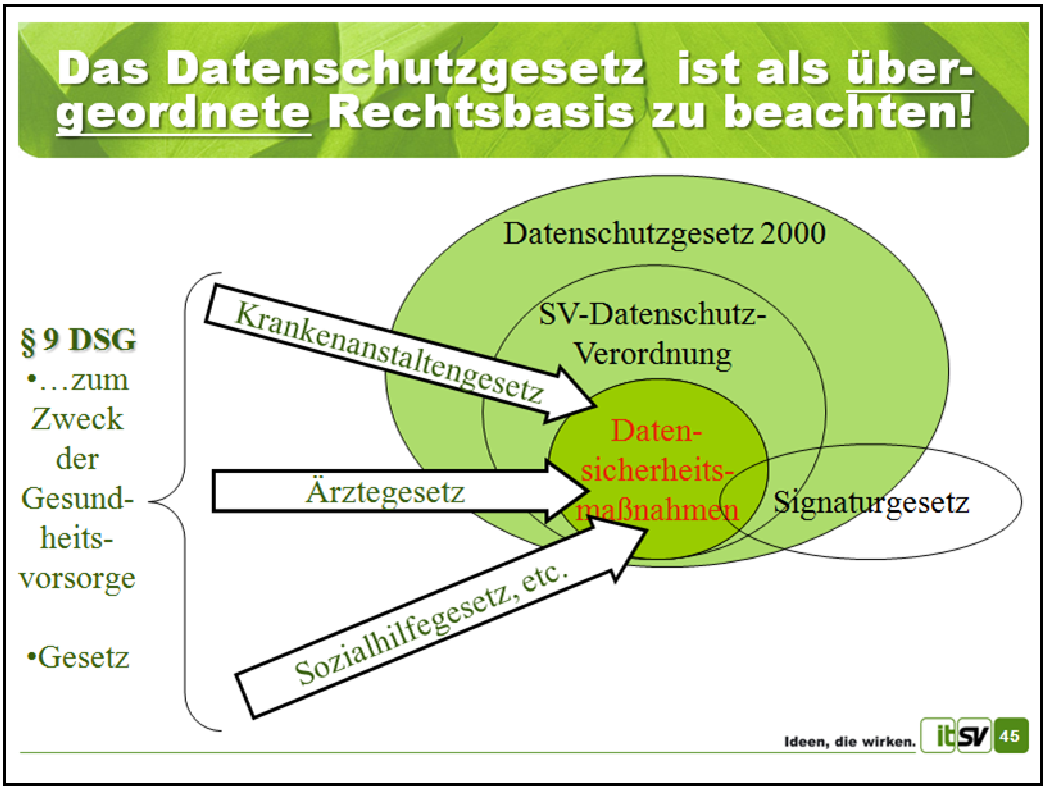
- § 12/3: Fälle von Genehmigungsfreiheit, betreffen best. Situationen unabhängig vom Ziel (außerhalb der EU)
  zB veröffentlichte oder indirekt pers-bez Daten, private Zwecke, Zustimmung etc.



§ 13: Genehmigung der DSK


Datenschutz im SV - Bereich
Das Gesundheitstelematikgesetz (GTelG)
ITSV GMBH _ Raimundgasse 1
A-1020 Wien
T: 050124 844 56 19
E: christoffer.stiger@itsv.at
www.itsv.at
ITSV Mitarbeiter
xxxxxxxx | xx.07.2009
Vortrag: Mag. Christoffer Stiger,
Bakk. LL.M. IT-Law
Ideen, die wirken.
itsv


Überblick
Datenschutzgesetz als Rechtsbasis
GTelG im datensicherheitsrechtlichen Kontext
Umsetzungsfristen - Anwendung des GTelG
Verwaltungsstrafen
Anwendungsbereich des GTelG
Elektronische Signatur
Verschlüsselungsverfahren
Identitätsprüfung
Verschlüsselungspflicht
Sicherstellung der Dokumentauthentizität
eHealth-Verzeichnisdienst



Das Datenschutzgesetz 2000 als Basis für das Gesundheitstelematikgesetz

§ 6 DSG Grundsätze für die Datenverwendung

§ 7 DSG Zulässigkeit der Verwendung v. Daten

§ 9 DSG Schutz v. Geheimhaltungsinteressen

- gesetzlichen Vorschriften
- Zustimmung
- lebenswichtige Interessen Zustimmung nicht rechtzeitig einholbar
- zum Zweck der Gesundheitsvorsorge + Verarbeitung durch Ärzte etc.

§§ 10, 11 DSG Inanspruchnahme von Dienstleistern

§ 14 DSG Datensicherheitsmaßnahmen

- Gesundheitstelematikgesetz (GTelG)
- § 9 SV-DSV

Das Gesundheitstelematikgesetz (als Teil des gesamten „Datenschutzrechtes“) spezifiziert die gem. § 14 Datenschutzgesetz zu implementierenden Sicherheitsmaßnahmen gezielt für den Gesundheitsbereich auf einem sehr hohen/strengen Sicherheitsniveau.

Daten dürfen nur verarbeitet und übermittelt werden, wenn:

Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind (§ 7 Abs. 1 DSG 2000) und schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden (§ 7 Abs. 1 DSG 2000).

Da Gesundheitsdaten sensible Daten iSd. § 4 Z 2 DSG 2000 sind, gilt § 9 DSG 2000, wonach die Verwendung von Daten nur in bestimmten Fällen zulässig ist; für den Bereich der Gesundheitsdaten sind die wichtigsten dieser Fälle, dass sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen (§ 9 Z. 3 DSG 2000),

oder

der Betroffene seine Zustimmung zur Verwendung der Daten ausdrücklich erteilt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt (§ 9 Z. 6 DSG 2000),

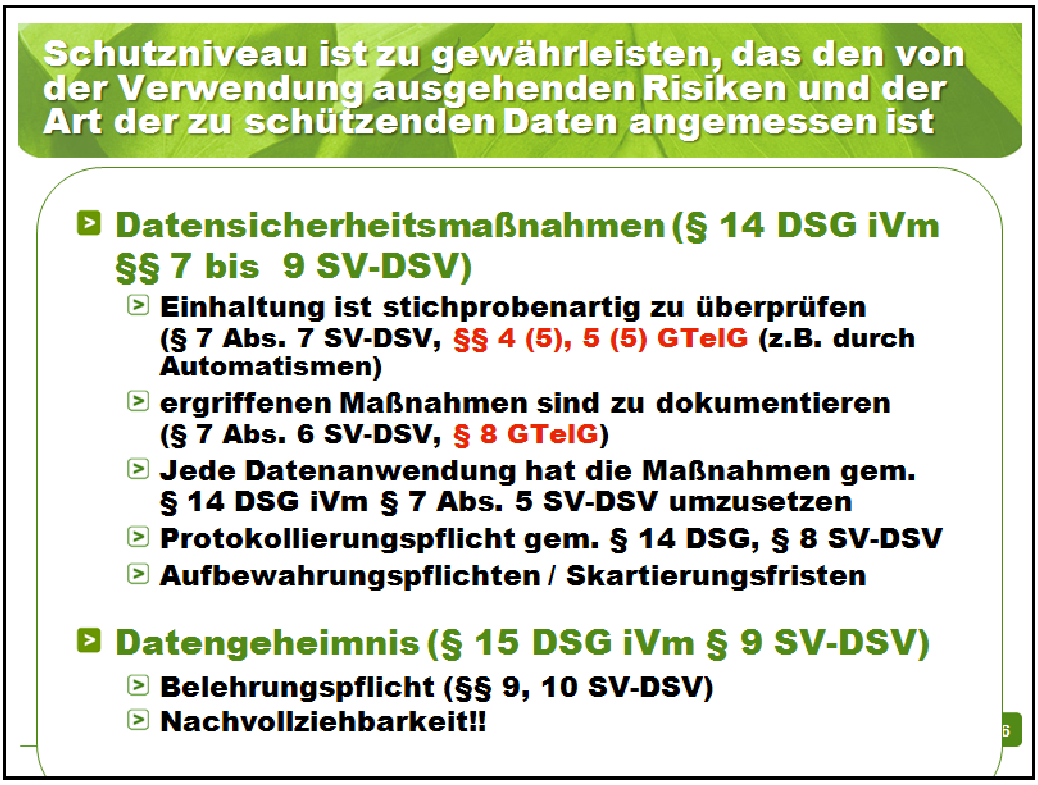
oder

die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann, z.B. Behandlung im Notfall (§ 9 Z. 7 DSG 2000),

oder

die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder Behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich sind und die Verwendung dieser Daten durch ärztliches Personal oder sonstiges Personal erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen (§ 9 Z. 12 DSG 2000).

Die Weiterverwendung von personenbezogenen Daten für wissenschaftliche oder statistische Zwecke ist nach Maßgabe der §§ 46 und 47 DSG 2000 zulässig.



Gemäß § 14 Abs. 1 iVm Abs. 2 erster sowie letzter Satz ist zu folgern, dass die u.a. Prinzipien nicht durchgehend verwirklicht werden müssen. Es kann daher *beispielsweise* die Protokollierungsverpflichtung entfallen, wenn auf eine Datenanwendung nur ein sehr beschränkter Personenkreis zugreift, sodass die Verantwortung bei allfälligem Missbrauch, bedingt durch organisatorische Maßnahmen, eindeutig erkennbar ist. Es ist jedoch in Summe ein System zu etablieren, welches je nach der Art der verwendeten Daten und nach Umfang und Zweck der Verwendung sowie unter Bedachtnahme auf den Stand der technischen Möglichkeiten und auf die wirtschaftliche Vertretbarkeit - sicherstellt, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind. Diese Maßnahmen müssen unter Berücksichtigung des Standes der Technik und der bei der Durchführung erwachsenden Kosten ein Schutzniveau gewährleisten, das den von der Verwendung ausgehenden Risiken und der Art der zu schützenden Daten angemessen ist. Diese Einschränkung ist allerdings **sehr restriktiv** zu beurteilen.

§ 14 Abs. 2 Datenschutzgesetz 2000:

Kompetenztrennungsprinzip (Z1): die Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und zwischen den Mitarbeitern ist ausdrücklich festzulegen. Es muss folglich eine genaue Rollenverteilung (beinhaltend eine genaue Rollenbeschreibung mit Funktionsbeschreibungen, Kommandostrukturen, u.ä.) existieren, was die Existenz einer klaren Aufbauorganisation bedingt.

Auftragsprinzip (Z2): die Verwendung von Daten ist an das Vorliegen gültiger Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter zu binden, was unter anderem die Verwirklichung des Kompetenztrennungsprinzips, die nachweisliche Belehrung über - beziehungsweise Bindung an - Geheimhaltungsverpflichtungen, eine Klassifikation von Geheimhaltungsstufen (geheim, streng geheim, u.ä.), sowie die Erstellung verschiedener Vorschriften betreffend den Umgang mit nicht mehr benötigten Datenträgern bedingt (Aktenshredder, Festplattenformatierungen, u.ä.).

Belehrungsverpflichtung (Z3): jeder Mitarbeiter ist über seine nach diesem Bundesgesetz und nach innerorganisatorischen Datenschutzvorschriften einschließlich der Datensicherheitsvorschriften bestehenden Pflichten zu belehren. Es ist folglich die Benutzung von Datenverarbeitungsanlagen, sowie jeweils einzelnen Datenanwendungen an einen Kenntnisnachweis zu binden (z.B: Teachwarekurse, inner und/oder außerbetriebliche Schulungen).

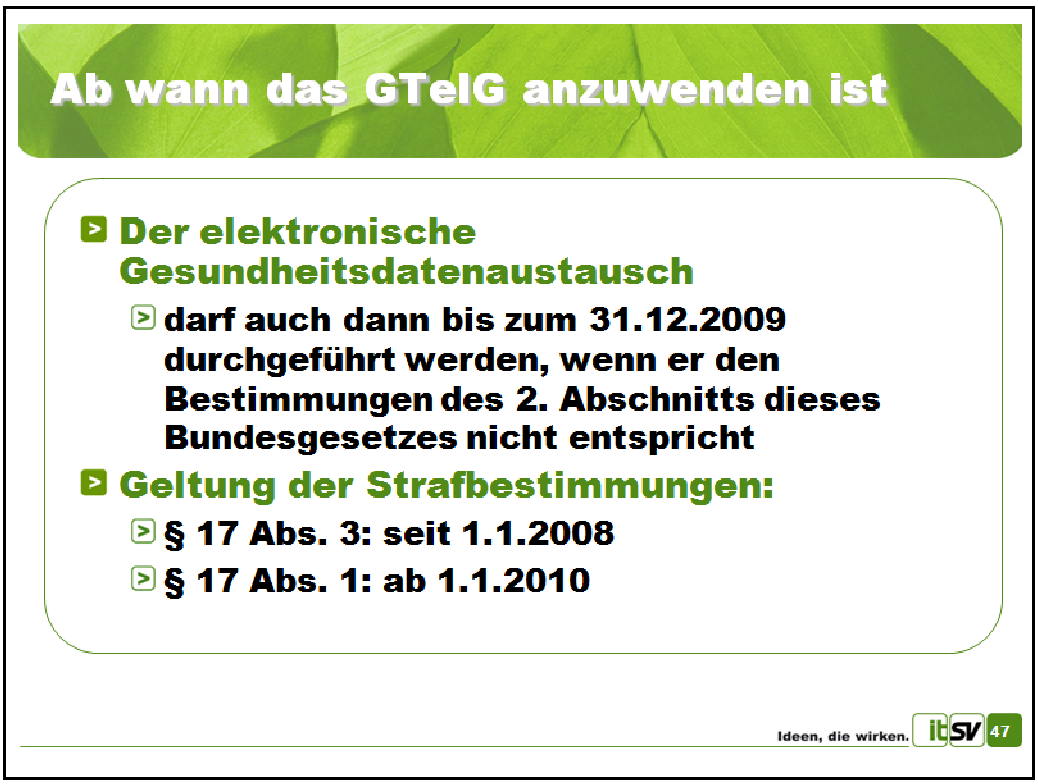
Zutrittsprinzip (Z4): die Zutrittsberechtigung zu den Räumlichkeiten des Auftraggebers oder Dienstleisters ist zu regeln. Es sind daher Zutrittsschranken (bauliche, technische sowie organisatorische) zu etablieren.

Benutzerverwaltung (Z 5 und 6): die Zugriffsberechtigung auf Daten und Programme und der Schutz der Datenträger vor der Einsicht und Verwendung durch Unbefugte ist zu regeln, sowie die Berechtigung zum Betrieb der Datenverarbeitungsgeräte festzulegen und jedes Gerät durch Vorkehrungen bei den eingesetzten Maschinen oder Programmen gegen eine unbefugte Inbetriebnahme abzusichern. Es ist folglich eine nicht zu umgehende (z.B. Einsatz von Passwörter, u.ä.) Benutzerverwaltung zu etablieren.

Protokollierungsverpflichtung (Z7): es ist Protokoll zu führen, damit tatsächlich durchgeführte Verwendungsvorgänge, wie insbesondere Änderungen, Abfragen und Übermittlungen, im Hinblick auf ihre Zulässigkeit im notwendigen Ausmaß nachvollzogen werden können. Eine Umgehung dieser Protokollierung, beispielsweise durch Zugriff auf die Datei mittels der Importfunktionen anderer Anwendungen, darf nicht möglich sein. *Übermittlungen* aus beim DVR gemeldeten Datenanwendungen brauchen nicht Protokolliert werden (§ 14 Abs. 3 DSG). Es ist nur eine zweckgebundene Verwendung der Protokolldateien erlaubt (§ 14 Abs. 4 DSG). *Grundsätzlich* beträgt die Aufbewahrungsfrist von Protokolldateien 3 Jahre (§ 14 Abs. 5 DSG). Grundsätzlich dürfen Protokolldateien nur für DS-Zwecke verwendet werden - ausgenommen: § §14 Abs. 4 DSG (org. Kriminal., Strafhöchstausmaß >5Jahre)

Dokumentationsprinzip (Z8): es ist eine Dokumentation über die nach Z 1 bis 7 getroffenen Maßnahmen zu führen, um die Kontrolle und Beweissicherung zu erleichtern (z.B: Datensicherheitshandbuch, Pflichtenheft).

***Grundvoraussetzung* ist eine ständige effiziente Kontrolle der Einhaltung aller o.a. Prinzipien.**

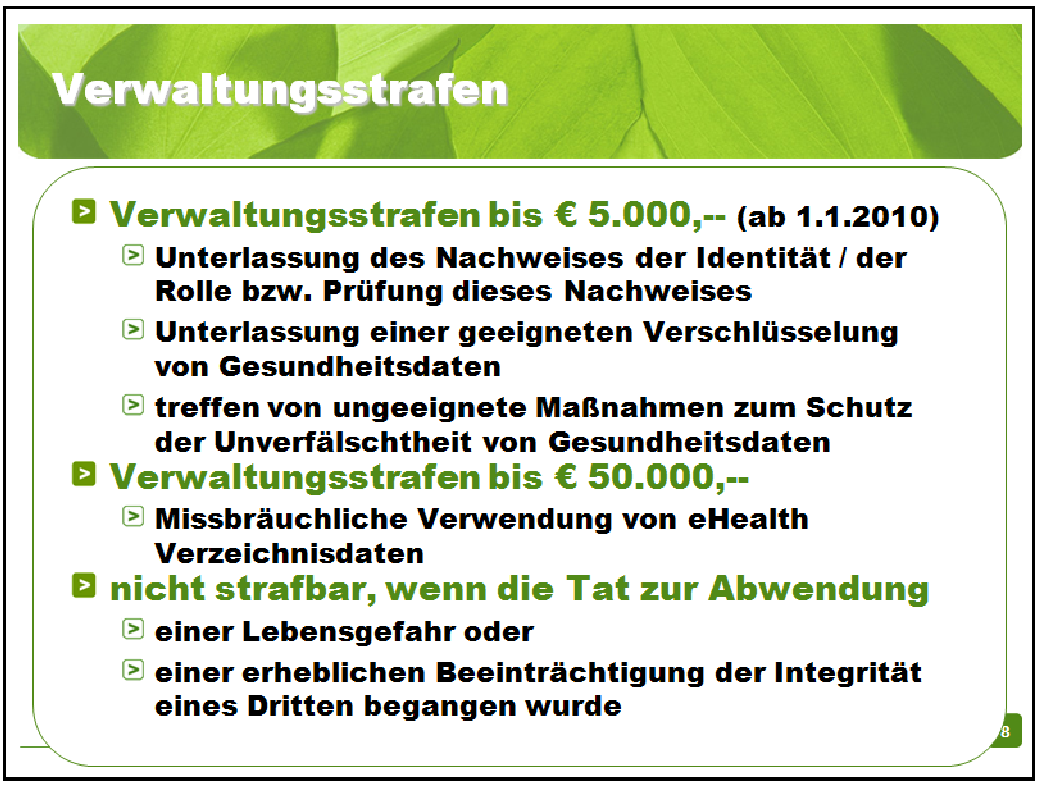


Übergangsbestimmungen

§ 19. (1) Die Betriebsbereitschaft des eHealth-Verzeichnisdienstes (§§ 9 bis 13) muss bis spätestens 1. Juli 2006 gegeben sein. Registrierungen oder die Freigabe des Zugriffs auf den eHealth-Verzeichnisdienst können jedoch nach Maßgabe einer früheren Betriebsbereitschaft, deren Zeitpunkt von der Bundesministerin für Gesundheit und Frauen/vom Bundesminister für Gesundheit und Frauen im Informationsdienst oder auf andere geeignete Weise zu veröffentlichen ist, erfolgen.
(2) Der elektronische Gesundheitsdatenaustausch darf auch dann bis zum 31.12.2009 durchgeführt werden, wenn er den Bestimmungen des 2. Abschnitts dieses Bundesgesetzes nicht entspricht.

Erlassung und In-Kraft-Treten von Verordnungen

§ 20. Verordnungen auf Grund dieses Bundesgesetzes in seiner jeweiligen Fassung dürfen bereits von dem Tag an erlassen werden, der der Kundmachung der durchzuführenden Gesetzesbestimmungen folgt; sie dürfen jedoch nicht vor den durchzuführenden Gesetzesbestimmungen in Kraft treten.



Verwaltungsstrafbestimmungen

§ 17. (1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu € 5.000,-- zu ahnden ist, wer beim elektronischen Gesundheitsdatenaustausch nach dem 31.12.2009

1. es entgegen der Bestimmungen der §§ 3 bis 5 unterlässt, die Nachweise der Identität und der Rolle zu erbringen oder diese Nachweise zu prüfen oder

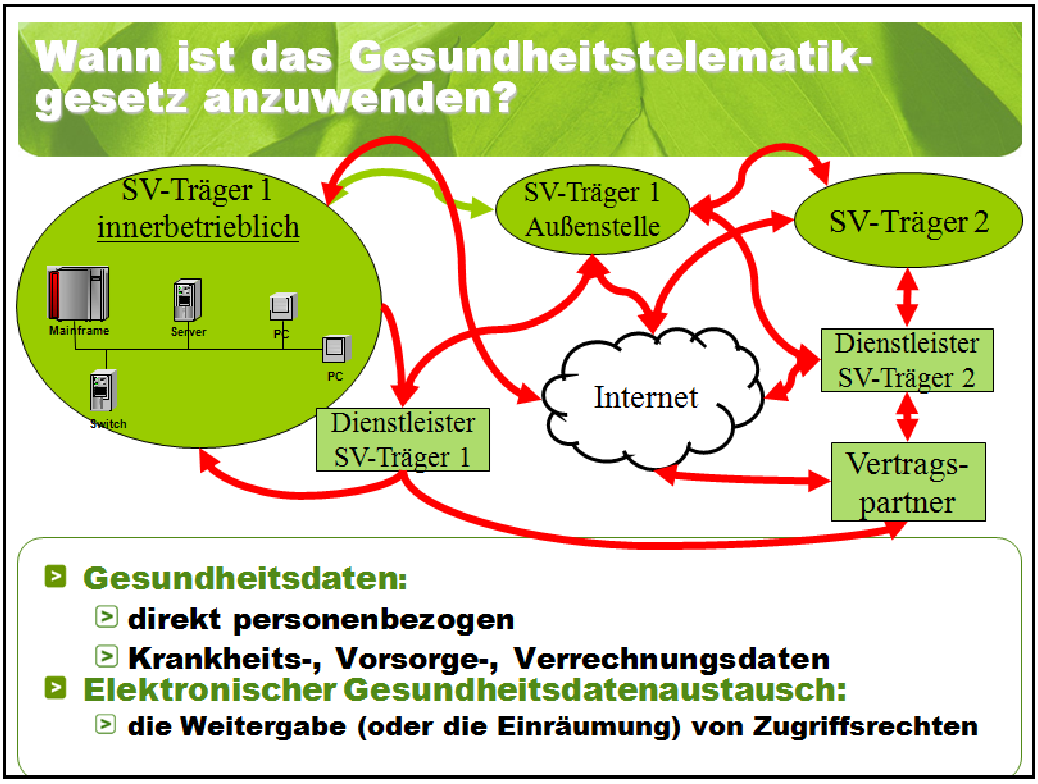
2. entgegen der Bestimmungen des § 6 die Verschlüsselung von Gesundheitsdaten unterlässt oder hiezu Methoden und Verfahren verwendet, die den qualitativen Anforderungen gemäß § 7 Abs. 5 nicht entsprechen oder

3. entgegen der Bestimmungen des § 7 keine elektronische Signatur verwendet oder eine elektronische Signatur verwendet, die den qualitativen Anforderungen nicht entspricht oder Gesundheitsdaten trotz fehlgeschlagener Signaturprüfung weitergibt oder verwendet.

(2) Eine Verwaltungsübertretung gemäß Abs. 1 ist nicht strafbar, wenn die Tat zur Abwendung einer gegenwärtigen oder unmittelbar drohenden Gefahr für das Leben einer/eines Dritten oder zur Abwendung einer gegenwärtigen oder unmittelbar drohenden Gefahr einer erheblichen Beeinträchtigung der physischen oder psychischen Integrität einer/eines Dritten begangen wurde.

(3) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu € 50.000,-- zu ahnden ist, wer entgegen der Bestimmung des § 9 Abs. 5 Daten oder Teile dieser Daten für andere Zwecke verwendet.

(4) Zuständig für Entscheidungen nach Abs. 1 bis 3 ist jene Behörde, in deren Sprengel die Verwaltungsübertretung begangen wurde.



Zu § 8 (Dokumentation):

Von diesem Bundesgesetz nicht erfasst wird der innerorganisatorische (innerbetriebliche) elektronische Gesundheitsdatenaustausch. Die im innerorganisatorischen Bereich zu treffenden bzw. getroffenen Datenschutz- und Datensicherheitsmaßnahmen einschließlich der Mechanismen ihrer Kontrolle sind gemäß § 14 DSG 2000 zu dokumentieren, was mit Abs. 1 klar gestellt wird. In den §§ 4, 5 und 7 sind jedoch für bestimmte technische Ausprägungen des elektronischen Gesundheitsdatenaustausches Abweichungen von den getroffenen Regelungen zugelassen, die einer ergänzenden Dokumentations- und Auskunftspflicht unterliegen.

Gegenstand

§ 1. (1) Mit diesem Bundesgesetz werden ergänzende Datensicherheitsbestimmungen für den elektronischen Verkehr mit Gesundheitsdaten festgelegt sowie ein Informationsmanagement für Angelegenheiten der Gesundheitstelematik eingerichtet.
(2) Ziele dieses Bundesgesetzes sind, durch bundeseinheitliche Mindeststandards die Datensicherheit beim elektronischen Verkehr mit Gesundheitsdaten anzuheben sowie die für die Entwicklung und Steuerung der Gesundheitstelematik im internationalen Kontext notwendigen Informationsgrundlagen zu schaffen bzw. zu verbreitern.

Begriffsbestimmungen

§ 2. Im Sinne dieses Bundesgesetzes bedeuten
1. Gesundheitsdaten: direkt personenbezogene Daten gemäß § 4 Z 1 DSG 2000 über die physische oder psychische Befindlichkeit eines Menschen, einschließlich der im Zusammenhang mit der Erhebung der Ursachen für diese Befindlichkeit sowie der medizinischen Vorsorge oder Versorgung, der Pflege, der Verrechnung von Gesundheitsdienstleistungen oder der Versicherung von Gesundheitsrisken erhobenen Daten. Dazu gehören insbesondere Daten die
a) die geistige Verfassung,
b) die Struktur, die Funktion oder den Zustand des Körpers oder Teile des Körpers,
c) die gesundheitsrelevanten Lebensgewohnheiten oder Umwelteinflüsse,
d) die verordneten oder bezogenen Arzneimittel, Heilbehelfe oder Hilfsmittel,
e) die Diagnose-, Therapie- oder Pflegemethoden oder

f) die Art, die Anzahl, die Dauer oder die Kosten von Gesundheitsdienstleistungen oder gesundheitsbezogene Versicherungsdienstleistungen betreffen.
2. Gesundheitsdiensteanbieterin/Gesundheitsdiensteanbieter: Auftraggeberinnen/Auftraggeber und Dienstleisterinnen/Dienstleister gemäß DSG 2000, deren regelmäßige Verwendung von Gesundheitsdaten Bestandteil ihrer Erwerbstätigkeit, ihres Betriebszwecks oder ihres Dienstleistungsangebotes ist.
3. Elektronischer Gesundheitsdatenaustausch: die Weitergabe von oder die Einräumung von Zugriffsrechten auf im Rahmen automationsunterstützter Datenanwendungen verwendeter Gesundheitsdaten mittels kommunikationstechnologischer Einrichtungen durch eine Gesundheitsdiensteanbieterin/einen Gesundheitsdiensteanbieter und zwar sowohl an Auftraggeberinnen/Auftraggeber (§ 4 Z 4 DSG 2000) als auch an Dienstleisterinnen/Dienstleister (§ 4 Z 5 DSG 2000).
4. Rolle: Klassifizierung von Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern nach der Art ihrer Erwerbstätigkeit, ihres Betriebszwecks oder ihres Dienstleistungsangebotes.

Zu § 2 des Entwurfs (Begriffsbestimmungen):

Zu Z 1:

Das DSG 2000 qualifiziert personenbezogene Gesundheitsdaten als ”sensible” Daten, für die das höchste Schutzniveau gilt. Eine Präzisierung, welche Daten dem Begriff „Gesundheitsdaten“ zuzuordnen sind, erfolgt nicht. Mit der WHO Definition von Gesundheit (Zustand des völligen körperlichen, geistigen und sozialen Wohlbefindens und nicht allein das Fehlen von Krankheit oder Gebrechen) wird deutlich, dass Gesundheitsdaten nicht mit Krankheitsdaten gleichzusetzen sind. In Z 1 des Entwurfes wird daher einerseits klar gestellt, dass unter Gesundheitsdaten auch Vorsorge-, Verrechnungs- und Versicherungsdaten zu verstehen sind. Andererseits werden diese Daten demonstrativ nach Datenkategorien beschrieben. Mit ”Struktur” wird der anatomische Aufbau des Körpers oder von Teilen des Körpers bezeichnet. Der Begriff ”Teil” des Körpers bezieht sich nicht nur auf sichtbare Ausprägungen, sondern auf alle Organe und Systeme, die in der medizinischen Wissenschaft als abgrenzbare Teile des Ganzen angesehen werden. Mit ”Funktion” werden die im menschlichen Körper ablaufenden Prozesse oder Vorgänge umschrieben, während ”Zustand” eine Beschreibung des Status ist. Ferner sind den Begriffen „Struktur“ bzw. „Funktion“ sowohl die personenbezogenen Basis-Informationen über das Erbgut (Sequenzdaten der DNA) als auch die daraus gewonnenen Erkenntnisse, etwa über die Bedeutung einer bestimmten Sequenz sowie die im Rahmen der Proteomik gewonnenen Erkenntnisse zu subsumieren. Mit lit. c werden Datenarten bezeichnet, die bei Bedarf im Rahmen der medizinischen Diagnostik erhoben werden und andererseits Sachverhalte – z.B. Daten über das Sexualleben, die dem Begriff „Lebensgewohnheiten“ zuzuordnen sind – betreffen, die selbst Gegenstand medizinischer Fragestellungen sein können.

Zu Z 2:

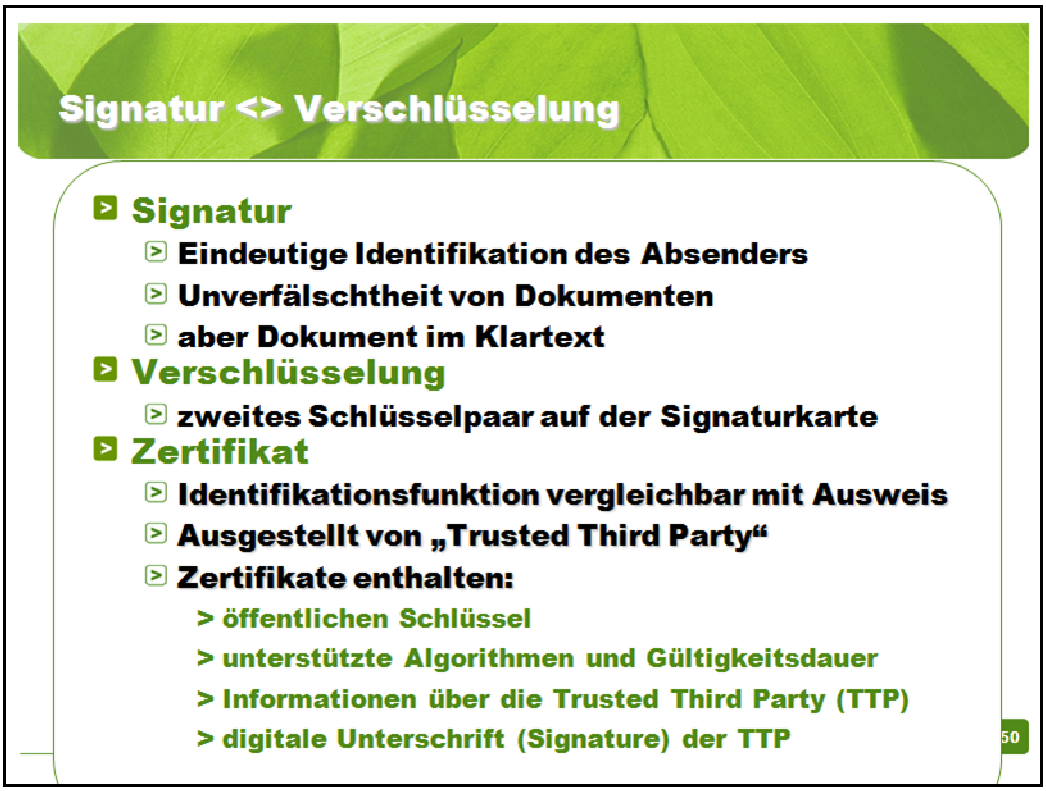
Ansatzpunkt für die im vorliegenden Entwurf vorgesehenen Datensicherheitsmaßnahmen ist das Gefahrenpotenzial beim Transport von Gesundheitsdaten. Als Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter sind jene Einrichtungen anzusehen, die durch eine **„regelmäßige“ und „berufsmäßige“** Auslösung von Kommunikationsvorgängen mit Gesundheitsdaten zu diesem Gefahrenpotenzial beitragen. Durch die Qualifikation der „Regelmäßigkeit“ sollen gelegentliche Übertragungsvorgänge, wie etwa fallweises Melden gesundheitsbezogener Angaben der Mitarbeiterinnen/MItarbeiter von Unternehmen, nicht dem Gesetz unterliegen.

Zu Z 3:

Der elektronische Gesundheitsdatenaustausch kann in unterschiedlicher technologischer Ausprägung (z.B. Mail, automatisierte Server-Server/Kommunikation, Client- Server/Applikationen) erfolgen. Dem Gesetz unterliegen alle Varianten und unabhängig davon, ob die Gesundheitsdaten aktiv weitergeben oder der Kommunikationspartnerin/dem Kommunikationspartner Zugriffsrechte auf Datenbestände eingeräumt werden. Nicht von Bedeutung ist, in welchem Datenformat oder in welcher Kombination von Datenformaten („multimediale Gesundheitsdaten“) die Gesundheitsdaten in elektronischer Form verwendet werden.

Zu Z 4:

Gemäß DSG 2000 (§ 7) ist die Übermittlung von Daten nur dann zulässig, wenn 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. Durch die berufliche/betriebliche Klassifizierung, die von der hiezu befugten Autorität zu bestätigen ist, soll dieser Prozess der Glaubhaftmachung in elektronisch überprüfbarer Form unterstützt und damit das für den elektronische Gesundheitsdatenaustausch vorauszusetzende Vertrauen gewährleistet werden. Grundsätzlich wird jedoch im Entwurf davon ausgegangen bzw. vorausgesetzt, dass Gesundheitsdaten rechtlich zulässig (gemäß DSG 2000) ausgetauscht werden.

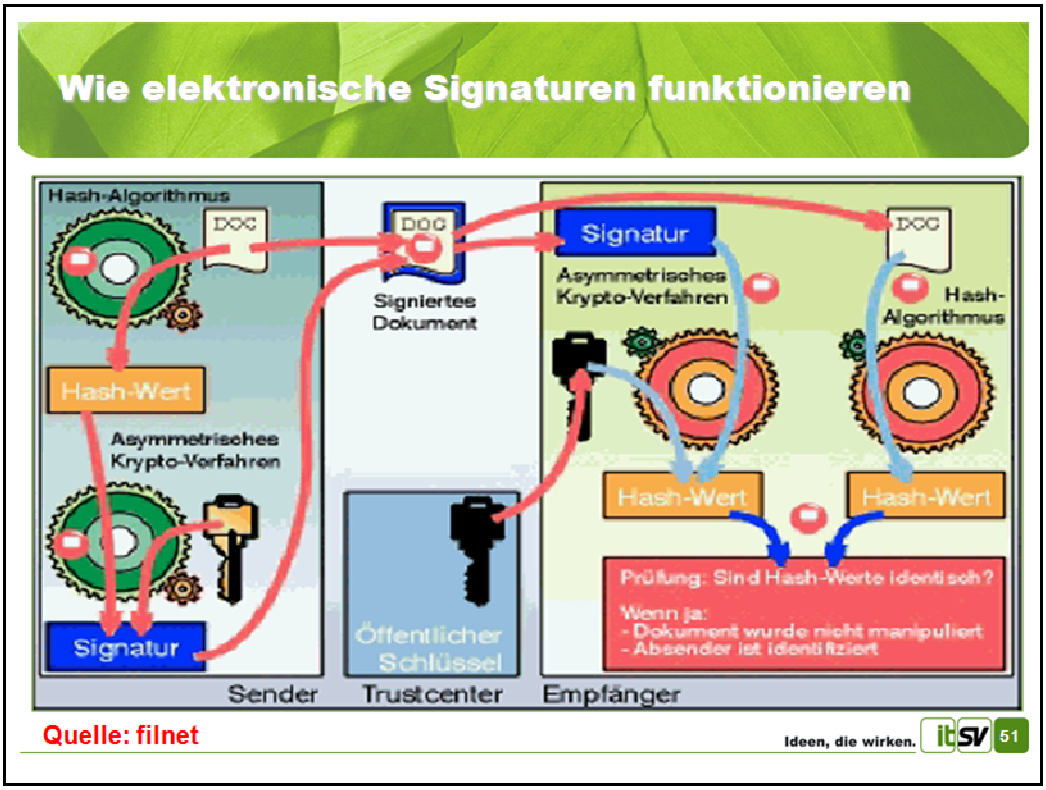


Unterschied zwischen Signatur und Verschlüsselung

Unter elektronischer Signatur versteht man Verfahren, die eine eindeutige Identifikation des Absenders ermöglichen sowie die Unverfälschtheit von Dokumenten sicherstellen.

Die Begriffe „Signatur" und „Verschlüsselung" werden oft ungenau verwendet. Bei der elektronischen Signatur wird das zu signierende Dokument durch die Ermittlung eines HashWertes (das ist ein elektronischer Fingerabdruck) elektronisch signiert und ist somit eindeutig einem bestimmten Absender zuordenbar, sowie vor jeglichen Veränderungen geschätzt. Das Dokument kann jedoch ohne Probleme von Dritten eingesehen werden.

Um Daten gegenüber Dritten zu sichern, ist es notwendig, diese zusätzlich zur Signatur noch elektronisch zu verschlüsseln. Die Verschlüsselung geschieht durch ein zweites sogenanntes Chiffrierschlüsselpaar auf der Signaturkarte. Die Nachricht wird so für Dritte unleserlich



1 Bildung des Hashwerts

Ein Hashwert kann als „digitaler Fingerabdruck" eines Dokuments gesehen werden. Es ist eine meist 20-stellige Prüfsumme, die einzigartig ist. Neben dieser Kollisionsfreiheit handelt es sich bei der Bildung des Hashwerts um eine Einwegfunktion – d.h., dass vom Hashwert nicht auf den ürsprüglichen Text geschlossen werden kann. Für die Ermittlung des Hashwerts gibt es mehrere Verfahren wie MD4/MD5, SHA-1 oder RIPEMD-160. Von A-Trust wird das SHA-1 Verfahren zur Bildung des Fingerprints verwendet. Die Signaturverordnung erlaubt neben dem SHA-1 Verfahren auch noch andere Verfahren.

Zuerst wird vom Text mittels der Hash-Funktion der Hashcode generiert. Dieser wird mit dem öffentlichen Schlüssel des Signators (Versenders) verschlüsselt und als „Signatur" dem Dokument angehängt. Der Text des Dokuments selbst wird dadurch weder verändert noch verschlüsselt. Anschließend kann das signierte Dokument – z.B. per E-Mail – an den Empfänger übermittelt werden.

2 Bildung der Signatur

Der erzeugte Hashwert wird direkt auf der Signaturkarte des Signators mit dem privaten Schlüssel verschlüsselt. Die somit erzeugte Signatur wird als Dateianhang gemeinsam mit dem signierten Dokument/Mail anschließend versendet

3 Kontrolle der Signatur

Der Empfänger der signierten Nachricht kann die Signatur durch den öffentlichen Schlüssel des Absenders auf die Echtheit prüfen. Durch die Software entschlüsselt der Empfänger die Signatur und erhält so den Hashwert (in Abbildung 3: mitgeschickter „Fingerabdruck").

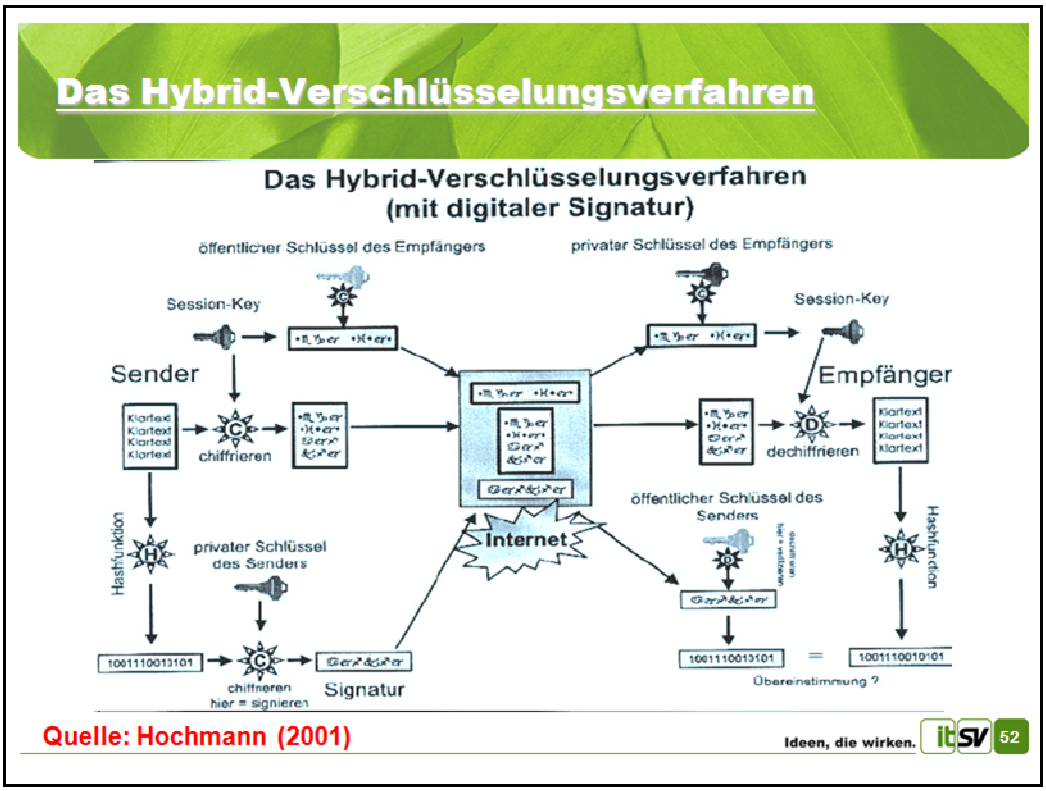
Von der empfangenen Nachricht wird beim Empfänger wieder wie beim Signator ein Hashwert ermittelt (neu erzeugter „Fingerabdruck"). Stimmen die beiden Hashwerte überein, liegt ein positives Prüfungsergebnis vor. Der Empfänger kann sich also sicher sein, dass das Dokument vom richtigen Absender stammt und dass es auf dem Weg durch das Internet nicht durch Dritte verändert wurde.

Zertifikat:

Der Empfänger erhält den öffentlichen Schlüssel des Senders durch das Zertifikat des Signators. Dieser kann entweder mit der E-Mail mitgesendet werden, oder der Emfpänger kann ihn aus dem Verzeichnisdienst des Zertifizierungsdienstanbieters downloaden.

Bei der Überprüfung des Zertifikats des Signators wird geprüft, wann und von wem es ausgestellt wurde; ob es noch gültig ist und ob es eventuell gesperrt wurde. Ist auch diese Überprüfung erfolgreich, kann sich der Empfänger vollkommen auf die Echtheit des Absenders und die Gültigkeit des Zertifikats verlassen.

(Quelle: Diplomarbeit v. David Roithner,)



Das Hybrid-Verschlüsselungsverfahren (mit digitaler Signatur)

Abbildung 12: Hybride Verschlüsselung mit elektronischer Signatur **Quelle:** Hochmann (2001); S. 27

Quelle: Roithner David Elektronische Signatur http://www.rechtsprobleme.at, Seite 18

2.4.3 Hybrides Verschlüsselungsverfahren (Triple-DES-Verfahren)

Das Hybride Verschlüsselungsverfahren kombiniert die Vorteile des symmetrischen und a-symmetrischen Verschlüsselungsverfahrens. So wird die Nachricht durch das symmetrische Verfahren schnell und einfach verschlüsselt. Anschließend wird mit Hilfe des asymmetrischen Verfahrens der Schlüssel sicher übertragen.

Auf den Signaturkarten von A-Trust wird das sogenannte Triple-DES Verfahren verwendet. Erst zum Transport des DES-Schl ssels wird dieser durch das asymmetrischen Verfahren mit dem öffentlichen Schlüssel des Empfängers dreimal verschlüsselt. Nur der Empfänger kann mit seinem privaten Schlüssel den DES-Schlüssel wieder entschlüsseln und anschließend die gesamte Nachricht (durch das symmetrische Verfahren) für ihn wieder lesbar machen.

Roithner David Elektronische SignaturQuelle: http://www.rechtsprobleme.at Seite 19

Im der unteren Hälfte der Abbildung 12 sieht man das in Kapitel 2.3 (Ablauf der Signatur) erklärte Signaturverfahren. So wird zuerst der Hashwert der Nachricht ermittelt und dieser anschließend mit dem privaten Schlüssel des Senders verschlüsselt. Der Empfänger kann diese Signatur mit dem öffentlichen Schlüssel des Senders wieder entschlüsseln. Anschließend wird der empfangene Hashwert mit dem gerade gebildeten Hashwert dieser Nachricht verglichen. So kann verifiziert werden, dass das Dokument auf dem Weg durch das Internet nicht geändert worden ist.

Der obere Bereich zeigt, wie das Dokument zuerst mit dem generierten Session-Key – den es nur einmal gibt – verschlüsselt wird. Erst dieser Session-Key wird dann durch das TripleDES-Verfahren verschlüsselt und gemeinsam mit der Nachricht verschickt. Nur der richtige Empfänger kann den Session-Key mit seinem privaten Schlüssel entschlüsseln und dadurch die Nachricht – durch das symmetrische Verfahren – wieder lesbar machen.

Datensicherheit beim elektronischen Gesundheitsdatenaustausch:

Nachweis von Identität und Rolle

§ 3. Im elektronischen Verkehr zwischen Gesundheitsdiensteanbietern dürfen Gesundheitsdaten nur weitergegeben oder Zugriffsrechte darauf eingeräumt werden, wenn Identität und Rolle der Empfängerin/des Empfängers oder jenes Gesundheitsdiensteanbieters, der ein eingeräumtes Zugriffsrecht auf Gesundheitsdaten in Anspruch nehmen will, nachgewiesen sind. Die Nachweise sind nach Maßgabe der §§ 4 und 5 in elektronischer Form zu erbringen und zu überprüfen.

Zu § 3 (Nachweis und Prüfung von Identität und Rolle):

Die Bestimmung legt in grundsätzlicher Form fest, dass Gesundheitsdaten in elektronischer Form nur ausgetauscht werden dürfen, wenn die Identität und die Rolle elektronisch nachgewiesen und geprüft sind.

Ein Gesundheitsdiensteanbieter hat die Wahlmöglichkeit, ob er die Nachweise gesondert erbringt und prüfbar macht oder dies im Wege der Eintragung in den eHealth-Verzeichnisdienst ermöglicht.

Identität

§ 4. (1) Der Nachweis der Identität ist durch Vorlage einer elektronischen Bescheinigung (Zertifikat), mit der die Identität des Gesundheitsdiensteanbieters bestätigt wird, zu erbringen und zu prüfen. Das Zertifikat muss den gemäß § 7 Abs. 5 festgelegten Mindestanforderungen entsprechen.
(2) Der Nachweis gemäß Abs. 1 kann unterbleiben, wenn der Gesundheitsdiensteanbieter in den eHealth-Verzeichnisdienst eingetragen ist und dies vom die Gesundheitsdaten weitergebenden oder den Zugriff darauf einräumenden Gesundheitsdiensteanbieter durch Einsichtnahme in den eHealth-Verzeichnisdienst überprüft wird.
(3) Wird der elektronische Gesundheitsdatenaustausch ausschließlich programmgesteuert abgewickelt, ist - abweichend von Abs. 1 und 2 - der Nachweis der Identität mittels Serverzertifikaten zu erbringen und programmgesteuert zu prüfen. Serverzertifikate müssen den gemäß § 7 Abs. 5 festgelegten Mindestanforderungen entsprechen.
(4) Wird im Rahmen des elektronischen Gesundheitsdatenaustausches eine Datenanwendung direkt aus der Entfernung bedient und ist der Nachweis bzw. die Prüfung der Identität gemäß Abs. 1 oder 2 im Einzelfall aus technischen oder wirtschaftlichen Gründen unzweckmäßig, ist die Identität im Zuge der Implementierung der Zugangsberechtigung nachzuweisen und zu prüfen. Während des Bestehens der Zugangsberechtigung ist die Identität in periodischen Abständen zu prüfen.
(5) Für die Prüfung der Identität im Rahmen des elektronischen Gesundheitsdatenaustausches während einer bestehenden Zugangsberechtigung gemäß Abs. 4 haben Gesundheitsdiensteanbieter den Grund, die Periodizität, die einen Monat nicht übersteigen darf, die bei der Prüfung einzuhaltende Vorgangsweise sowie die Mechanismen zur Sicherstellung und Kontrolle ihrer Durchführung zu dokumentieren.

Zu § 4 (Identität):

Nachweis und Prüfung der Identität erfolgen durch Vorlage bzw. Prüfung eines Zertifikats. Der Identitätsnachweis kann unter Hinweis auf die Eintragung in den eHealth-Verzeichnisdienst unterbleiben, die Prüfung wird durch Verifizierung der Verzeichniseintragung vereinfacht. Die Identitätsprüfung hat im Rahmen der Eintragung zu erfolgen, die Aktualität der Daten wird durch die Verpflichtung zur laufenden Berichtigung gewährleistet.

Durch die Festlegung von qualitativen Mindestanforderungen an die zu verwenden Zertifikate steht jenen Gesundheitsdiensteanbietern, die bereits über fortgeschrittenere Technologien (z.B. Bürgerkarte) verfügen, die Möglichkeit offen, diese auch zu verwenden.

Die Abs. 3 und 4 sehen besondere Bestimmungen für die Identifizierung bei speziellen technischen Lösungen (server-server, client-server) vor, wobei die Modalitäten für Identitätsprüfungen im Rahmen von client-server/Anwendungen zu dokumentieren und ihre Beachtung nachzuweisen sind (Abs. 5 bzw. § 8 Abs. 2).

Rolle

§ 5. (1) Die Bundesministerin für Gesundheit und Frauen/Der Bundesminister für Gesundheit und Frauen hat die für den elektronischen Gesundheitsdatenaustausch in Betracht kommenden Rollen sowie jene Stellen, die die Zuordnung von Rollen zu einem Gesundheitsdiensteanbieter authentisch bestätigen, mit Verordnung festzulegen.
(2) Der Nachweis der Rolle ist durch Vorlage einer elektronischen Bescheinigung (Zertifikat) einer gemäß Abs. 1 festgelegten Stelle zu erbringen und zu prüfen. Das Zertifikat muss den gemäß § 7 Abs. 5 festgelegten Mindestanforderungen entsprechen.
(3) Der Nachweis gemäß Abs. 2 kann unterbleiben, wenn der Gesundheitsdiensteanbieter in den eHealth-Verzeichnisdienst eingetragen ist und die Rolle vom die Gesundheitsdaten weitergebenden oder den Zugriff darauf einräumenden Gesundheitsdiensteanbieter durch Einsichtnahme in den eHealth-Verzeichnisdienst überprüft wird.
(4) Wird der elektronische Gesundheitsdatenaustausch ausschließlich programmgesteuert abgewickelt und ist der Nachweis und die Prüfung der Rolle im Einzelfall aus technischen oder wirtschaftlichen Gründen unzweckmäßig, hat der Nachweis bzw. die Prüfung der Rolle der Empfängerin/des Empfängers der Gesundheitsdaten vor der erstmaligen Durchführung des Gesundheitsdatenaustausches zu erfolgen. Im laufenden Betrieb ist die Rolle in periodischen Abständen zu prüfen.

(5) Wird im Rahmen des elektronischen Gesundheitsdatenaustausches eine Datenanwendung direkt aus der Entfernung bedient und ist der Nachweis und die Prüfung der Rolle im Einzelfall aus technischen oder wirtschaftlichen Gründen unzweckmäßig, hat der Nachweis und die Prüfung der Rolle vor der Implementierung der Zugangsberechtigung zur Datenanwendung zu erfolgen. Während des Bestehens der Zugangsberechtigung ist die Rolle in periodischen Abständen zu prüfen.
(6) Für die Prüfung der Rolle im Rahmen des elektronischen Gesundheitsdatenaustausches im laufenden Betrieb gemäß Abs. 4 oder während einer bestehenden Zugangsberechtigung gemäß Abs. 5 haben Gesundheitsdiensteanbieter den Grund, die Periodizität, die einen Monat nicht übersteigen darf, die bei der Prüfung einzuhaltende Vorgangsweise sowie die Mechanismen zur Sicherstellung und Kontrolle ihrer Durchführung zu dokumentieren

Zu § 5 (Rollen)

Mit der in Abs. 1 vorgesehenen Verordnung sind die Rollen für den elektronischen Gesundheitsdatenaustausch sowie jene Stellen, die diese Rollen bestätigen, festzulegen. Bezüglich der Rollen werden dies nicht nur die Gesundheitsdiensteanbieter im engeren Sinn sein, sondern auch Personen oder Institutionen, die an den Schnittstellen von Gesundheits- und Sozialwesen tätig sind und aufgrund ihrer beruflichen oder betrieblichen Tätigkeit regelmäßig Gesundheitsdaten verwenden (z.B. Rehabilitationseinrichtungen).

Die Bestätigung der Rollen soll im Wesentlichen durch juristische Personen des öffentlichen Rechts erfolgen. Dies können berufliche Interessenvertretungen (z.B. Österreichische Ärztekammer, Österreichische Apothekerkammer) oder solche Einrichtungen sein, die aufgrund bestehender Rechtsvorschriften zur Festlegung von Voraussetzungen für den Betrieb oder die Erteilung von Betriebsbewilligungen berufen sind. Bestehen für bestimmte Rollen solche Einrichtungen nicht, ist in der Verordnung zu festzulegen, welche Stelle eine solche Bestätigung erteilt.

Der Nachweis bzw. die Prüfung der Rolle orientieren sich an den Bestimmungen der Identitätsprüfung, womit unterstrichen wird, dass diese Vorgänge im Rahmen des elektronischen Gesundheitsdatenaustausches eine Einheit bilden sollen. Im Hinblick darauf, dass Identitätsnachweis und -prüfung auch mittels qualitativ besseren Methoden möglich sein soll, werden beide Vorgänge getrennt geregelt.

E-Government-Gesetz:

Identität und Authentizität

§ 3. (1) Im elektronischen Verkehr mit Auftraggebern des öffentlichen Bereichs im Sinne des § 5 Abs. 2 des Datenschutzgesetzes 2000, BGBl. I Nr. 165/1999, dürfen Zugriffsrechte auf personenbezogene Daten (§ 4 Z 1 DSG 2000), an welchen ein schutzwürdiges Geheimhaltungsinteresse im Sinne des § 1 Abs. 1 DSG 2000 besteht, nur eingeräumt werden, wenn die eindeutige Identität desjenigen, der zugreifen will, und die Authentizität seines Ersuchens nachgewiesen sind. Dieser Nachweis muss in elektronisch prüfbarer Form erbracht werden. Ist nur der Nachweis der Wiederholungsidentität möglich, darf Zugriff nur auf jene personenbezogenen Daten des Einschreiters gewährt werden, die er selbst unter dieser Identität zur Verfügung gestellt hat.

(2) Im Übrigen darf eine Identifikation von Betroffenen im elektronischen Verkehr mit Auftraggebern des öffentlichen Bereichs nur insoweit verlangt werden, als dies aus einem überwiegenden berechtigten Interesse des Auftraggebers geboten ist, insbesondere weil dies eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist.

Die Funktion "Bürgerkarte„

§ 4. (1) Die Bürgerkarte dient dem Nachweis der eindeutigen Identität eines Einschreiters und der Authentizität des elektronisch gestellten Anbringens in Verfahren, für die ein Auftraggeber des öffentlichen Bereichs eine für den Einsatz der Bürgerkarte taugliche technische Umgebung eingerichtet hat.

(2) Die eindeutige Identifikation einer natürlichen Person, die rechtmäßige Inhaberin einer Bürgerkarte ist, wird in ihrer Bürgerkarte durch die Personenbindung bewirkt: Von der

Stammzahlenregisterbehörde (§ 7) wird elektronisch signiert bestätigt, dass der in der Bürgerkarte als Inhaberin bezeichneten natürlichen Person eine bestimmte Stammzahl zur eindeutigen Identifikation zugeordnet ist. Hinsichtlich des Identitätsnachweises im Fall der Stellvertretung gilt § 5.

(3) Die Eintragung der Personenbindung in der Bürgerkarte erfolgt durch die Stammzahlenregisterbehörde oder in ihrem Auftrag durch andere Behörden oder sonstige geeignete Stellen, die in der gemäß Abs. 5 zu erlassenden Verordnung näher zu bezeichnen sind. Die Eignung ist nach dem Vorhandensein der notwendigen technischen Ausstattung und der zu ihrer Nutzung notwendigen Fachkenntnisse sowie der Verlässlichkeit im Hinblick auf die Einhaltung der rechtlichen Rahmenbedingungen zu beurteilen.

(4) Die Authentizität eines mit Hilfe der Bürgerkarte gestellten Anbringens wird durch die in der Bürgerkarte enthaltene elektronische Signatur nachgewiesen.

(5) Die näheren Regelungen zu den Abs. 1 bis 4 sind, soweit erforderlich, durch Verordnung des Bundeskanzlers im Einvernehmen mit den allfällig sonst zuständigen Bundesministern zu erlassen. Vor Erlassung der Verordnung sind die Länder und die Gemeinden, letztere vertreten durch den Gemeindebund und den Städtebund, anzuhören.

Bürgerkarte und Stellvertretung

§ 5. (1) Soll die Bürgerkarte für vertretungsweise Anbringen verwendet werden, muss auf der Bürgerkarte des Vertreters ein Hinweis auf die Zulässigkeit der Vertretung eingetragen sein. Dies geschieht dadurch, dass die Stammzahlenregisterbehörde 1. bei Nachweis eines aufrechten Vollmachtsverhältnisses bzw. Vorliegen gesetzlicher Stellvertretung auf Antrag des Vertreters die Stammzahl des Vertretenen und das Bestehen eines Vollmachtsverhältnisses mit allfälligen inhaltlichen und zeitlichen Beschränkungen auf der Bürgerkarte des Vertreters einträgt oder 2. in den Fällen berufsmäßiger Parteienvertretung, in welchen ein besonderer Vollmachtsnachweis nicht erforderlich ist, auf der Bürgerkarte des Vertreters die Berechtigung zur berufsmäßigen Parteienvertretung elektronisch nachprüfbar anmerkt. Die elektronische Identifikation des Vertretenen erfolgt diesfalls gemäß § 10 Abs. 2.

(2) § 4 Abs. 3 gilt für die nach dem Abs. 1 notwendigen Eintragungen in die Bürgerkarte sinngemäß.

(3) Soweit bei Gemeinden oder Bezirksverwaltungsbehörden diese Dienstleistung eingerichtet ist, können bei diesen Behörden unabhängig von ihrer sachlichen und organisatorischen Zuständigkeit hiezu eigens ermächtigte Organwalter für Betroffene auf deren Verlangen Anträge in bürgerkartentauglichen Verfahren stellen. Der Antrag wird mit Hilfe der Bürgerkarte des Organwalters gefertigt, die elektronische Identifikation des Betroffenen im Antrag erfolgt gemäß § 10 Abs. 2. Die generelle Befugnis des Organwalters zur Antragstellung für Betroffene muss aus dem Signaturzertifikat seiner Bürgerkarte hervorgehen; der konkrete Auftrag seitens des Betroffenen ist durch die Beurkundung der bei der Behörde aufzubewahrenden Kopie des Antrags als Niederschrift gemäß § 14 AVG zu dokumentieren.

Stammzahl

§ 6. (1) In der Bürgerkarte erfolgt die eindeutige Identifikation von Betroffenen durch ihre Stammzahl.

(2) Für natürliche Personen, die im Zentralen Melderegister einzutragen sind, wird die Stammzahl durch eine mit starker Verschlüsselung gesicherte Ableitung aus ihrer ZMR-Zahl (§ 16 Abs. 1 des Meldegesetzes 1991, BGBl. Nr. 9/1992) gebildet. Für alle anderen natürlichen Personen ist ihre Ordnungsnummer im Ergänzungsregister (Abs. 4) für die Ableitung der Stammzahl heranzuziehen. Die Benützung der ZMR-Zahl zur Bildung der Stammzahl ist keine Verwendung von Daten des Zentralen Melderegisters im Sinne des § 16a des Meldegesetzes 1991.

(3) Für juristische Personen und sonstige Betroffene, die keine natürlichen Personen sind, ist als Stammzahl die Firmenbuchnummer (§ 3 Z 1 des Firmenbuchgesetzes, BGBl. Nr. 10/1991) bzw. die ZVR-Zahl (§ 18 Abs. 3 des Vereinsgesetzes 2002, BGBl. I Nr. 66/2002) bzw. die im Ergänzungsregister (Abs. 4) vergebene Ordnungsnummer zu verwenden.

(4) Betroffene, die weder im Melderegister noch im Firmenbuch oder im Vereinsregister eingetragen sein müssen, sind auf ihren Antrag oder in den Fällen des § 10 Abs. 2 auf Antrag des Auftraggebers der Datenanwendung von der Stammzahlenregisterbehörde (§ 7) für Zwecke des elektronischen Nachweises ihrer eindeutigen Identität in das Ergänzungsregister einzutragen. Voraussetzung hiefür ist bei natürlichen Personen der Nachweis jener Daten, die den Identitätsdaten im Sinne des § 1 Abs. 5a des Meldegesetzes 1991 entsprechen, bei anderen Betroffenen der Nachweis ihres rechtlichen Bestandes einschließlich ihrer rechtsgültigen Bezeichnung. Das Ergänzungsregister wird getrennt nach natürlichen Personen und sonstigen Betroffenen geführt. In dem die sonstigen Betroffenen erfassenden Teil des Ergänzungsregisters kann auch die Erteilung von Handlungsvollmachten eingetragen werden. Bei welchen Stellen der Nachweis von Daten für die Eintragung in das Ergänzungsregister im Inland und im Ausland erbracht werden kann und welche Stellen zur Eintragung der Personenbindung in die Bürgerkarte ermächtigt sind, ist in der gemäß § 4 Abs. 5 zu erlassenden Verordnung des Bundeskanzlers zu regeln. In dieser Verordnung ist weiters zu regeln, inwieweit ein Kostenersatz für die Befassung der Stammzahlenregisterbehörde und der von ihm beauftragten Stellen für Zwecke des Identitätsnachweises im Zusammenhang mit der Eintragung im Ergänzungsregister sowie für Zwecke der Eintragung von Hinweisen auf die Stellvertretung zu leisten ist; die Gebietskörperschaften sind vom Kostenersatz jedenfalls auszunehmen.

(5) Zum bloßen Nachweis der Wiederholungsidentität kann der Betroffene auch ohne Nachweis der nach Abs. 3 geforderten Daten auf seinen Antrag von der Stammzahlenregisterbehörde mit einer Ersatz- Stammzahl ausgestattet werden. Diese ist aufgrund von Daten des Betroffenen zu bilden, die in ihrer Summe - wie etwa Name und Geburtsdatum und Geburtsort oder Seriennummer eines Zertifikats - eine hinreichende Unterscheidbarkeit erwarten lassen; sie muss als Ersatz-Stammzahl erkennbar sein.

(6) Die von der Stammzahlenregisterbehörde verwendeten mathematischen Verfahren zur Bildung der Stammzahlen (starkes Verschlüsselungsverfahren bei natürlichen Personen) und Ersatz-Stammzahlen (Hash-Wert über die Merkmale und zusätzlich starke Verschlüsselung bei natürlichen Personen) werden durch die Stammzahlenregisterbehörde festgelegt und - mit Ausnahme der verwendeten kryptographischen Schlüssel - im Internet veröffentlicht.

3.1. MAGDA-LENA Kommunikationsteilnehmer-ID

3.1.1 Authentifizierung

Die Authentizität jedes Teilnehmers im Gesundheitsdatennetz muss gesichert sein. Dazu muss sich ein Teilnehmer bei einer noch zu bestimmenden Stelle anmelden, worauf er eine Teilnehmerberechtigung für eine bestimmte Zeitspanne erhält. Nach deren Ablauf hat der Teilnehmer um eine Verlängerung anzusuchen bzw. sich im Falle eines Ausscheidens aktiv abzumelden. Durch diesen Prozess wird in der für die Verwaltung der Teilnehmerdaten zuständigen Stelle laufend die Teilnehmerliste aktualisiert und die Authentizität der Teilnehmer überprüft. Diese Stelle muss auch mit der entsprechenden Einrichtung, wie z.B. Standesvertretung (Ärztekammer, Apothekerkammer usw.), welche die richtige Identifikation der Teilnehmer gewährleisten kann, in Verbindung stehen. Für zahlreiche potentielle Teilnehmer von MAGDA-LENA bzw. Leistungsanbieter sind entsprechende Organisationen zu nominieren, die diese Teilnehmer identifizieren.

3.1.2 Registrierte Directories

Jeder Teilnehmer muss eindeutig identifizierbar sein, indem er innerhalb einer Organisation, der er zugeteilt ist, in einem registrierten Directory eindeutig

identifizierbar ist. Derzeit existieren mehrere solche Verzeichnisse. Die umfassendsten sind:

Ärzte: Vertragspartnernummer des Hauptverbandes, Ärztenummer der Ärzteliste der Ärztekammer

Apotheken: Apothekenbetriebsnummer

Krankenanstalten (ambulant/stationär): Krankenanstaltsnummer, wenn möglich ergänzt durch den 6- bzw.8-stelligen Funktionscode der jeweiligen Abteilung Versicherungen (Kostenträger): sozial/privat (unklar).

Weiters bestehen noch für weitere Leistungserbringer des Gesundheitswesens Vertragspartnernummern des Hauptverbandes. Bis zur Einführung eines neuen Identifikationssystems für die Leistungserbringer sind die derzeitigen ID´s zu verwenden. Auf eine mögliche Erweiterbarkeit ist zu achten. Darüber hinaus muss auch jeder Provider im MKK eindeutig identifizierbar sein. Ein entsprechendes Verzeichnis der MAGDA-LENA- Provider ist einzurichten. Ein systematischer Aufbau einer eindeutigen ID für alle Anbieter ist empfehlenswert. Um bei den verschiedenen Nummernsystemen eine Eindeutigkeit zu gewährleisten sind die Nummernsysteme analog zu Codesystemen (vgl. §2.5) beim für Gesundheit zuständigen Ministerium zu registrieren: Die Registriernummer ist der Teilnehmer- ID voranzustellen.

Die registrierten Directories stehen allen Teilnehmern zur Verfügung. Über die Qualität des jeweiligen Nummernformats und die Wartung der Directories findet man mehr im Anhang (9.1. und 9.2.).

3.1.3 Rollen der Teilnehmer

Neben der Authentizität der Teilnehmer muss auch ihre Rolle im Gesundheitsdatennetz definiert sein. Der Absender ist verantwortlich dafür, dass er seine Dokumente nur an berechtigte Teilnehmer adressiert. Daraus ergibt sich auch, dass der Absender den Typ des zu übermittelnden Dokuments festlegen muss. Die Rolle des Teilnehmers ist vom für Gesundheit zuständigen Bundesministerium festzulegen.

3.1.4 ID der Dokumente

Die verschickten Daten (Befunde etc.) müssen durch eine eindeutige Dokumenten-ID eindeutig identifizierbar sein.

Eine Empfehlung ist, einen mit dem Dokument zu verschlüsselnden Header zu verwenden. Dieser enthält zumindest die ID des Absenders, Zeitstempel, Aufenthaltsnummer und soll durch zusätzliche Merkmale ergänzt werden, so dass eine eindeutige Dokumentidentifikation ermöglicht wird.

3.2 Patienten-ID

3.2.1 Patienten-ID bei allgemeinem Datenaustausch

Bei der Übermittlung von Patientendaten muss immer eine eindeutige Patienten-ID mitgeschickt werden. Daneben werden weiterhin die herkömmlichen Patientendaten (Geburtsname, Familienname, Vorname, Geschlecht, Geburtsdatum, Nationalität) angegeben, können aber gegebenenfalls auch wegfallen (gemäß CEN ENV 12018).

Derzeit kommt für die Patienten-ID nur die Österreichische Sozialversicherungsnummer (SV-Nr) in Frage. Über mögliche und vielleicht auch notwendige Alternativen gibt der Anhang Auskunft (siehe 9.3.). Da die Einführung der Chipkarte im Gesundheitswesen die Änderung des jetzigen Status mit sich bringen könnte, sollte auf jeden Fall in allen Computersystemen die Aufwärtskompatibilität der Patienten-ID gewährleistet sein (Vorschlag: 32 Stellen in Anlehnung an den im Anhang angeführten ASTM Standard).

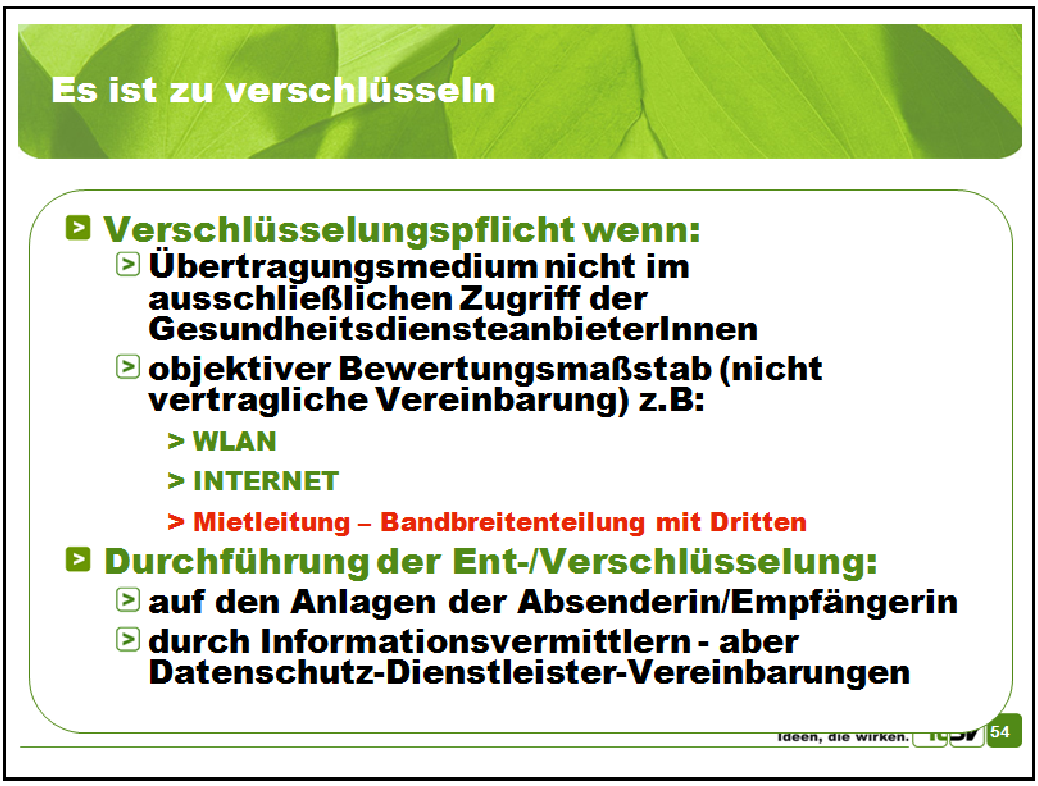
Bis zur Einführung einer neuen Patienten-ID ist die Sozialversicherungsnummer zu verwenden.

3.2.2 Patienten-ID bei bilateralem Datenaustausch

Bei einem rein bilateralen Datenaustausch (z.B.: Arzt – Labor – Arzt) werden die Daten – wenn möglich – in anonymisierter Form übermittelt. In diesem Fall wird statt der Patienten-ID ein intern eindeutiges Identifizierungsverfahren verwendet.

FÜR DETAILS SIEHE ANHANG:

III.a - Identifikationsvariable



Datensicherheit beim elektronischen Gesundheitsdatenaustausch:

Vertraulichkeit

§ 6. (1) Unbeschadet der für die Verwendung personenbezogener Daten nach dem DSG 2000 bestehenden Datensicherheitsvorschriften haben Gesundheitsdiensteanbieter beim elektronischen Gesundheitsdatenaustausch über ein Medium, das nicht ihrem ausschließlichen Zugriff unterliegt, von ihnen verschiedene Dritte von der Kenntnisnahme von Gesundheitsdaten durch inhaltliche Verschlüsselung der Daten auszuschließen. Zur inhaltlichen Verschlüsselung sind kryptographische Verfahren einzusetzen, die nach dem jeweiligen Stand der Technik mit wirtschaftlich vernünftigem Aufwand nicht kompromittiert werden können.

(2) Die Verschlüsselung hat auf den Anlagen des Absenders zu erfolgen, die Entschlüsselung auf den Anlagen des Empfängers der Gesundheitsdaten.

Zu § 6 des Entwurfs (Vertraulichkeit):

Die Sensibilität der Gesundheitsdaten gebietet, für ihren Transport mittels Medien, die eine Verletzung der Vertraulichkeit der Daten nicht ausschließen lassen, einen angemessenen Schutz durch Verwendung kryptographischer Verfahren und Methoden vorzusehen. Die dafür in Betracht kommenden qualitativen Mindestanforderungen sind in der Verordnung gemäß § 7 Abs. 5 festzulegen.

Nicht ausschließlich dem Zugriff von Gesundheitsdiensteanbietern unterliegt etwa die Übermittlung von Gesundheitsdaten per Funk (z.B. wireless LAN) sowie die Übermittlung von Gesundheitsdaten über vertraglich zugesicherte Leitungen von Fremdbetreibern, wenn diese Leitungen auch anderen Nutzern (z.B. bei Vereinbarungen über die Zurverfügungstellung von Bandbreiten) zur Verfügung gestellt werden (können).

Ausschlaggebend für die Beurteilung der Ausschließlichkeit des Zugriffs ist eine objektive Betrachtung anhand der jeweiligen technischen Ausprägungen des verwendeten Mediums und nicht die im Zuge der Bereitstellung der Leitung allenfalls erfolgten (vertraglichen) Zusicherungen des Verfügungsberechtigten der Leitung. Die Ausschließlichkeit ist jedenfalls dann nicht gegeben, wenn der Datentransport – wenn auch nur teilweise – über das Internet erfolgt. Als wirtschaftlich nicht

vernünftig ist ein Aufwand insbesondere dann anzusehen, wenn er auf Grund des dafür erforderlichen Aufwands (einzusetzende Ressourcen) von einem betriebswirtschaftlich zweckmäßig handelnden Subjekt zur Erzielung des beabsichtigten Erfolgs nicht getätigt würde.

Die Vertraulichkeit kann wirksam nur dann gewährleistet werden, wenn die Verschlüsselung vor Durchführung des Transports der Gesundheitsdaten durchgeführt wird. Abs. 2 schließt daher auch aus, dass Gesundheitsdaten über die in Abs. 1 bezeichneten Medien im Klartext an eine Dienstleisterin/einen Dienstleister, Netzbetreiber (Provider) oder an einen sonstigen, zwischen weitergebender/weitergebendem und empfangender/empfangendem Gesundheitsdiensteanbieterin/absendenden Gesundheitsdiensteanbieter eingeschaltete Informationsmittlerin/eingeschalteten Informationsmittler weitergegeben werden. Nicht ausgeschlossen ist dadurch, dass Informationsmittlerinnen/Informationsmittler Gesundheitsdaten zu Transportzwecken entschlüsseln oder umschlüsseln (Ent- und Neuverschlüsselung). Diesbezügliche Datenschutz- bzw. Datensicherheitsvereinbarungen müssen jedoch zwischen Auftraggeber und Dienstleister für den konkreten Einzelfall getroffen werden.

4. Datenschutz und Datensicherheit

Für jede Verwendung von Daten und insbesondere für sensible Daten „ . . . Ist sicherzustellen, dass die Daten vor zufälligen oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und dass die Daten Unbefugten nicht zugänglich sind „ § 14 Abs. 1 DSG 2000.

4.1 MAGDA-LENA II Sicherheitspolitik

Die im folgenden beschriebenen Elemente der Sicherheitspolitik gelten einerseits für die Teilnehmer des Gesamtsystems, die miteinander Daten austauschen, als **auch für die „Binnenstruktur“ der einzelnen Teilnehmer**.

Benutzerkontrolle (Authentifizierung)

Die Benutzerkontrolle muss sicherstellen, dass nur authentifizierte Benutzer elektronischen Zugriff auf Daten im System erhalten. Jeder Zugriff, ob berechtigt oder nicht berechtigt, ist zu protokollieren. In Hinblick auf versuchte oder vermutete Verletzungen des Datenschutzes ist das Protokoll in regelmäßigen Zeitintervallen oderauf Anforderung auszuwerten und es sind unberechtigte Zugriffe mit geeigneten Gegenmaßnahmen zu unterbinden. Die Authentifikation muss dem jeweiligen Stand der Technik entsprechen. Bei hohem Schutzbedarf ist eine zusätzliche, mindestens nach Ablauf eines in der Policy vorgegebenen Zeitintervalls durchzuführende Authentifikation gegenüber dem Kommunikationspartner erforderlich.

Zugriffskontrolle (Autorisierung)

Auch authentifizierte Benutzer eines Systems dürfen elektronisch nur auf solche sensiblen Daten zugreifen bzw. Zugriffsrechte erhalten, welche für die berufliche Tätigkeit bzw. für die Behandlung einer Person notwendig sind. Die Begründung, welche sich implizit aus dem Kontext ergeben kann (z.B. Patient in Behandlung), ist nachweislich elektronisch zu dokumentieren. (Beispiel: ein authentifizierter niedergelassener Arzt, fordert von einem Krankenhaus die Krankengeschichte für einen Patienten x an, mit der Begründung, dass x bei ihm in Behandlung sei. Das Krankenhaus kann darauf vertrauen, dass der Arzt nicht unrechtmäßig für einen Dritten Daten anfordert; es muss aber Verbote des Patienten beachten und darf nicht irrelevante Daten, wie z.B. Relig.-Bekenntnis, Abrechnungsdaten, übermitteln.) Sind sensible Daten für die Behandlung eines Patienten unbedingt notwendig, kann auch der nicht im System autorisierte Arzt im Rahmen der technischen und gesetzlichen Möglichkeiten auf diese Daten zugreifen. Das heißt, ein Arzt, der authentifiziert (dem System bekannt) ist, aber normalerweise auf die Daten nicht zugreifen dürfte (nicht autorisiert ist) – z.B. weil er nach der Datenlage im System noch nicht behandelnder Arzt ist (unerwarteter Notfall). Diese Zugriffe sind gesondert zu protokollieren und vom System zu verifizieren (ob z.B. der Patient nach dem Zugriff als Patient an dieser Stelle behandelt wurde) und die sicherheitsrelevanten Informationen einer Kontrollinstanz (z.B. dem Leiter der Organisationseinheit) zu übermitteln.

Alle Protokolle sind periodisch oder im Anlassfall zu überprüfen, Zugriffsverletzungen und versuchte Zugriffe auf sensible Daten sind mit geeigneten Mitteln zu unterbinden. Die hier festgelegten Bestimmungen der Zugriffskontrolle treffen nur auf die mit der Übertragung von MAGDA-LENA relevanten Daten verbundenen Zugriffe auf Daten zu. Die lokale und interne Organisation der Kommunikationspartner wird durch MAGDA-LENA II nicht angesprochen.

Übermittlungskontrolle

Jede elektronische Übermittlung von sensiblen Daten ist vertraulich mittels hinreichend starker Verschlüsselung (gemäß Anhang IV.a) durchzuführen. Die Verschlüsselung hat End to End zu geschehen, ein Offenlegen des Klartextes auf der Übertragung etwa zum Zwecke der Umschlüsselung ist nicht vorzusehen. Weiters ist die Datenintegrität sowie der Datenursprung der übermittelten Informationen bzw. die Identität des Senders durch anerkannte und geeignete Methoden (z.B. elektronische Signatur) sicherzustellen. Jede elektronische Übermittlung von sensiblen Daten ist durch eine Rückmeldung des Kommunikationspartners zu bestätigen. Bei der Anwendung elektronischer Signaturen sind die gesetzlichen Bestimmungen des Signaturgesetzes und der Verordnung zu beachten.

Die im Planungsstadium befindliche Sozialversicherungskartensystem ist als Schlüsselkarte geplant und diese Technologie kann die Anforderungen an die Übermittlungskontrolle im Bereich der elektronischen Signatur und gegebenenfalls auch der Verschlüsselung erfüllen.

Organisationskontrolle

Die regelmäßige Kontrolle der Organisationsstrukturen ist eine wichtige Voraussetzung, um die gesetzlichen Rahmenbedingungen zum Schutz der betroffenen Personen und Dienstleister einhalten zu können. Schwachstellen im System können damit identifiziert und innerhalb festgelegter Zeiträume beseitigt werden. In der Sicherheitspolitik sind sowohl die Zeitintervalle für eine regelmäßige Überprüfung als auch die Maßnahmen, welche bei einer Verletzung der Sicherheitspolitik zu ergreifen sind, festzulegen. Mangelnde Organisation und Qualität stellen ein Sicherheitsrisiko für jedes System dar.

Vertrauenswürdige Betriebsumgebung

Die vertrauenswürdige Betriebsumgebung muss den Schutz im Betrieb des gesamten Netzes gewährleisten. Dabei sind auch alle Aspekte der übrigen Kommunikation (z.B. Internetanbindung) mit einzubeziehen. Der Provider von Kommunikationselementen und Kommunikationsdiensten ist dafür verantwortlich, dass unter Einhaltung der von Ihm erteilten und schriftlich aufliegenden Belehrung eine Verletzung des Datenschutzes nicht erfolgen kann. Tritt eine Organisationseinheit selbst und ohne einen Provider in Anspruch zu nehmen auf, dann trägt sie auch diese Verantwortung des vertrauenswürdigen Betriebes. Auch in diesem Fall muss die Betriebspolicy, die der Belehrung des Providers gleichkommt offengelegt sein.

Ein Netzwerkbetreiber ist zudem für die Verfügbarkeit des Netzes und für die Zustellungsnachweise verantwortlich. Jedenfalls liegt es in der Verantwortung des Providers einer MAGDA-LENA konformen Lösung, dass eine solche mit anderen MAGDA-LENA konformen Lösungen auf der Kommunikationsebene verträglich ist.

FÜR DETAILS SIEHE ANHÄNGE

IV.a: Anforderung an Verfahren und Mechanismen (normativ)

IV.b: Sicherheitsmaßnahmen und Sicherheitsempfehlungen (normativ gemäß Konformitätserklärung)

Vertrag zwischen Netzbetreiber und Kunden

• Die Übereinkunft hinsichtlich der Nutzung der Dienste eines Netzbetreibers durch den Kunden ist in jedem Fall vertraglich zu regeln, wobei insbesondere auf §11 DSG 2000 zu verweisen ist. Wie in MAGDA-LENA 1.0 (Punkt 5.5) bereits angeführt, sind Richtlinien wie

• Verfügbarkeit

• Security

• HotLine / Help Desk

• Reaktionszeiten

• Wartung

• Accountingfunktionen zu Verrechnungszwecken

• Gebühren, etc.

vertraglich festzulegen.

8. Anhang IV.b: Sicherheitsmaßnahmen und Sicherheitsempfehlungen (normativ gemäß Konformitätserklärung)

8.1 Sicherheitsmaßnahmen

Um die in Kapitel 4 beschriebene Sicherheitspolitik auch technisch realisieren zu können, sind folgende Sicherheitsmaßnahmen notwendig. Diese Maßnahmen können je nach Größe der Organisationseinheit durchaus unterschiedlich sein. Als Minimalforderungen müssen jedoch entsprechende Methoden für Authentifikation, Zugriffskontrolle, Vertraulichkeit, Datenintegrität und Ursprungsnachweis implementiert sein. Die dazu notwendigen Mechanismen und Implementierungen des Keymanagements, der Sicherheitstoken, der Passwortsysteme, der Verschlüsselung und der elektronischen Signatur müssen geeignet und soweit im Anhang zu MAGDALENA II genauer spezifiziert, diesem entsprechend umgesetzt werden.

Authentifikation und Zugriffskontrolle

Bevorzugt zur Authentifikation von Personen oder Systemen sind Verfahren einzusetzen, welche eine Zertifizierungsstruktur mit eingebundenen Sicherheitstoken, die auch in geeigneter Weise vor fahrlässiger Benutzung schützen können (z.B. Smartcards) unterstützen. Integrierte und ortsbezogene Systeme (z.B. personalisierter Sicherheitstoken zum Raumzutritt und zur EDV-Authentifikation) können die Anforderungen der Benutzerfreundlichkeit und der Sicherheit gleichzeitig erfüllen. Für die EDV-Authentifikation werden asymmetrische Methoden, die gleiche Techniken wie die elektronische Signatur nutzen bzw. zero-knowledge Methoden als angemessen empfohlen. Herkömmliche Passworte sind nur mehr in jenen Fällen, wo dies aus technischen oder organisatorischen Gründen derzeit nicht möglich ist und konventionelle Passwortsysteme eingesetzt werden, müssen diese einer vorgegebenen Policy (Länge und Zeichenwahl) entsprechen. Die Übergangsphase darf längstens 2 Jahre betragen. Alle eingesetzten Mechanismen sind mit einem automatischen Ablaufdatum zu versehen. Die Authentifikation muss im System effizient umgesetzt sein und es müssen Umgehungsmechanismen auch für Insider ausgeschlossen sein.

Vertraulichkeit

Geeignete Verschlüsselung von sensiblen Daten mit hinreichender Schlüssellänge und vertrauenswürdigem Keymanagement garantiert, dass diese Informationen vertraulich zwischen den Kommunikationspartnern übermittelt werden können. Die Methoden sind für gleichzeitige und zeitversetzte Kommunikation zwar unterschiedlich, doch in den entsprechenden Standards, die im Anhang zu MAGDA-LENA II aufgelistet sind, verfügbar. Die Verschlüsselung zur Vertraulichkeit ist für die Übertragung und für die allfällige Speicherung jedenfalls unterschiedlich zu wählen. Die Verschlüsselung der gespeicherten Daten ist nicht Gegenstand von MAGDA-LENA II. Der Sessionkey für eine vertrauliche Kommunikation ist nur während des betreffenden Kommunikationsprozesses relevant. Keys für unterschiedliche Sessions sind hinreichend unterschiedlich zu wählen, damit dadurch keine Sicherheitslücke entsteht.

Eine Hinterlegung bzw. Langzeitspeicherung der Schlüssel der Übertragung ist nicht vorzusehen. Die Verarbeitung der Schlüssel muss so gestaltet sein, dass diese weder aus Backups, noch aus Swapspaceanalysen oder sonstigen temporären Datenrelikten des Systems ermittelt werden können. Weiters werden die entsprechenden Rahmenbedingungen (siehe Anforderungen an Keymanagement)

eingehalten werden, welche für den sicheren Schlüsselaustausch als auch für die sichere Generierung dieser Schlüssel notwendig sind. In die Erzeugung des Sessionkeys sind Verfahren der Authentifizierung einzubinden, die hinreichend kryptographische Stärke besitzen. Die konkreten Anforderungen werden im Anhang zu MAGDA-LENA näher festgelegt.

Datenintegrität

Um die Unverfälschtheit der in elektronischen Netzen übermittelten Daten zu garantieren sind Methoden notwendig, welche die Datenintegrität der übermittelten Informationen anzeigen. Als einfachste Methoden sind Prüfsummen bzw. Hash - Algorithmen zu nennen. Implizit wird die Datenintegrität von übermittelten Informationen auch gewährleistet, wenn der Ursprungsnachweis mittels elektronischer Signatur erfolgt. Die Rahmenbedingungen hierfür sind im Signaturgesetz und der Signaturverordnung festgelegt. Bei sensiblen Anwendungsteilen, die eine zusätzliche Kontrolle der Integrität der Informationen durch Personen nicht ermöglichen oder bei welchen aus dem Prozedere heraus eine solche in der Regel entfällt, sind als Methoden der Datenintegrität jene Verfahren einzusetzen, die den sicheren elektronischen Signaturen nach SigG bzw. SigVO entsprechen. Dies muss jedenfalls bei allen vollautomatisierten Vorgängen, die im Bereich der ärztlichen Tätigkeit eingesetzt werden, der Fall sein.

Ursprungsnachweis

Der Ursprungsnachweis von Daten kann durch den Einsatz asymmetrischer kryptographischer Verfahren gewährleistet werden. Hierfür werden die Elemente, Methoden und Verfahren der elektronischen Signatur (inklusive der notwendigen Rahmenbedingungen) empfohlen. Dies gilt auch dann, wenn diese Methoden automatisiert ausgelöst werden und daher keine Signaturen im Sinne des SigG sind. Die entsprechenden technischen und organisatorischen Grundlagen für die elektronische Signatur sind im Signaturgesetz und der Signaturverordnung festgelegt. Ein Ursprungsnachweis nach den Technologien der sicheren elektronischen Signaturen muss jedenfalls bei allen vollautomatisierten Vorgängen, die im Bereich der ärztlichen Tätigkeit eingesetzt werden, erfolgen.

8.2 Empfehlungen

Sind die Methoden für Authentifikation, Vertraulichkeit, Datenintegrität und Ursprungsnachweis verbindlich zu implementieren, sind die nachstehenden Sicherheitsmaßnahmen nur von größeren Organisationseinheiten zu implementieren. Die nachstehenden Maßnahmen sollen sicherstellen, dass sicherheitsrelevante Komponenten schwer manipuliert bzw. umgangen werden können. Neben den sicherheitstechnischen Überlegungen sind die Realisierungen der nachstehenden Sicherheitsdienste auch von wirtschaftlichen Überlegungen abhängig. Für Betreiber von Netzwerken bzw. Provider ist zusätzlich zu den Punkten a. - c. Punkt d. Verfügbarkeit des Systems anzuwenden.

Zutrittskontrolle

Der Zugang zu den eigenen Netzwerken von außen (einkommender Datenverkehr insbesondere auch von offenen Netzen) soll über entsprechende Sicherheitskomponenten (z.B. Firewalls, abgesicherte RAS Server) erfolgen. Diese Komponenten sind vertrauenswürdig aufzubauen und zu betreiben. Der Zutritt zu diesen Komponenten darf nur einem eingeschränkten und in der Sicherheitspolicy festgelegten Personenkreis möglich sein. Jeder Zutritt in diesem Bereich ist zu protokollieren und in geeigneter Weise periodisch oder bei Bedarf auszuwerten. Ausreichende Mechanismen sind zu installieren, um den Missbrauch möglichst verhindern zu können.

Audit Trail

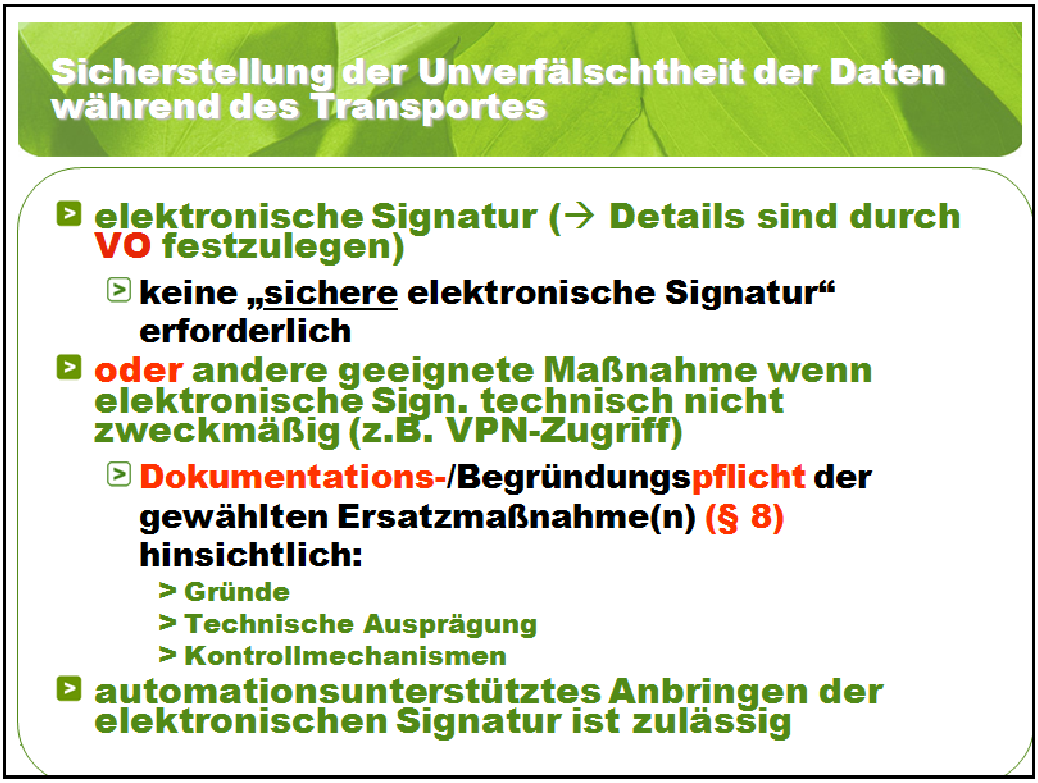
Große Organisationseinheiten bzw. Dienstleister sind verpflichtet, die gesamte anfallende Protokollierung regelmäßig oder bei Bedarf auszuwerten. Ebenso sind auch nicht erfolgreiche Attacken von außen auf das System zu protokollieren und mit Gegenmaßnahmen zu beantworten. Mittels Audit Trails sollen alle Maßnahmen auf ihre Effizienz überprüft werden. Protokolle sind elektronisch und in gesicherter Form (zeitgestempelt und elektronisch signiert) aufzubewahren.

Wartung

Alle Maßnahmen, welche zur Instandhaltung eines Systems eingesetzt werden können, bedürfen zusätzlicher Regelungen. Hierzu zählen die Wartung vor Ort, die Fernwartung sowie das Software Update. Eine Wartung vor Ort soll nur in Gegenwart eines Vertreters des Auftraggebers erfolgen, Fernwartung soll auf nicht sicherheitsrelevante Komponenten des Systems beschränkt werden. Das Update von Software Modulen bzw. das Upgrade von Hardware Komponenten soll ebenfalls nach bestimmten Richtlinien erfolgen. Wird Fernwartung ermöglicht, so ist eine klare Policy festzulegen. Anhang „Fernwartung“ zu MAGDA-LENA II gibt dazu ein Beispiel an.

Verfügbarkeit des Systems

Der Betreiber eines Netzwerkes bzw. Provider hat für die gesicherte Zustellung innerhalb eines definierten Zeitraums zu sorgen. Das Kommunikationssystem hat entsprechende Informationen (z.B. Identifikation, Zeitpunkt der Kommunikation) am System zu protokollieren. Diese Daten sind entsprechend dem Telekommunikationsgesetz aufzubewahren bzw. bei Bedarf zu überprüfen. Die genannten organisatorischen und technischen Maßnahmen können durch weitere Sicherheitsmaßnahmen ergänzt werden. Alle unter 4.2 Organisatorischen Rahmenbedingungen und im Anhang aufgezählten Maßnahmen sind Minimalanforderungen für ein sicheres Kommunikationssystem. In bestimmten Bereichen können die genannten Anforderungen nach Durchführung einer Risikoanalyse während eines beschränkten Übergangszeitraumes (längstens jedoch für 2 Jahre) aufgeschoben werden. Die Sicherheit des Systems muss jedoch durch geeignete technische und organisatorische Maßnahmen gewährleistet sein. Alle genannten Maßnahmen können durch andere Methoden ersetzt werden, soweit diese zumindest gleichwertige Sicherheit gewährleisten. Die einzusetzenden Methoden sind in Anhang D beschrieben.



Datensicherheit beim elektronischen Gesundheitsdatenaustausch:

Integrität

§ 7. (1) Die Integrität (Unverfälschtheit) von weiterzugebenden Gesundheitsdaten ist durch Verwendung elektronischer Signaturen, die den gemäß Abs. 5 festgelegten Mindestanforderungen entsprechen müssen, nachzuweisen bzw. zu prüfen.
(2) Die Verwendung elektronischer Signaturen gemäß Abs. 1 kann unterbleiben, wenn der

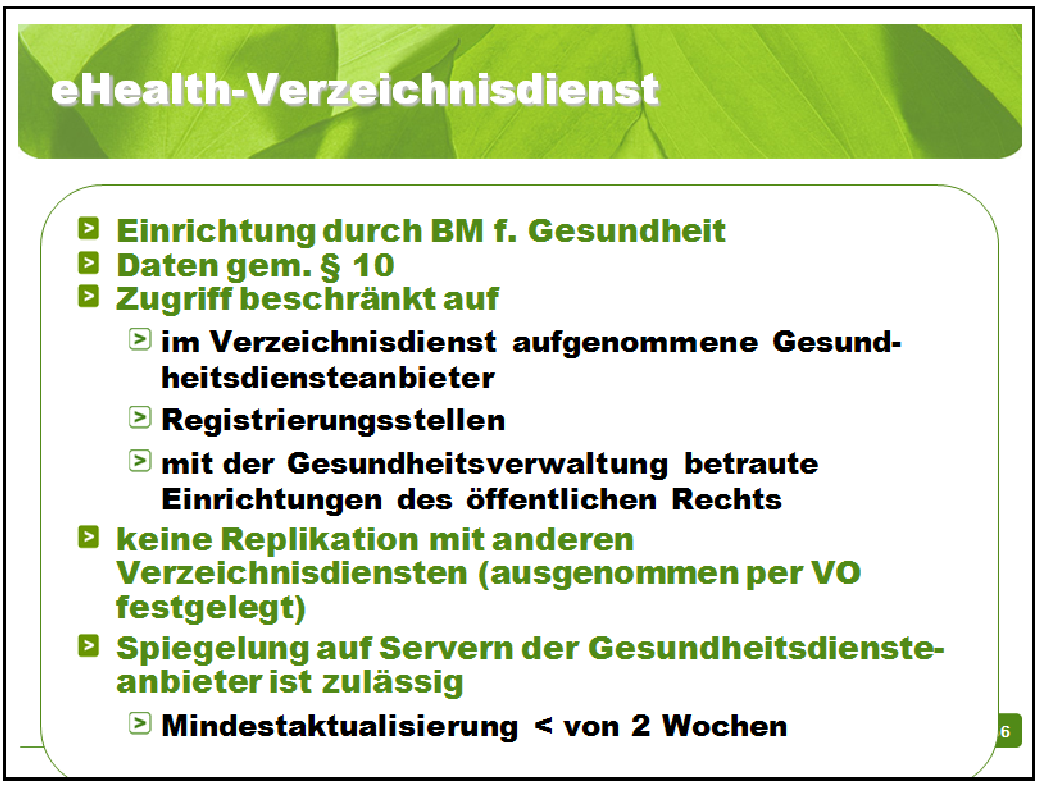
elektronische Gesundheitsdatenaustausch ausschließlich programmgesteuert oder durch direkte Bedienung einer Datenanwendung aus der Entfernung erfolgt. Gegebenenfalls haben Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter, die den programmgesteuerten Gesundheitsdatenaustausch durchführen sowie Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter, die Rechte zur Bedienung ihrer Datenanwendung aus der Entfernung einräumen, die Gründe und die von ihnen getroffenen Maßnahmen, die ein vergleichbares Datensicherheitsniveau gewährleisten müssen sowie die Mechanismen zur Sicherstellung und Kontrolle ihrer Einhaltung zu dokumentieren.
(3) Das Anbringen elektronischer Signaturen kann automationsunterstützt erfolgen.
(4) Im Fall einer fehlgeschlagenen Signaturprüfung dürfen die empfangenen Gesundheitsdaten nicht verwendet werden.
(5) Die qualitativen Mindestanforderungen für Zertifikate gemäß den §§ 4 und 5, für die Verschlüsselung gemäß § 5 sowie für elektronische Signaturen sind von der Bundesministerin für Gesundheit und Frauen/vom Bundesminister für Gesundheit und Frauen mit Verordnung festzulegen.

Zu § 7 des Entwurfs (Integrität):

Die Überprüfbarkeit der Integrität (Unverfälschtheit) der elektronisch ausgetauschten Gesundheitsdaten ist durch die elektronische Signierung der weiterzugebenden Gesundheitsdaten sicher zu stellen. Die Empfängerin/Der Empfänger der Gesundheitsdaten hat sich durch Signaturprüfung zu vergewissern, dass die Gesundheitsdaten während des elektronischen Transports nicht verändert wurden.

Die Verwendung elektronischer Signaturen kann bei bestimmten Arten des elektronischen Gesundheitsdatenaustausches etwa aus technischen Gründen nicht zweckmäßig oder notwendig sein (z.B. bei Datenzugriffen oder – weitergaben über virtual private networks). Abs. 2 lässt daher abweichende Lösungen zu, für die die Gründe, die technische Ausprägung und die Kontrollmechanismen zu dokumentieren sind und die der Auskunftspflicht gemäß § 8 Abs. 2 unterliegen.

Die Anbringung elektronischer Signaturen kann automationsunterstützt erfolgen, demnach müssen die elektronischen Signaturen im Sinne dieses Bundesgesetzes nicht die Anforderungen einer sicheren elektronischen Signatur gemäß Signaturgesetz erfüllen. Bestehen auf Grund der Signaturprüfung Zweifel an der Integrität der übertragenen Daten (Fehlschlagen der Signaturprüfung), dürfen die empfangenen Gesundheitsdaten nicht verwendet werden. Auf die speziell auf Notfälle abstellende Regelung in § 17 Abs. 2 wird hingewiesen.



Informationsmanagement

eHealth-Verzeichnisdienst

§ 9. (1) Die Bundesministerin für Gesundheit und Frauen/Der Bundesminister für Gesundheit und Frauen kann zur Förderung des elektronischen Gesundheitsdatenaustausches, zur Verbesserung des Zugangs zu Informationen über gesundheitsbezogene Dienste sowie zu Planungs- und Berichtszwecken einen eHealth-Verzeichnisdienst einrichten.
(2) Der eHealth-Verzeichnisdienst hat insbesondere für die in § 10 bezeichneten Daten eine nach unterschiedlichen Kriterien gestaltete Suchfunktion, die die Auffindbarkeit von Informationen über Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern gewährleistet, zu enthalten.
(3) Der Zugriff auf die im eHealth-Verzeichnisdienst enthaltenen Daten ist auf die in den eHealth-Verzeichnisdienst aufgenommenen Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter, die Registrierungsstellen sowie mit der Gesundheitsverwaltung betrauten Einrichtungen des öffentlichen Rechts einzuschränken. Bei der technischen Ausgestaltung der Suchfunktion sind darüber hinaus wirksame Mechanismen zur Verhinderung des Missbrauchs von Daten zu implementieren.
(4) Der eHealth-Verzeichnisdienst nimmt am Replikationsmechanismus mit anderen Verzeichnisdiensten nicht teil. Die Bundesministerin für Gesundheit und Frauen/Der Bundesminister für Gesundheit und Frauen kann jedoch mit Verordnung, die insbesondere den Zeitpunkt für den Beginn der Replikation sowie die dafür erforderlichen technischen Umstände zu enthalten hat, eine solche Teilnahme vorsehen.
(5) Im eHealth-Verzeichnisdienst eingetragene Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter sowie Registrierungsstellen sind berechtigt, die im eHealth-Verzeichnisdienst gespeicherten Daten auf ihren Anlagen zu speichern (Spiegelung bzw. Replikation). Diese Daten dürfen ausschließlich zum Zweck des elektronischen Gesundheitsdatenaustausches und zur Sicherstellung der Aktualität und Richtigkeit des eHealth-Verzeichnisdienstes verwendet werden und sind regelmäßig, längstens jedoch innerhalb von zwei Wochen, zu aktualisieren.
(6) Die Bundesministerin für Gesundheit und Frauen/Der Bundesminister für Gesundheit und Frauen kann mit Verordnung nähere Bestimmungen über die in den eHealth-Verzeichnisdienst aufzunehmenden Daten, das Registrierungsverfahren sowie über die Führung des eHealth-Verzeichnisdienstes erlassen.

Zu § 9 des Entwurfs (eHealth-Verzeichnisdienst):

Auf Grund der Fragmentierung des Gesundheitswesens und damit auch der Leistungserstellung sind bundesweit keine komprimierten Informationsgrundlagen über Art und Anzahl der am elektronischen Gesundheitsdatenaustausch teilnehmenden Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter verfügbar. Der eHealth-Verzeichnisdienst dient einerseits der statistischen Erfassung und Ausweisung von Personen und Einrichtungen, die am elektronischen Gesundheitsdatenaustausch teilnehmen, andererseits werden in ihm die Zuordnungen von Rollen zu Gesundheitsdiensteanbietern ausgewiesen. Durch Vorkehrungen für eine hohe Datenqualität und –aktualität wird nicht nur das notwendige Vertrauen hinsichtlich der rollenbezogenen Identität der Kommunikationspartnerin/des Kommunikationspartners geschaffen, sondern können die organisatorischen und technischen Maßnahmen zur Gewährleistung von Datensicherheit auf ein ökonomisch zweckmäßiges Ausmaß beschränkt werden. Der weitere Nutzeffekt des Verzeichnisdienstes ist die Verwendung der Daten für Planungs- und Berichtszwecke.

Der Zugriff auf den Verzeichnisdienst wird zunächst auf Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter, Registrierungsstellen und die Einrichtungen der öffentlichen Gesundheitsverwaltung eingeschränkt. Der Verzeichnisdienst nimmt daher am Replikationsmechanismus mit vergleichbaren Verzeichnissen nicht teil; diese Möglichkeit kann allenfalls zu einem späteren Zeitpunkt und nach Vorliegen entsprechender Erfahrungen mit Verordnung eröffnet werden. Demgegenüber wird es den in Abs. 5 genannten Stellen gestattet, die Daten auf ihre Anlagen zu replizieren. Damit wird eine Vereinfachung der Prüfungsvorgänge vor Ort und die Reduzierung der Verfügbarkeit des Verzeichnisdienstes angestrebt.

Mit Verordnung (Abs. 6) der Bundesministerin für Gesundheit und Frauen/des Bundesministers für Gesundheit und Frauen wird eine Präzisierung der in den Verzeichnisdienst aufzunehmenden Daten vorgenommen bzw. werden nähere Bestimmungen über die Führung des Verzeichnisdienstes erlassen.

Inhalte

§ 10. (1) In den eHealth-Verzeichnisdienst sind insbesondere folgende Daten aufzunehmen:
1. Name oder Bezeichnung der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters,
2. Angaben zur postalischen und elektronischen Erreichbarkeit,
3. die eindeutige Kennung (OID) und den symbolischen Bezeichner,
4. die Rolle(n) der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters,
5. Angaben zur geografischen Lokalisierung der Gesundheitsdiensteanbieterin/des Gesundheitsdiensteanbieters,
6. die zur Verschlüsselung von Gesundheitsdaten erforderlichen Angaben,
7. die Bezeichnung jener Stelle(n), die die Zuordnung der Rolle(n) zum Gesundheitsdiensteanbieter bestätigt hat (haben),
8. das Datum der Registrierung und der letzten Berichtigung sowie die Bezeichnung der Registrierungsstelle, die diese Verzeichniseintragungen durchgeführt hat.
(2) Die eindeutige Kennung (Abs. 1 Z 3) ist anhand der ÖNORM A 2642, "Kommunikation offener Systeme, Verfahren zur Registrierung von Informationsobjekten in Österreich" vom 1. März 1997, aus der Kennung (OID) des Bundesministeriums für Gesundheit und Frauen abzuleiten.
(3) Ergänzend zu den gemäß Abs. 1 bereits aufgenommenen Daten können organisatorischen Untergliederungen einer Gesundheitsdiensteanbieterin/eines Gesundheitsdiensteanbieters in den eHealth-Verzeichnisdienst aufgenommen werden, wenn diese am elektronischen Gesundheitsdatenaustausch teilnehmen und die/der organisatorisch übergeordnete Gesundheitsdiensteanbieterin/Gesundheitsdiensteanbieter zustimmt. Diesbezüglich sind in den eHealth-Verzeichnisdienst die Angaben gemäß Abs. 1 und 2 mit der Maßgabe aufzunehmen, dass die eindeutige Kennung der organisatorischen Untergliederung aus der Kennung der/des organisatorisch übergeordneten Gesundheitsdiensteanbieterin/Gesundheitsdiensteanbieters abzuleiten ist.
(4) In den Verzeichnisdienst können darüber hinaus zusätzliche Daten über die betreffende Gesundheitsdiensteanbieterin/den betreffenden Gesundheitsdiensteanbieter oder die von ihr/ihm angebotenen gesundheitsbezogenen elektronischen Dienste aufgenommen werden. Diese Zusatzinformationen müssen sich auf die nähere Beschreibung ihres/seines rollenspezifischen Dienstleistungsangebots beziehen oder Informationen darstellen, für das Auffinden oder die Inanspruchnahme eines elektronischen Dienstes erforderlich sind.

Zu § 10 des Entwurfs (Inhalte des Verzeichnisdienstes):

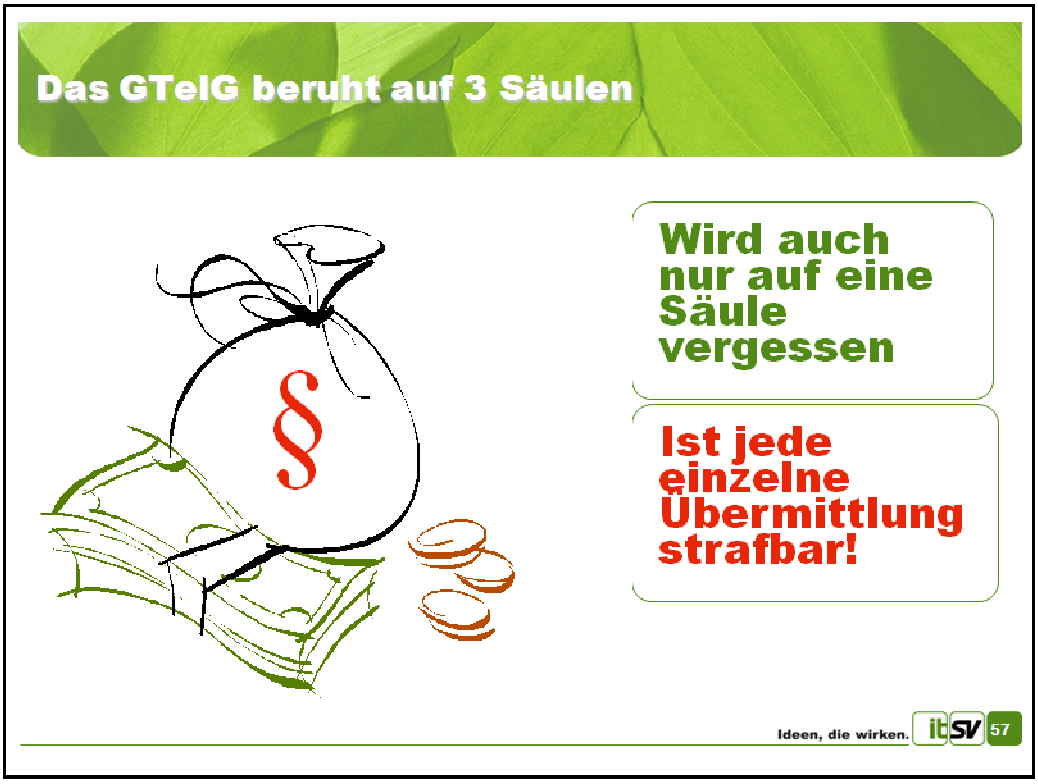
In den Verzeichnisdienst jedenfalls aufzunehmen sind die in Abs. 1 bezeichneten Daten. Dem Förderungsaspekt der elektronischen Kommunikation von Gesundheitsdaten entsprechend, können jedoch zusätzliche Angaben, etwa über die von der Gesundheitsdiensteanbieterin/vom Gesundheitsdiensteanbieter angebotenen elektronischen Dienste (z.B. web services), aufgenommen werden (Abs. 4).

Zur Aufnahme des in Abs. 1 Z 3 vorgesehenen Identifikationsmerkmals für Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter ist festzuhalten, dass es derzeit kein Österreich weit akzeptiertes Identifikationsmerkmal für Gesundheitsdienstanbieter gibt, sondern verschiedene Systeme (Krankenanstaltennummer, Vertragspartnernummer, Apothekenbetriebsnummer u.dgl.) zur Anwendung gelangen, die von den jeweils vergebenden Institutionen verwaltet werden. Für manche Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter bestehen derzeit keine vergleichbaren Kennzeichen. Für eine systematische Erfassung und Auffindbarkeit von Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern spielt jedoch eine eindeutige Identifikation eine entscheidende Rolle. Ihr Fehlen könnte insbesondere bei der Erstellung und Wartung von Datenbanksystemen, die Österreich weite Daten enthalten, zu erheblichen Problemen führen. Auf die vordringliche Inangriffnahme dieser Problematik wurde bereits in den Magdalena-Empfehlungen hingewiesen.

Für den Aufbau des Identifikationskennzeichens bieten sich die veröffentlichten Standards für die Registrierung von Personen, Organisationen bzw. Informationsobjekten als Orientierung an. Dies sind insbesondere die diesbezüglichen ISO/IEC-Standards und die in Umsetzung dieser Standards verabschiedete ÖNORM A 2642 (Abs. 2). Dieses System gewährleistet eine weltweit eindeutige Identifizierung von Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern.

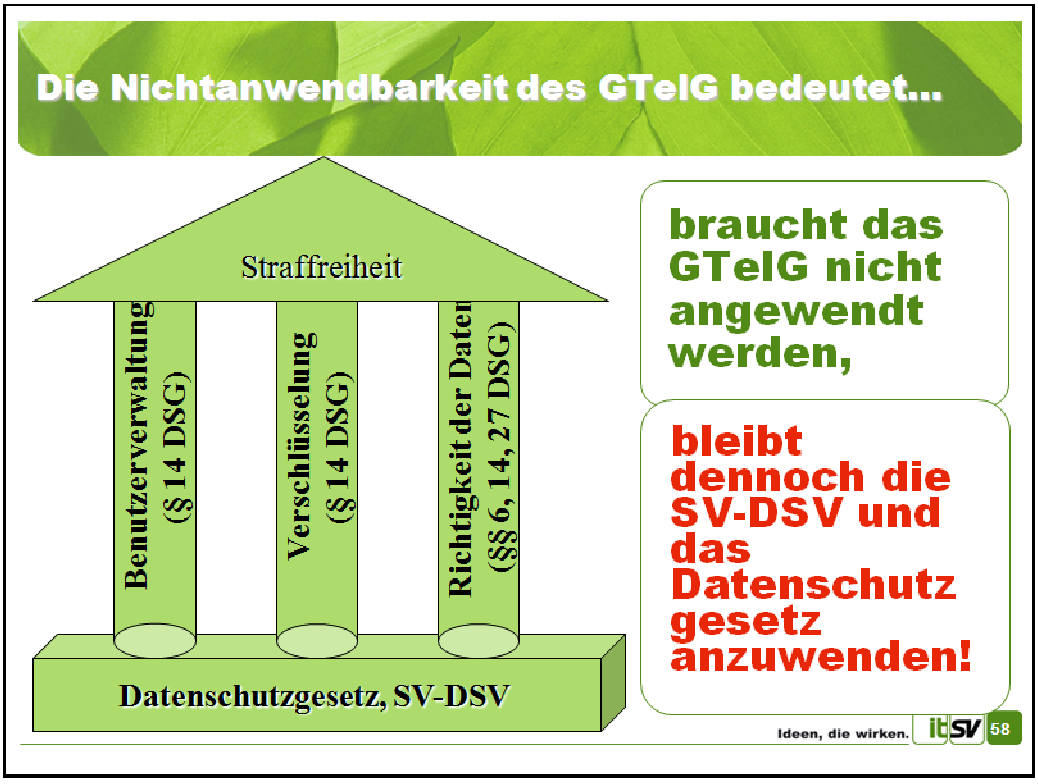
Zur Rolle (Abs. 1 Z 4) ist festzuhalten, dass eine Gesundheitsdiensteanbieterin/ein Gesundheitsdiensteanbieter mehrere Rollen einnehmen kann (z.B. Psychotherapeut/Psychotherapeutin – niedergelassene Ärztin/niedergelassener Arzt). Im Verzeichnisdienst müssen alle Rollen, einschließlich der sie bestätigenden (unterschiedlichen) Autoritäten, aufgenommen werden können.

Die geografische Lokalisierung von Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern (Abs. 1 Z 5) bezweckt, den Verzeichnisdienst nach regionalen Gesichtspunkten für Planungs- und Berichtszwecke auswerten zu können (z.B. zur Feststellung der elektronischen Versorgungsdichte). Dafür kommen der ISO-Standard 3166 oder ähnliche Standards in Betracht. Bei Bedarf nach präziseren regionalen Angaben wäre die dafür erforderlichen Detaillierungen in der Verordnung gemäß § 9 Abs. 6 vorzunehmen.



Achtung:

Nur weil ich meine Daten verschlüssele heißt dass nicht, dass ich von der Haftung des Gesundheitstelekommunikationsgesetzes befreit bin. Ich muss alle Bestimmungen des GTelG erfüllen, damit ich straffrei bleibe. Das GTelG schreibt die Einhaltung aller 3 Säulen vor!!



Es ist immer zu beachten, dass die Nichtanwendbarkeit des Gesundheitstelekommunikationsgesetzes nicht bedeutet, dass ich die Identität des Zugriffsberechtigten nicht zu prüfen habe, dies schreibt bereits das Datenschutzgesetz und die Datenschutzverordnung für die Sozialversicherung vor. Eben dasselbe gilt für eine etwaige Verschlüsselungspflicht und die Sicherstellung, dass die nur richtige Daten verarbeitet und übermittelt werden.

Das Gesundheitstelematikgesetz schreibt nur strengere (technische) Vorgehensweisen vor, wie ich diese Ziele umzusetzen habe.

Hier einige Fragen zu diesem Thema.

* Sind SV Daten, Gesundheitsdaten?

Ja, alle Daten der SV (so sie einen "Patienten (gesunde wie kranke)"-Bezug haben und desweiteren nicht rein statistischer Natur (d.h. anonym oder zumindest indirekt personenbezogen) sind, sind als Gesundheitsdaten iSd GTelG anzusehen:

§ 1 : Gesundheitsdaten sind direkt personenbezogene Daten gemäß § 4 Z 1 DSG 2000 über die physische oder psychische Befindlichkeit eines Menschen, einschließlich der im Zusammenhang mit der Erhebung der Ursachen für diese Befindlichkeit sowie der medizinischen Vorsorge oder Versorgung, der Pflege, der Verrechnung von Gesundheitsdienstleistungen oder der Versicherung von Gesundheitsrisken erhobenen Daten. Dazu gehören insbesondere Daten die

a) die geistige Verfassung,

b) die Struktur, die Funktion oder den Zustand des Körpers oder Teile des Körpers,

c) die gesundheitsrelevanten Lebensgewohnheiten oder Umwelteinflüsse,

d) die verordneten oder bezogenen Arzneimittel, Heilbehelfe oder Hilfsmittel,

e) die Diagnose-, Therapie- oder Pflegemethoden oder

f) die Art, die Anzahl, die Dauer oder die Kosten von Gesundheitsdienstleistungen oder gesundheitsbezogene Versicherungsdienstleistungen betreffen.

* Was sind eigene Netze?

o MPLS: nein

o CNA-Netz: nein

Eigene Netze liegen nur dann vor, wenn ausschließlich eine Zugriffsmöglichkeit für den jeweiligen Gesundheitsdiensteanbieter vorliegt (auch bei Außenstellen zu beachten). Nicht ausschließlich dem Zugriff von Gesundheitsdiensteanbieterinnen unterliegt etwa die Übermittlung von Gesundheitsdaten per Funk (z.B. wireless LAN) sowie die Übermittlung von Gesundheitsdaten über vertraglich zugesicherte Leitungen von Fremdbetreiberinnen/Fremdbetreibern, wenn diese Leitungen auch anderen Nutzerinnen/Nutzern (z.B. bei Vereinbarungen über die Zurverfügungstellung von Bandbreiten) zur Verfügung gestellt werden (können). Ausschlaggebend für die Beurteilung der Ausschließlichkeit des Zugriffs ist eine objektive Betrachtung anhand der jeweiligen technischen Ausprägungen des verwendeten Mediums und nicht die im Zuge der Bereitstellung der Leitung allenfalls erfolgten (vertraglichen) Zusicherungen der/des Verfügungsberechtigten der Leitung. Die Ausschließlichkeit ist jedenfalls dann nicht gegeben, wenn der Datentransport – wenn auch nur teilweise – über das Internet erfolgt.

Als GesundheitsdiensteanbieterInnen sind jene Einrichtungen anzusehen, die durch eine „regelmäßige“ und „berufsmäßige“ Auslösung von Kommunikationsvorgängen mit Gesundheitsdaten zu diesem Gefahrenpotenzial beitragen. Durch die Qualifikation der „Regelmäßigkeit“ sollen gelegentliche Übertragungsvorgänge, wie etwa fallweises Melden gesundheitsbezogener Angaben der MitarbeiterInnen von Unternehmen, nicht dem Gesetz unterliegen.

* Kann Verschlüsselungsdienste auch von Dritten zur Verfügung gestellt werden?

JA:

Die Vertraulichkeit kann wirksam nur dann gewährleistet werden, wenn die Verschlüsselung vor Durchführung des Transports der Gesundheitsdaten durchgeführt wird. § 6 Abs. 2 schließt daher auch aus, dass Gesundheitsdaten über die in Abs. 1 bezeichneten Medien im Klartext an eine Dienstleisterin/einen Dienstleister, Netzbetreiberin/Netzbetreiber (Provider) oder an einen sonstigen, zwischen weitergebender/weitergebendem und empfangender/empfangendem Gesundheitsdiensteanbieterin/absendenden Gesundheitsdiensteanbieter eingeschaltete Informationsmittlerin/eingeschalteten Informationsmittler weitergegeben werden. Nicht ausgeschlossen ist dadurch, dass Informationsmittlerinnen/Informationsmittler Gesundheitsdaten zu Transportzwecken entschlüsseln oder umschlüsseln (Ent- und Neuverschlüsselung). Diesbezügliche Datenschutz- bzw. Datensicherheitsvereinbarungen müssen jedoch zwischen Auftraggeberin/Auftraggeber und Dienstleisterin/Dienstleister für den konkreten Einzelfall getroffen werden.

* Mindestanforderung /Verschlüsselung

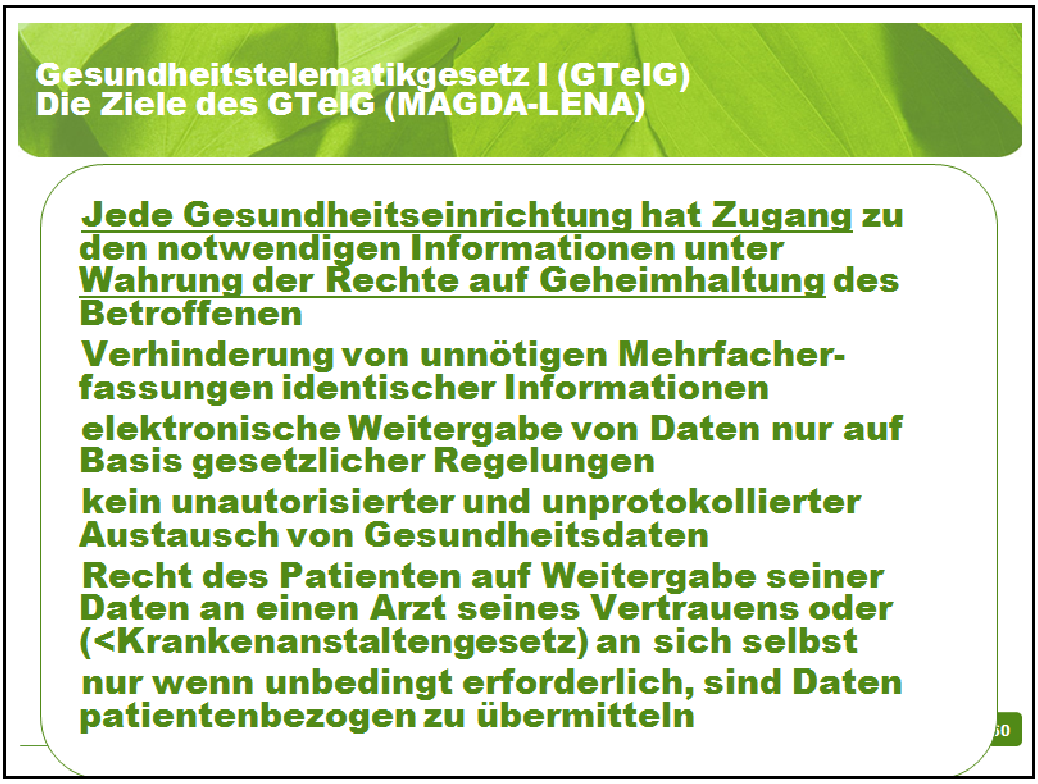
"Stand der Technik": § 6 Abs. 1: Zur inhaltlichen Verschlüsselung sind kryptographische Verfahren einzusetzen, die nach dem jeweiligen Stand der Technik mit wirtschaftlich vernünftigem Aufwand nicht kompromittiert werden können. Als wirtschaftlich nicht vernünftig ist ein Aufwand insbesondere dann anzusehen, wenn er auf Grund des dafür erforderlichen Aufwands (einzusetzende Ressourcen) von einem betriebswirtschaftlich zweckmäßig handelnden Subjekt zur Erzielung des beabsichtigten Erfolgs nicht getätigt würde.

* Kann man das CNSV Netz als innerbetriebliches Datennetz der SV gesehen werden?

NEIN (es findet ein Datenaustausch zwischen verschiedenen Gesundheitsdiensteanbieter statt,somit ist das GTelG anzuwenden - Die bloßen Eigentumsverhältnisse sind da nicht maßgeblich)

* Ist eine Verschlüsselung erforderlich wenn die BEV über das CNSV geführt wird?

"Nicht ausschließlich" dem Zugriff von Gesundheitsdiensteanbieterinnen unterliegt etwa die Übermittlung von Gesundheitsdaten über vertraglich zugesicherte Leitungen von Fremdbetreiberinnen/Fremdbetreibern, wenn diese Leitungen auch anderen Nutzerinnen/Nutzern (z.B. bei Vereinbarungen über die Zurverfügungstellung von Bandbreiten) zur Verfügung gestellt werden (können). Ausschlaggebend für die Beurteilung der Ausschließlichkeit des Zugriffs ist eine objektive Betrachtung anhand der jeweiligen technischen Ausprägungen des verwendeten Mediums und nicht die im Zuge der Bereitstellung der Leitung allenfalls erfolgten (vertraglichen) Zusicherungen der/des Verfügungsberechtigten der Leitung.



Zu § 8 (Dokumentation):

Von diesem Bundesgesetz nicht erfasst wird der innerorganisatorische (innerbetriebliche) elektronische Gesundheitsdatenaustausch. Die im innerorganisatorischen Bereich zu treffenden bzw. getroffenen Datenschutz- und Datensicherheitsmaßnahmen einschließlich der Mechanismen ihrer Kontrolle sind gemäß § 14 DSG 2000 zu dokumentieren, was mit Abs. 1 klar gestellt wird. In den §§ 4, 5 und 7 sind jedoch für bestimmte technische Ausprägungen des elektronischen Gesundheitsdatenaustausches Abweichungen von den getroffenen Regelungen zugelassen, die einer ergänzenden Dokumentations- und Auskunftspflicht unterliegen.

Gegenstand

§ 1. (1) Mit diesem Bundesgesetz werden ergänzende Datensicherheitsbestimmungen für den elektronischen Verkehr mit Gesundheitsdaten festgelegt sowie ein Informationsmanagement für Angelegenheiten der Gesundheitstelematik eingerichtet.
(2) Ziele dieses Bundesgesetzes sind, durch bundeseinheitliche Mindeststandards die Datensicherheit beim elektronischen Verkehr mit Gesundheitsdaten anzuheben sowie die für die Entwicklung und Steuerung der Gesundheitstelematik im internationalen Kontext notwendigen Informationsgrundlagen zu schaffen bzw. zu verbreitern.

Begriffsbestimmungen

§ 2. Im Sinne dieses Bundesgesetzes bedeuten
1. Gesundheitsdaten: direkt personenbezogene Daten gemäß § 4 Z 1 DSG 2000 über die physische oder psychische Befindlichkeit eines Menschen, einschließlich der im Zusammenhang mit der

Erhebung der Ursachen für diese Befindlichkeit sowie der medizinischen Vorsorge oder Versorgung, der Pflege, der Verrechnung von Gesundheitsdienstleistungen oder der Versicherung von Gesundheitsrisken erhobenen Daten. Dazu gehören insbesondere Daten die
a) die geistige Verfassung,
b) die Struktur, die Funktion oder den Zustand des Körpers oder Teile des Körpers,
c) die gesundheitsrelevanten Lebensgewohnheiten oder Umwelteinflüsse,
d) die verordneten oder bezogenen Arzneimittel, Heilbehelfe oder Hilfsmittel,
e) die Diagnose-, Therapie- oder Pflegemethoden oder
f) die Art, die Anzahl, die Dauer oder die Kosten von Gesundheitsdienstleistungen oder gesundheitsbezogene Versicherungsdienstleistungen betreffen.
2. Gesundheitsdiensteanbieterin/Gesundheitsdiensteanbieter: Auftraggeberinnen/Auftraggeber und Dienstleisterinnen/Dienstleister gemäß DSG 2000, deren regelmäßige Verwendung von Gesundheitsdaten Bestandteil ihrer Erwerbstätigkeit, ihres Betriebszwecks oder ihres Dienstleistungsangebotes ist.
3. Elektronischer Gesundheitsdatenaustausch: die Weitergabe von oder die Einräumung von Zugriffsrechten auf im Rahmen automationsunterstützter Datenanwendungen verwendeter Gesundheitsdaten mittels kommunikationstechnologischer Einrichtungen durch eine Gesundheitsdiensteanbieterin/einen Gesundheitsdiensteanbieter und zwar sowohl an Auftraggeberinnen/Auftraggeber (§ 4 Z 4 DSG 2000) als auch an Dienstleisterinnen/Dienstleister (§ 4 Z 5 DSG 2000).
4. Rolle: Klassifizierung von Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbietern nach der Art ihrer Erwerbstätigkeit, ihres Betriebszwecks oder ihres Dienstleistungsangebotes.

Zu § 2 des Entwurfs (Begriffsbestimmungen):

Zu Z 1:

Das DSG 2000 qualifiziert personenbezogene Gesundheitsdaten als ”sensible” Daten, für die das höchste Schutzniveau gilt. Eine Präzisierung, welche Daten dem Begriff „Gesundheitsdaten“ zuzuordnen sind, erfolgt nicht. Mit der WHO Definition von Gesundheit (Zustand des völligen körperlichen, geistigen und sozialen Wohlbefindens und nicht allein das Fehlen von Krankheit oder Gebrechen) wird deutlich, dass Gesundheitsdaten nicht mit Krankheitsdaten gleichzusetzen sind. In Z 1 des Entwurfes wird daher einerseits klar gestellt, dass unter Gesundheitsdaten auch Vorsorge-, Verrechnungs- und Versicherungsdaten zu verstehen sind. Andererseits werden diese Daten demonstrativ nach Datenkategorien beschrieben. Mit ”Struktur” wird der anatomische Aufbau des Körpers oder von Teilen des Körpers bezeichnet. Der Begriff ”Teil” des Körpers bezieht sich nicht nur auf sichtbare Ausprägungen, sondern auf alle Organe und Systeme, die in der medizinischen Wissenschaft als abgrenzbare Teile des Ganzen angesehen werden. Mit ”Funktion” werden die im menschlichen Körper ablaufenden Prozesse oder Vorgänge umschrieben, während ”Zustand” eine Beschreibung des Status ist. Ferner sind den Begriffen „Struktur“ bzw. „Funktion“ sowohl die personenbezogenen Basis-Informationen über das Erbgut (Sequenzdaten der DNA) als auch die daraus gewonnenen Erkenntnisse, etwa über die Bedeutung einer bestimmten Sequenz sowie die im Rahmen der Proteomik gewonnenen Erkenntnisse zu subsumieren. Mit lit. c werden Datenarten bezeichnet, die bei Bedarf im Rahmen der medizinischen Diagnostik erhoben werden und andererseits Sachverhalte – z.B. Daten über das Sexualleben, die dem Begriff „Lebensgewohnheiten“ zuzuordnen sind – betreffen, die selbst Gegenstand medizinischer Fragestellungen sein können.

Zu Z 2:

Ansatzpunkt für die im vorliegenden Entwurf vorgesehenen Datensicherheitsmaßnahmen ist das Gefahrenpotenzial beim Transport von Gesundheitsdaten. Als Gesundheitsdiensteanbieterinnen/Gesundheitsdiensteanbieter sind jene Einrichtungen anzusehen, die durch eine **„regelmäßige“ und „berufsmäßige“** Auslösung von Kommunikationsvorgängen mit Gesundheitsdaten zu diesem Gefahrenpotenzial beitragen. Durch die Qualifikation der „Regelmäßigkeit“ sollen gelegentliche Übertragungsvorgänge, wie etwa fallweises Melden gesundheitsbezogener Angaben der Mitarbeiterinnen/MItarbeiter von Unternehmen, nicht dem Gesetz unterliegen.

Zu Z 3:

Der elektronische Gesundheitsdatenaustausch kann in unterschiedlicher technologischer Ausprägung (z.B. Mail, automatisierte Server-Server/Kommunikation, Client- Server/Applikationen) erfolgen. Dem Gesetz unterliegen alle Varianten und unabhängig davon, ob die Gesundheitsdaten aktiv weitergeben oder der Kommunikationspartnerin/dem Kommunikationspartner Zugriffsrechte auf Datenbestände eingeräumt werden. Nicht von Bedeutung ist, in welchem Datenformat oder in welcher Kombination von Datenformaten („multimediale Gesundheitsdaten“) die Gesundheitsdaten in elektronischer Form verwendet werden.

Zu Z 4:

Gemäß DSG 2000 (§ 7) ist die Übermittlung von Daten nur dann zulässig, wenn 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. Durch die berufliche/betriebliche Klassifizierung, die von der hiezu befugten Autorität zu bestätigen ist, soll dieser Prozess der Glaubhaftmachung in elektronisch überprüfbarer Form unterstützt und damit das für den elektronische Gesundheitsdatenaustausch vorauszusetzende Vertrauen gewährleistet werden. Grundsätzlich wird jedoch im Entwurf davon ausgegangen bzw. vorausgesetzt, dass Gesundheitsdaten rechtlich zulässig (gemäß DSG 2000) ausgetauscht werden.