UNIVERSITÄTSLEHRGANG
FÜR INFORMATIONSRECHT UND RECHTSINFORMATION
AN DER RECHTSWISSENSCHAFTLICHEN FAKULTÄT DER UNIVERSITÄT WIEN

Data-Mining und Datenschutz

MASTER THESIS

zur Erlangung des akademischen Grades

MASTER OF LAWS (LL.M.)

INFORMATIONSRECHT UND RECHTSINFORMATION

an der Universität Wien

(Universitätslehrgang für Informationsrecht und Rechtsinformation)

vorgelegt von

Mag. Barbara Seidl

begutachtet von

ao. Univ. Prof. Dr. Dietmar Jahnel

im September 2003

Hinweise

Dieses Layout basiert auf der Typoskriptvorlage der Österreichischen Rechtswissenschaftlichen Studien (ÖRSt). Die Verwendung, Bearbeitung und allfällige Veröffentlichung der Bearbeitung erfolgt mit freundlicher Bewilligung des Manz-Verlages. Ansonsten wird auf das UrhG verwiesen.

Zeitschriftenartikel werden mit der Anfangsseitenzahl zitiert, um eine leichtere Auffindbarkeit in der RDB zu ermöglichen.

Die URLs wurden zuletzt am 1. September 2003 überprüft.

Inhaltsverzeichnis

I. Einleitung

Jedes Geschehen, jeder Gegenstand im täglichen Leben stellt ein Datum dar. Jedermann hat Anspruch auf Geheimhaltung dieser ihn betreffenden Daten.

Unternehmen und Staat benötigen Informationen zur bestmöglichen Erfüllung ihrer Pflichten und Geltendmachung ihrer Rechte. Zu diesem Zweck werden Daten gesammelt und in Datenbanken gespeichert, die nicht nur im Einzelfall Auskunft geben, sondern auch für künftige Entscheidungen ausschlaggebend sein können. Zum Ziel wird es immer mehr, Verhaltensweisen und Gewohnheiten von Personen genau zu untersuchen und so weit wie möglich vorherzusagen, um wirtschaftliche Vorteile zu erzielen.

Wie sich aktuell zeigt, ist es problemlos möglich, eine CD mit gespeicherten Daten von zwei Millionen Österreichern über Haushaltsgröße, Partnerschaft, Kaufkraft, Altersklasse, Gebäudeart, Anzahl der Kinder usw herzustellen, wobei zusätzlich vier Mal jährlich ein Update erfolgen soll.[1]

Der Gesetzgeber räumt dem Datenschutz einen besonderen Stellenwert ein und ermöglicht die Weitergabe von Daten nur unter ganz bestimmten Voraussetzungen.

Das Spannungsverhältnis zwischen den Geheimhaltungsinteressen jedes einzelnen Menschen hinsichtlich seiner personenbezogenen Daten und den Interessen der Datenbankinhaber an der ökonomischen Auswertung genau dieser Daten soll in dieser Arbeit untersucht werden. Zu diesem Zweck ist zunächst eine allgemeine Definition des "Data-Minings" sowie der grundlegenden Begriffe des österreichischen Datenschutzrechts nötig. Sodann erfolgt die Subsumierung des Data-Minings unter das DSG 2000.

---

[1] http://futurezone.orf.at/futurezone.orf?read=detail&view=bw&id=180049&tmp=80570, http://www.kurier.at/multimedia/365234.php.

II. Data-Mining

Anzahl und Größe der Datenbanken sowie der darin gespeicherten Datenmengen nehmen täglich zu. Die Auffindung von interessanten und nützlichen Mustern und Regeln in den so gespeicherten Daten bedeutet zusätzliches Wissen. Preisausschreiben, Kundenkarten und Rabatte zielen nicht auf das Kundenwohl, sondern auf die Sammlung von Kundendaten.

Automationsunterstützte Methoden vereinfachen die Datenerfassung sowie die Erstellung von Datenprofilen und sind heute für jedermann zugänglich. Technik, Anschaffungs- und Betriebskosten stellen kaum mehr Hürden für Interessenten dar.

So wie es beim „Mining" um die Aufsuchung, Gewinnung und Aufbereitung von mineralischen Rohstoffen wie Kohle, Erze, Salze und Gesteine geht, hat das Data-Mining die Aufbereitung von Daten in Verfahren, die selbständig Annahmen generieren (maschinelles Lernen), diese prüfen und dem Anwender relevante Ergebnisse in verständlicher Form präsentieren, zum Ziel. Berücksichtigt werden auch bereits bekannte Lösungsansätze aus dem Bereich der Künstlichen Intelligenz (zB neuronale Netze, Entscheidungsbäume) sowie herkömmliche statistische Verfahren (zB Clusteranalyse)[2] Data-Mining ist zwar grundsätzlich lediglich ein Teilschritt des **„Knowledge Discovery in Databases (KDD)**"[3], wird im kommerziellen Bereich aber sprachlich als Synonym für KDD verwendet. Auch in dieser Arbeit soll der Begriff Data-Mining alle Stufen der Suche nach neuem Wissen erfassen.

Als **Data-Mining** bezeichnet man die **softwaregestützte automatisierte Vorhersage** von bspw Lösungsvorschlägen **auf Basis von bekannten Verhaltensschemata aus der Vergangenheit sowie die Ermittlung von bisher unbekannten Zusammenhängen, Mustern und Trends in sehr großen Datenbanken**.[4] Das erklärte Ziel ist es, neues Wissen freizulegen, zu entdecken und es zu nutzen. Data-Mining erzeugt implizite Informationen.[5]

Weitere Ziele des Data-Minings sind die Segmentierung, die Klassifikation, die Prognose, die Konzeptbeschreibung, die Abweichungserkennung und die Abhängigkeitsanalyse.[6]

---

[2] *Krahl/Windheuser/Zick*, Data Mining, 1998, 23.
[3] *Heuer/Saake*, Datenbanken, 2000[2], 585.
[4] *Hansen/Neumann*, Wirtschaftsinformatik I, 2001[8], 474.
[5] *Krahl/Windheuser/Zick*, Data Mining, 1998, 24.
[6] *Heuer/Saake*, Datenbanken, 2000[2], 587.

A. Data-Mining

Data-Mining umfasst nicht nur eine einzelne Technik oder ein einzelnes technisches Verfahren. Die Ermittlung des neuen Wissens erfolgt vielmehr in einem Prozess, der von der **Bereitstellung der Daten bis zur Anwendung der gewonnenen Erkenntnisse** reicht. Die konkrete Ausgestaltung dieses Prozesses ist vom Einzelfall abhängig. Es handelt sich um einen **iterativen Prozess**, dessen tatsächliche Planung und Ausführung nicht automatisierbar ist. Noch immer steht der Mensch im Mittelpunkt, der Ziel und Vorgangsweise festlegt. Er interagiert mit sehr umfangreichen Datenbanken und setzt eine Menge heterogener Werkzeuge ein, um einzelne Teilprobleme zu lösen, bevor die Resultate zu entscheidungsrelevanten Erkenntnissen verdichtet werden können. Hierbei lassen sich vier Phasen des Data-Mining-Prozesses (KDD-Prozesses) unterscheiden – **Planungs-**, **Vorbereitungs-**, **Data-Mining- und Auswertungsphase**.

1. Data-Mining-Modelle

Grundsätzlich ist die Unterscheidung zweier Data-Mining Modelle möglich, die sich unter verschiedenen Ansätzen dem Ziel nähern – das Verification und das Discovery Modell.

a) Verification Model[7]

Von einem Anwendungsexperten formulierte **Hypothesen und Fragen werden** mit Hilfe verschiedener Abfrage- und Analysetools **anhand der Daten bestätigt oder verworfen**. Diese Methode entspricht den meisten klassischen statistischen Analysemethoden.

b) Discovery Model[8]

Dieser Methode liegt die **automatische Auffindung von Hypothesen** zugrunde. Sie werden gleichzeitig generiert und anhand der Daten überprüft. Im **direkten Prozess** ist die Zielvariable vorgegeben, während die abhängigen Variablen gesucht werden sollen. Im **indirekten Prozess** wird dagegen ohne Verwendung von vorab definierten Variablen versucht, aus den gespeicherten Daten neue Zusammenhänge bzw Korrelationen zu finden.

---

[7] http://www.ai.univie.ac.at/oefai/ml/kdd/wasist.html.
[8] http://www.unet.univie.ac.at/~a9560254/pub/dm/.

2. Die Phasen des Data-Minings

Ziel der **Planungsphase** ist die Festlegung der konkreten Aufgabenstellung und die Auswahl der für deren Erfüllung erforderlichen Experten. In der anschließenden **Vorbereitungsphase** soll mit der Sammlung von Daten und deren Aufbereitung durch Integration und Data Cleaning, dem Entfernen oder Berichtigen offensichtlich falscher oder widersprüchlicher Daten eine „Mining Base" als Ausgangsbasis für die sodann anzuwendenden Analysefunktionen und -methoden geschaffen werden. In der **Miningphase** findet schließlich die eigentliche Suche nach interessanten Mustern statt. Aufgrund der hierdurch erlangten Erkenntnisse kann es notwendig werden, bestimmte Schritte aus der Vorbereitungsphase zu wiederholen, um so zB zusätzliche Daten in die Mining Base einzufügen. Aufgabe der **Auswertungsphase** ist die Auswertung der Ergebnisse der Miningphase, um sie auch für Nichtexperten verständlich zu machen. Dieses Ziel wird durch Interpretation, vor allem durch Visualisierung und Zusammenstellen der Ergebnisse und auch der Nutzung des gewonnenen Wissens erreicht.[9]

B. Wissen durch Data-Mining

Muster in Datenbeständen, die bestimmte Eigenschaften aufweisen und in einer formalen Sprache dargestellt werden, stellen Wissen durch Data-Mining dar.

1. Eigenschaften

Muster müssen in einer leicht verständlichen Sprache formuliert oder in graphischer Form dargestellt werden (**understandable**). Sie haben auch auf zukünftige Daten mit einer gewissen Sicherheit zuzutreffen (**valid**) und müssen aber dennoch neu sein. Die auf diese Art neuen Muster müssen weiters für die konkrete Aufgabenstellung verwendbar und relevant sein (**useful**). Vom Algorithmus wird verlangt, autonom komplexe Zusammenhänge zu untersuchen und nur interessante Zusammenhänge als Wissen zu präsentieren (**non-trivial**). Auch das gefundene Wissen an sich hat interessant zu sein (**interesting**).[10]

Muster haben daher understandable, valid, useful, non-trivial und interesting zu sein.

---

[9] *Heuer/Saake*, Datenbanken, 2000[2], 586.

[10] http://www.ai.univie.ac.at/oefai/ml/kdd/wi-eigensch.html.

2. Formale Sprache

Die für die Beschreibung der Muster gewählte Sprache muss **für Menschen leicht verständlich** sein. Die Visualisierung von Ergebnissen spielt daher eine wichtige Rolle.[11]

3. Die häufigsten Arten von Mustern

a) Regeln[12]

aa) Klassifikationsregeln

Die Datenbank wird zunächst in mehrere Klassen von Daten unterteilt. Die Klassifikationsregeln ordnen neue Objekte, die in der Ausgangsdatenbank nicht vorgekommen sein müssen, möglichst gut einer der vorhandenen Klassen zu.

bb) Charakteristische Regeln

Charakteristische Regeln beschreiben möglichst kompakt, welche Eigenschaften allen zu einer Klasse gehörenden Objekten gemeinsam sind. Sie befassen sich daher mit typischen Eigenschaften von Objekten einer bestimmten Klasse.

cc) Regressionsregeln

Regressionsregeln bestimmen nicht wie die Klassifikationsregeln die Zugehörigkeit eines Objektes zu einer bestimmten Klasse, sondern sagen einen numerischen Wert voraus.

b) Cluster

Die Objekte einer Datenbank werden in einer selbständigen Klassifizierung basierend auf statistischen Verfahren zu Gruppen zusammengefasst. Das Data-Mining geht über diese bloß statistische Auswertung hinaus, indem zusätzlich eine verständliche Beschreibung der Gruppen vorgenommen wird. Die Ähnlichkeiten der Objekte innerhalb einer Kategorie sollen möglichst groß, zwischen den Kategorien aber gering sein.[13]

---

[11] http://www.ai.univie.ac.at/oefai/ml/kdd/wi-eigensch.html.
[12] http://www.ai.univie.ac.at/oefai/ml/kdd/wi-klass.html.
[13] *Heuer/Saake*, Datenbanken, 2000[2], 586.

c) Abhängigkeitsmuster

Abhängigkeitsmuster ermitteln statistische Abhängigkeiten zwischen Variablen der relevanten Datensätze.[14]

aa) Assoziationsregeln

Assoziationsregeln beschreiben welche Gruppen von Objekten, welche Eigenschaft usw häufig gemeinsam auftreten.

bb) Determinationen und funktionale Abhängigkeiten

Diese Begriffe behandeln Abhängigkeiten zwischen Attributen von Objekten. Ist der Wert eines Attributs bei allen Objekten eindeutig durch die Werte derselben Mengen von Attributen bestimmt, so liegt eine funktionale Abhängigkeit vor. Ist der Wert zwar nicht immer, aber sehr oft von anderen Attributen bestimmt, spricht man von Determinationen. Auf diese Weise können kausale Zusammenhänge leicht in einer Datenbank aufgespürt werden.[15]

d) Verbindungsmuster

Verbindungsmuster zielen auf die Auffindung von Regelmäßigkeiten zwischen verschiedenen Objekten ein und derselben Datenbank und unter Umständen sogar verschiedener Datenbanken.[16]

e) Sequenzmuster

Dieses Verfahren dient der Suche nach häufig auftretenden Episoden oder Ereignisfolgen in Datenbeständen, denen eine bspw zeitliche Ordnung der einzelnen Datensätze zugrunde liegt.[17]

f) Abweichungen von erwarteten statistischen Verteilungen

Nach diesem Muster verfügt eine Teilmenge von Objekten einer Datenbank über andere Eigenschaften als aufgrund der Gesamtmenge eigentlich statistisch zu erwarten gewesen wäre.[18]

---

[14] *Heuer/Saake*, Datenbanken, 2000[2], 586.
[15] http://www.ai.univie.ac.at/oefai/ml/kdd/wi-ass.html.
[16] http://www.ai.univie.ac.at/oefai/ml/kdd/wi-link.html.
[17] *Heuer/Saake*, Datenbanken, 2000[2], 586.
[18] http://www.ai.univie.ac.at/oefai/ml/kdd/wi-abw.html.

g) Formeln und mathematische Gesetzmäßigkeiten

Bei der Analyse von numerischen Daten kann auch daran Interesse bestehen, den Zusammenhang zwischen Variablen in mathematischer Form herauszufinden.[19]

C. Die häufigsten Techniken des Data-Minings

1. Warenkorbanalyse

Die Warenkorbanalyse kommt beispielsweise im Einzelhandel zur Anwendung. Sie findet Gruppen von häufig gemeinsam verkauften Produkten. Wird sie mit Kundendaten verknüpft, können Kaufwahrscheinlichkeiten für zukünftige Einkäufe errechnet und die Kunden mit personen- bzw gruppenbezogenen Werbeaktionen angesprochen werden.[20] Auch für Warenplatzierungen kann die Warenkorbanalyse hilfreich sein. Sie gehört zur Gruppe der Clusteranalysen.[21]

2. Fallbasiertes Schließen

Aus den Erfahrungen der Vergangenheit werden mit dieser Technik zukünftige Entscheidungen abgeleitet. Charakteristische Eigenschaften und relevante Parameter von einzelnen Entscheidungsfällen sind in einer Fall-Datenbank gespeichert. Soll eine neue Entscheidung getroffen werden, werden die Parameter gesichtet und mit der Datenbank verglichen. Gesucht wird dabei nach größtmöglichen Übereinstimmungen mit den historischen Daten, wobei der Grad der Ähnlichkeit der Konstellationen zur Genauigkeit der Vorhersage proportional ist.[22] Die neuen Fälle werden wieder in der Datenbank abgelegt.[23]

3. Entscheidungsbaum

Komplexe Gesamtentscheidungen werden durch eine Menge von Teilentscheidungen gelöst.[24] An jedem Knoten eines solchen Entscheidungsbaumes wird ein Attribut abgefragt und eine Entscheidung getroffen. Dies passiert so lange, bis ein Knoten erreicht wird, an dem keine weitere Verzweigung mehr möglich ist.[25] In jedem Knoten wird dasjenige Attribut gesucht, das die Klassifikation auf den betrachteten Daten am besten

---

[19] http://www.ai.univie.ac.at/oefai/ml/kdd/wi-gesetz.html.
[20] http://www.unet.univie.ac.at/~a9560254/pub/dm/.
[21] *Heuer/Saake*, Datenbanken, 2000[2], 587.
[22] http://wwwai.wu-wien.ac.at/~koch/lehre/inf-sem-ws-00/nentwich/mining.pdf.
[23] *Hansen/Neumann*, Wirtschaftsinformatik I, 2001[8], 473.
[24] http://wwwai.wu-wien.ac.at/~koch/lehre/inf-sem-ws-00/nentwich/mining.pdf.
[25] *Krahl/Windheuser/Zick*, Data Mining, 1998, 69.

erklärt. Die Daten werden sodann in Untermengen geteilt und einer neuerlichen separaten Betrachtung zugeführt.[26]

4. Neuronale Netze

Das kleinste Element eines neuronalen Netzes ist das Neuron. Es verarbeitet Inputgrößen zu einem Output und tauscht Informationen per Stimulationen über Verbindungen mit anderen Neuronen aus. Da die Neuronen somit untereinander mit Input und Output verknüpft sind, entsteht insgesamt ein informationsverarbeitendes System.[27] Ein bestimmter Input führt zu einem bestimmten Output, wobei der Weg zur Lösung aber nicht einsichtig wird.

5. Genetische Algorithmen

Genetische Algorithmen stellen eine Form der Selbstorganisation dar. Aus zufällig bereitgestellten Anfangslösungen wird eine nahezu optimale Ergebnislösung entwickelt, wozu die Evolutionstheorie mit ihren wesentlichen Elementen genutzt wird. So werden aus einer vorgegebenen Palette an Lösungsvorschlägen die besten ausgelesen (Selektion), ihre Kenngrößen rekombiniert und als neue Generation von Basislösungen aufgefasst (Kreuzung). Die Kenngrößen werden zusätzlich zufälligen Abänderungen unterworfen (Mutation). Das System wird so von Generation zu Generation zu immer besseren Lösungen optimiert.[28]

6. Automatische Clusteranalyse

Die automatische Clusteranalyse erfolgt meist als erster Schritt in sehr großen Datenbeständen, um eine erste Auffindung von Gruppen durchzuführen. Diese Gruppen werden sodann mittels anderer Techniken weiter untersucht.[29]

7. Analyse von Beziehungen zwischen den Datensätzen

Diese Analysetechnik versucht Beziehungen zwischen den einzelnen Datensätzen einer Datenbank herzustellen. Sie unterliegt der Einschränkung, nur mit strukturierten Daten umgehen zu können. Die verwendeten Daten müssen daher speziell dafür aufbereitet werden.[30]

---

[26] *Krahl/Windheuser/Zick*, Data Mining, 1998, 69.
[27] http://www.unet.univie.ac.at/~a9560254/pub/dm/.
[28] *Krahl/Windheuser/Zick*, Data Mining, 1998, 93.
[29] http://www.unet.univie.ac.at/~a9560254/pub/dm/.
[30] http://www.unet.univie.ac.at/~a9560254/pub/dm/.

D. Problematische Trends

Wesentliches Merkmal des Data-Minings ist die Suche nach bisher unbekannten Beziehungen. Zweck sowie mögliche Verwendungen der Resultate sind daher im Prozessablauf unbestimmt.[31]

1. Customer Relationship Management CRM

Kundenbeziehungsmanagement stellt eine Unternehmenspolitik dar, die mit Hilfe von Informationstechnologien alle kundenbezogenen Daten und Abläufe zusammenfasst und optimiert.[32] Dabei steht entweder die Kundenzufriedenheit oder der Unternehmensprofit im Vordergrund.

2. Customer Profile Exchange CPEX

Daten sollen nicht nur im eigenen Interesse ausgewertet, sondern auch an Dritte weitergegeben bzw veräußert werden. Unter http://www.cpexchange.org wurde ein offener Standard geschaffen, der den **weltweiten Datenaustausch** erleichtert. Globale Datenflüsse führen dazu, dass die Übersicht verloren geht, wo und bei wem welche Daten gespeichert und verarbeitet werden. Die immer größeren Datenpools erlauben auch die Erstellung von immer präziseren und aussagekräftigeren Kundenprofilen.[33]

Dies alles führt zu einer Vorratshaltung von Daten mit unbekannten Zielen. Die Intransparenz steigt, für den Betroffenen sind die Einsatzmöglichkeiten „seiner" Daten nicht mehr einschätzbar. Die Missbrauchsgefahr ist offensichtlich.

Trotz dieser Trends darf aber nicht vergessen werden, dass das Data-Mining auch abseits von der Analyse „wirtschaftlicher" Daten zum Einsatz gelangt. Flugzeughersteller setzen zum Beispiel Data-Mining-Techniken ein, um bislang unbekannte Zusammenhänge zwischen verschiedenen Defekten in ähnlichen Flugzeugtypen zu entdecken.[34]

---

[31] http://www.akwien.at/396_11161.htm.
[32] *Hansen/Neumann*, Wirtschaftsinformatik I, 2001[8], 583.
[33] http://www.akwien.at/396_11161.htm.
[34] *Hansen/Neumann*, Wirtschaftsinformatik I, 2001[8], 475.

III. Das Bundesgesetz über den Schutz personenbezogener Daten – DSG 2000

Die Anknüpfung im Datenschutz erfolgt nicht an Wissen oder Information sondern an **auf geeigneten Medien gespeicherten Daten mit Personenbezogenheit**. Im Datenschutzrecht stehen einander Auftraggeber und Betroffener gegenüber. Jeder der beiden verfolgt ein bestimmtes Ziel – während der Auftraggeber personenbezogene Daten verarbeiten möchte, ist der Betroffene auf die Wahrung seiner Privatsphäre und seines Grundrechtes auf Datenschutz bedacht. Er ist Träger bestimmter Rechte, wo hingegen den Auftraggeber entsprechende Pflichten treffen. Auf Seiten des Auftraggebers kann zusätzlich noch ein Dienstleister hinzutreten. Rechte und Pflichten der beteiligten Personen entspringen dem DSG 2000.

Das Problem der datenschutzrechtlichen Privatsphäre liegt weniger in der Preisgabe von Daten als in der unerlaubten Speicherung und Nutzung für andere, neue Zwecke.[35]

A. Begriffsdefinitionen

1. Das Grundrecht auf Datenschutz - § 1 DSG 2000

Jedermann hat, insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten, soweit ein schutzwürdiges Interesse daran besteht. Das Bestehen eines solchen Interesses ist ausgeschlossen, wenn Daten infolge ihrer allgemeinen Verfügbarkeit oder wegen ihrer mangelnden Rückführbarkeit auf den Betroffenen einem Geheimhaltungsanspruch nicht zugänglich sind.

Jedermann hat, soweit ihn betreffende personenbezogene Daten zur automationsunterstützten Verarbeitung oder zur Verarbeitung in manuell, dh ohne Automationsunterstützung geführten Dateien bestimmt sind, nach Maßgabe gesetzlicher Bestimmungen 1. das Recht auf Auskunft darüber, wer welche Daten über ihn verarbeitet, woher die Daten stammen, und wozu sie verwendet werden, insbesondere auch, an wen sie übermittelt werden; 2. das Recht auf Richtigstellung unrichtiger Daten und das Recht auf Löschung unzulässigerweise verarbeiteter Daten.

[35] *Schweighofer*, Data Mining und Datenschutz, DuD 21 (1997), 459.

2. Daten - § 4 Z 1 und 2 DSG 2000

Personenbezogene Daten sind alle Angaben über Betroffene (Z 3), deren Identität bestimmt oder bestimmbar ist. Nur indirekt personenbezogen sind Daten für einen Auftraggeber (Z 4), Dienstleister (Z 5) oder Empfänger einer Übermittlung (Z 12) dann, wenn sie die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen können. Sensibel und besonders schutzwürdig sind Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben.

Der Begriff der Daten wird weit verstanden.[36] So sind Daten nicht nur dann personenbezogen, wenn die Identität des Betroffenen für den jeweiligen Verwender bestimmbar ist, sondern auch, wenn dies nur für einen Dritten gilt. In der Folge wird daher zwischen **direkt und indirekt personenbezogenen Daten** differenziert. Jeder Datenart werden unterschiedliche Beschränkungen auferlegt. Der Verwender nur indirekt personenbezogener Daten unterliegt erleichterten datenschutzrechtlichen Bedingungen.

Bezüglich der möglichen Bestimmbarkeit der Identität der Betroffenen sind als mögliche **Mittel der Identifikation** nur solche anzusehen, **die vernünftigerweise angewendet werden**.[37] Das sind solche, die weder ihrer Art nach, noch ihrem Aufwand nach vollkommen ungewöhnlich sind. Durch die Kombination von mehreren Angaben, die für sich allein noch keine Bestimmbarkeit ermöglichen, kann die Bestimmbarkeit erzeugt werden. Das DSG 2000 fordert eine sichere und nicht auf hoher Wahrscheinlichkeit basierende Bestimmbarkeit der Identität.

Anonymisierten Daten kann niemand auf eine in ihrer Identität bestimmte Person zurückführen. Es besteht kein Personenbezug, weshalb derartige Daten auch nicht in datenschutzrechtlicher Hinsicht relevant sind.

Personenbezogen sind alle Angaben über den Betroffenen unabhängig davon, ob sie seinen beruflichen oder privaten Bereich betreffen. Auch Wirtschaftsdaten können daher personenbezogene Daten sein, ebenso Werturteile und Vermutungen in Bild- oder Tonform.[38] Stimme und Fingerabdrücke sind personenbezogene Informationen.[39]

Hinsichtlich **sensibler Daten** besteht die Gefahr ihrer diskriminierenden Verwendung. Zu prüfen ist allein, ob das Datum unter eine der taxativ aufgezählten Datenkategorien fällt. Ein **Diskriminierungsrisiko** des konkreten Informationsgehaltes ist dagegen unwesentlich. [40]

---

[36] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 26.
[37] Erwägungsgrund 26, EG-Datenschutzrichtlinie 95/46/EG.
[38] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 117.
[39] *Ghali*, Datenschutz (1999), 140.
[40] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 112.

3. Der Auftraggeber - § 4 Z 4 DSG 2000

Auftraggeber sind natürliche oder juristische Personen (nicht aber deren Organe), Personengemeinschaften (wie etwa OHG, KG, GesbR) oder Rechtsträger und Organe einer Gebietskörperschaft bzw die Geschäftsapparate solcher Organe (zB Bundesministerien, Ämter der Landesregierungen), wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z 9), dies unabhängig davon, ob sie die Verarbeitung selbst durchführen oder hiezu einen anderen heranziehen. Als Auftraggeber gelten die genannten Personen, Personengemeinschaften und Einrichtungen auch dann, wenn sie einem anderen Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen und der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten. Wurde jedoch dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten ausdrücklich untersagt und nimmt er sie dennoch vor oder hat er die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln gemäß § 6 Abs 4 DSG 2000 eigenverantwortlich zu treffen, so gilt der Auftragnehmer als datenschutzrechtlicher Auftraggeber.

Der datenschutzrechtliche Auftraggeberbegriff ist vom zivilrechtlichen Auftragsverhältnis zu unterscheiden und davon unabhängig.[41] Im Wesentlichen kommt es für die Qualifikation als **datenschutzrechtlicher Auftraggeber** allein auf faktische Umstände an – nämlich **die Entscheidung zur Datenverarbeitung**. Die Frage der rechtlichen Zulässigkeit der Verarbeitung hat dabei unberücksichtigt zu bleiben.[42]

Der Einsatz von EDV ist grundsätzlich dem Werkbesteller als Auftraggeber zuzurechnen. Dafür bedarf es keiner ausdrücklichen Vereinbarung zwischen ihm und dem Auftragnehmer. Wurde allerdings der Einsatz von EDV ausdrücklich verboten, ist der Auftragnehmer datenschutzrechtlicher Auftraggeber, wenn er dennoch EDV einsetzt. Da er sich aber für die Auftraggebereigenschaft auf keine entsprechende Rechtsgrundlage berufen kann, wird eine automationsunterstützte Verarbeitung auf Grund seiner autonomen Entscheidung unzulässig sein.[43]

Zu beachten bleiben auch jene Beauftragungsverhältnisse, in welchen traditionellerweise der **Auftragnehmer selbständig („eigenverantwortlich") über die Verwendung der ihm übergebenen Informationen entscheidet** und auch nach den ihn treffenden Standesregeln verpflichtet und dafür verantwortlich ist. Dies gilt zB für bestimmte freie Berufe wie Rechtsanwälte, Wirtschaftstreuhänder, Unternehmens- und Finanzberater.

---

[41] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 28.
[42] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 120.
[43] *Ghali*, Datenschutz (1999), 141.

Datenschutzrechtliche Auftraggeber werden die Auftragnehmer in diesen Fällen, wenn sie die **Entscheidung über die Verarbeitung der überlassenen Daten** auf Grund von Rechtsvorschriften, Standesregeln oder Verhaltensregeln nach § 6 Abs 4 DSG 2000 **eigenverantwortlich zu treffen haben**. In diesem Zusammenhang könnte es im Sinn der Rechtssicherheit zweckmäßig sein, in **Verhaltensregeln** gemäß § 6 Abs 4 DSG 2000 klarzustellen, wem in welchen Konstellationen die Auftraggebereigenschaft zukommt (vgl IV. B. 1.).[44] Es ist schwer vorstellbar, dass die Klienten solcher freier Dienstleistungsberufe als datenschutzrechtliche Auftraggeber partiell für im Rahmen des Dienstleistungsverhältnisses erfolgende Datenverarbeitungen verantwortlich sein sollen.[45]

Der **Auftraggeber ist für die Zulässigkeit der Verwendung von Daten** nach § 7 DSG 2000 **verantwortlich**. Er hat Maßnahmen zur **Gewährleistung der Datensicherheit** zu treffen, wobei auf dem Stand der technischen Möglichkeiten und nach der wirtschaftlichen Vertretbarkeit sicherzustellen ist, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind, dass ihre Verwendung ordnungsgemäß erfolgt und sie Unbefugten nicht zugänglich sind (§ 14 DSG 2000). Den Auftraggeber trifft die **Meldepflicht** an die Datenschutzkommission vor Aufnahme einer Datenanwendung gemäß § 17 DSG 2000. Weiters unterliegt er einer **Informationspflicht** (§ 24 DSG 2000) sowie einer **Auskunftspflicht** gegenüber dem Betroffenen über die zu seiner Person verarbeiteten Daten, wenn der Betroffene dies schriftlich verlangt und seine Identität in geeigneter Form nachweist (§ 26 DSG 2000). Den Auftraggeber trifft auch die Pflicht unrichtige oder entgegen den Bestimmungen des DSG 2000 verarbeitete **Daten richtigzustellen oder zu löschen** (§ 27 DSG 2000).

4. Der Betroffene - § 4 Z 3 DSG 2000[46]

> *Betroffener ist jede vom Auftraggeber (Z 4) verschiedene natürliche in- und ausländische oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden.*[47]

Der Betroffene ist der Träger der wesentlichen Rechte nach dem DSG 2000. Der Auftraggeber ist selbst dann nicht Betroffener im Sinne des DSG 2000, wenn er Daten verwendet, die ihn selbst betreffen. Auch **Personengemeinschaften ohne Rechtspersönlichkeit** (wie zB Hauseigentümergemeinschaften, GesbR) können Betroffene sein.

Nicht unter die Definition des Betroffenen fallen **Verstorbene** oder **rechtlich nicht mehr existente juristische Personen**.

---

[44] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 62.
[45] *Holoubek/Potacs*, Öffentliches Wirtschaftsrecht Band 1, 2002, 251.
[46] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 119.
[47] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 28.

5. Der Dienstleister - § 4 Z 5 DSG 2000

Dienstleister sind natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden (vgl § 4 Z 8 DSG 2000).

Wesentlich für die Stellung des Dienstleisters ist nach dieser Begriffsbestimmung die **Beauftragung durch den Auftraggeber**. Die Verarbeitung darf nur über **Weisung des Auftraggebers** erfolgen.[48] Die datenschutzrechtliche Verantwortung verbleibt im Außenverhältnis beim Auftraggeber.[49]

Die Pflichten des Dienstleisters sind in § 11 DSG 2000 geregelt.

6. Die Datei - § 4 Z 6 DSG 2000

Eine Datei ist eine strukturierte, dh nach einer bestimmten Ordnung dargestellte, Sammlung von Daten, die nach mindestens einem Suchkriterium (zB eine bestimmte Eigenschaft oder bestimmte Kenntnisse[50]) zugänglich ist und einen leichten Zugriff ermöglicht.[51]

Unter den Dateibegriff fallen auch **Karteien und Listen bei manueller Verarbeitung**, nicht aber Akten, solange ihr Inhalt nicht nach einem Suchkriterium strukturiert ist.[52]

Eine Struktur der Sammlung ist zu bejahen, wenn sie eine **äußere Ordnung** aufweist, nach der die verschiedenen Arten von Daten in einer bestimmten **räumlichen Verteilung** auf dem oder den Datenträgern oder in einer bestimmten **physikalischen oder logischen Struktur** dargestellt sind.[53]

---

[48] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 120.
[49] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 29.
[50] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 31.
[51] *Ghali*, Datenschutz (1999), 142.
[52] *Jahnel/Schramm/Staudegger*, Informatikrecht (2003[2]), 249.
[53] OGH 28. Juni 2000, 6 Ob 148/00 h = ÖJZ 2001/1 = RdW 2000/727 = ZVR 2001/31.

7. Die Verwendung von Daten - § 4 Z 8 DSG 2000

Unter der Verwendung von Daten ist jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten zu verstehen.

Das Verwenden von Daten als Überbegriff vereint sämtliche Schritte der Datenverarbeitung.[54]

8. Die Verarbeitung von Daten - § 4 Z 9 DSG 2000

Das Verarbeiten von Daten umfasst das **Ermitteln**, als Erhebung der Daten in der Absicht, sie in einer Datenanwendung zu verwenden, weiters das **Erfassen** und **Speichern,** als Aufnahme der Daten auf dem Datenträger, das **Aufbewahren**, das **Ordnen** als Sortieren der Daten nach bestimmten Kriterien, das **Vergleichen**, das **Verändern,** als Änderung der Aussage oder der Darstellung der Daten, wozu auch eine Berichtigung, Ergänzung oder das teilweise Löschen zählt, das **Verknüpfen,** als das miteinander in Beziehung setzen von zwei oder mehreren Daten durch einen automationsunterstützten Vorgang, sodass ein Zusammenhang zwischen den Daten ersichtlich wird oder wenn zwei oder mehrere bisher getrennt dargestellte Datensätze nunmehr in einem Datensatz dargestellt werden, das **Vervielfältigen,** als Vorgang, bei dem die Daten auf demselben oder einem anderen Datenträger unverändert nochmals festgehalten werden, das **Abfragen**, das **Ausgeben** etwa durch Darstellung auf einem Bildschirm oder durch Ausdrucke, das **Benützen** in Form einer konventionellen Nutzung der Daten oder auch durch automationsunterstützten Zugriff, das **Überlassen,** als Weitergabe von Daten vom Auftraggeber an einen Dienstleister, das **Sperren,** als Verhinderung des Zugriffes auf die Daten für eine oder mehrere Personen, das **Löschen,** als Verhinderung des Zugriffes auf die Daten für alle Personen, das **Vernichten** sowie **jede andere Art** der **Handhabung von Daten** einer Datenanwendung durch den Auftraggeber oder Dienstleister.[55] Das **Übermitteln von Daten** ist dagegen **nicht im Verarbeitungsbegriff inkludiert**, weil dafür andere Zulässigkeitsvoraussetzungen zu prüfen sind.[56]

---

[54] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 63.
[55] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 122.
[56] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 63.

9. Das Übermitteln von Daten - § 4 Z 12 DSG 2000

Das Übermitteln von Daten erfasst die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten und darüber hinaus auch die Verwendung von Daten für ein anderes Aufgabengebiet des Auftraggebers.

Unter **Aufgabengebiet** ist eines von mehreren Tätigkeitsfeldern eines Auftraggebers zu verstehen, das **in seinem Umfang** nach der Verkehrsauffassung **geeignet ist, für sich alleine den gesamten Geschäftsbereich eines Auftraggebers zu bilden**.[57] Es ist nach dem Zweck, den der Auftraggeber mit der Datenverarbeitung verfolgt, zu bestimmen.[58]

Die Daten dürfen nur bei Erfüllung der in den §§ 6 ff DSG 2000 vorgesehenen Voraussetzungen für einen anderen Aufgabenbereich, als jenen, für den die Verarbeitung ursprünglich erfolgt ist, verwendet werden. Die **Übermittlung** kann auch **durch** Verwendungsänderung im Bereich des Auftraggebers und der anschließenden **Weiterverwendung für ein anderes Aufgabengebiet durch ein- und dieselbe Person** erfolgen.

Auch die **Weitergabe automationsunterstützt verarbeiteter Daten in konventioneller Form** stellt eine **Übermittlung** dar. Dies kann bspw durch Ausdrucke geschehen. Die neuerliche Weitergabe der konventionell übermittelten Daten fällt aber nur dann unter die Begriffsbestimmung der Datenübermittlung, wenn der erste Empfänger die Daten vor der Weitergabe automationsunterstützt verarbeitet.[59]

10. Die Zustimmung - § 4 Z 14 DSG 2000

Unter einer Zustimmung nach dem DSG 2000 ist die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen zu verstehen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt.

Für die Wirksamkeit einer Zustimmung nach § 4 Z 14 DSG 2000 kommt es auf die Freiheit zur Entscheidung an - schon das Bestehen eines Abhängigkeitsverhältnisses kann sie so einschränken, dass die Einwilligung nicht rechtswirksam ist.[60] Die Einwilligung muss **nicht unbedingt ausdrücklich und schriftlich** erfolgen. Die Ausdrücklichkeit ist lediglich bei der Verwendung sensibler Daten erforderlich, die Schriftlichkeit spielt für die Frage der Nachweisbarkeit eine Rolle.[61] Schweigen ist aber nur dann eine

---

[57] *Ghali*, Datenschutz (1999), 142.
[58] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 116.
[59] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 123.
[60] *Drobesch/Grosinger,* Das neue österreichische Datenschutzgesetz (2000), 126
[61] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 117.

Zustimmung, wenn dies in Bezug auf eine bestimmte Datenverwendung vereinbart oder gesetzlich vorgesehen wurde.

Wesentlich ist der **Bezug der Einwilligung auf einen konkreten Verwendungsfall**. Dem Betroffenen müssen **Zweck, Auftraggeber und Umfang der Datenverwendung** klar sein. Zukünftige Verwendungen müssen daher konkretisierbar sein.[62] Abstrakte Ermächtigungen ohne konkreten Sachverhaltsbezug sind unzulässig. Eine **unrichtige oder unvollständige Information** des Betroffenen durch den Auftraggeber **macht die Einwilligung unwirksam**. Ob die Zustimmung gesondert oder im Zusammenhang mit anderen rechtlichen Vorgängen erteilt wird, ist unwesentlich. Sie kann jederzeit widerrufen werden.[63]

[62] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 34.
[63] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 125.

IV. Die Verarbeitung und Übermittlung von Daten im DSG 2000

Die Zulässigkeit der Verarbeitung und Übermittlung von Daten unterliegt einer mehrstufigen Prüfung, die sich aus den §§ 6 – 9 DSG 2000 ergibt.

A. § 7 Abs 3 DSG 2000

> *Die Zulässigkeit einer **Datenverwendung** setzt voraus, dass die dadurch verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den gelindesten zur Verfügung stehenden Mitteln erfolgen und dass die Grundsätze des § 6 DSG 2000 eingehalten werden.*

Damit wird der **Verhältnismäßigkeitsgrundsatz** hinsichtlich der zulässigen Eingriffe in das Grundrecht auf Datenschutz nochmals ausdrücklich festgehalten.[64]

B. § 6 DSG 2000

§ 6 DSG 2000 umschreibt die allgemeinen Grundsätze der Zulässigkeit der Verwendung von Daten, die vor allem bei der Auslegung der ihm nachfolgenden Bestimmungen des DSG 2000 bedeutsam sind.

1. Treu und Glauben und rechtmäßige Weise - § 6 Abs 1 Z 1 DSG 2000

> *Daten dürfen nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden.*

Kennt der Betroffene die **Umstände des Datengebrauchs** sowie das **Bestehen und die Durchsetzbarkeit seiner Rechte**, liegt eine **Verwendung von Daten nach Treu und Glauben** vor. Wird er dagegen über diese Umstände und Rechte in die Irre geführt oder im Unklaren gelassen, ist dies nicht mehr der Fall.

Zur näheren Festlegung dessen, was in einzelnen Bereichen als Verwendung von Daten nach Treu und Glauben anzusehen ist, besteht gem § 6 Abs 4 DSG 2000 im privaten Bereich die Möglichkeit Verhaltensregeln

[64] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 68.

festzulegen. Die rechtliche Qualität solcher **„Datenschutz-Verhaltensregeln“** ist fraglich. Aus dem Wortlaut der Gesetzesbestimmung lässt sich zu dieser Frage nichts gewinnen. Berufsrechtliche Vorschriften, die zur Erlassung von Standes- oder Verhaltensregeln im Rahmen der Selbstverwaltung als Satzung ermächtigen, könnten bspw dafür herangezogen werden. Die inhaltliche Determinierung müsste dem DSG 2000 entnommen werden. Verhaltensregeln, die ohne eine derartige Ermächtigung erlassen würden, hätten dagegen keinen rechtlich verbindlichen Charakter, sondern würden als Empfehlungen Interpretationshilfe leisten.[65] Die Praxis hat von dieser Möglichkeit noch keinen Gebrauch gemacht. Es **existieren derzeit keine solche Verhaltensregeln** gem § 6 Abs 4 DSG 2000.

Um von einer Verwendung der Daten auf rechtmäßige Weise sprechen zu können, muss der **Auftraggeber eine ausreichende rechtliche Befugnis bzw Zuständigkeit** für die Art der Benützung von Daten, die er mit seiner Datenanwendung bezweckt, besitzen.[66]

2. Zweckbeschränkung - § 6 Abs 1 Z 2 und 3 DSG 2000

Daten dürfen nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden („Wesentlichkeitsgrundsatz“).

Jeder Zweckwechsel ist eine **Übermittlung** iSd § 4 Z 12 DSG 2000, die einer besonderen rechtlichen Grundlage bedarf und nur unter den Voraussetzungen des § 7 Abs 2 und 3 DSG 2000 zulässig ist. Unklare Verarbeitungszwecke gehen zu Lasten des Auftraggebers.[67] Die Daten müssen für den Zweck der Datenanwendung wesentlich sein und dürfen über ihn nicht hinausgehen.[68] So soll insbesondere keine Ballastinformation für einen allfälligen noch nicht vorhersehbaren Bedarf angehäuft werden, denn die **Vorratsbeschaffung von Daten** ist **unzulässig**.[69]

3. Sachliche Richtigkeit - § 6 Abs 1 Z 4 DSG 2000

Daten dürfen nur so verwendet werden, dass sie im Hinblick auf den Verwendungszweck im Ergebnis sachlich richtig und, wenn nötig, auf den neuesten Stand gebracht sind.

Die sachliche Richtigkeit der Daten ist im Hinblick auf den deklarierten Zweck der Datenanwendung gefordert. So sollte bei Datensammlungen klar erkennbar sein, welches **Ausmaß an objektiver Richtigkeit** die gespeicherten Daten voraussichtlich besitzen. Eine regelmäßige Überprüfung auf Aktualität

---

[65] *Holoubek/Potacs*, Öffentliches Wirtschaftsrecht Band 1, 2002, 258.
[66] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 66.
[67] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 39.
[68] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 130.
[69] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 40.

wird besonders wichtig sein, um ungerechtfertigte Nachteile für Betroffene zu vermeiden.[70]

4. Datenaufbewahrung - § 6 Abs 1 Z 5 DSG 2000

Daten dürfen so lange in personenbezogener Form aufbewahrt werden, als dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist. Eine längere Aufbewahrungsdauer kann sich aus besonderen gesetzlichen, insbesondere archivrechtlichen Vorschriften ergeben.

5. Auftraggeberverantwortung für Datenanwendungen - § 6 Abs 2 und 3 DSG 2000

Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der genannten Grundsätze, dies gilt auch dann, wenn er für die Datenanwendung Dienstleister heranzieht.

C. § 7 Abs 1 DSG 2000

*Daten dürfen nur **verarbeitet** werden, soweit Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen des jeweiligen Auftraggebers gedeckt sind und die schutzwürdigen Geheimhaltungsinteressen der Betroffenen nicht verletzen.*

Die Zulässigkeit einer konkreten Datenanwendung beruht auf der **Berechtigung des Auftraggebers** und der **Berücksichtigung der schutzwürdigen Interessen der Betroffenen**.

1. Die Berechtigung des Auftraggebers

Maßgebend für die Berechtigung des Auftraggebers ist, ob Zweck und Inhalt der Datenanwendung von den gesetzlichen Zuständigkeiten oder seinen rechtlichen Befugnissen gedeckt sind. Solche ergeben sich aus den **individuellen Berechtigungen** in Verbindung mit den ihnen zugrunde liegenden rechtlichen Vorgaben wie zB aus Regelungen über die Ausübung bestimmter Berufe, dem Gesellschaftsvertrag, Gewerbeschein oder der Vereinssatzung.[71]

---

[70] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 66.
[71] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 42.

2. Schutzwürdige Geheimhaltungsinteressen

a) Nicht sensible Daten - § 8 DSG 2000

Das Vorliegen oder Nichtvorliegen schutzwürdiger Geheimhaltungsinteressen bei nicht sensiblen Daten ist in § 8 Abs 1 DSG 2000 in einer Generalklausel in vier näheren Umschreibungen geregelt. Die Absätze 2 bis 4 nennen Beispiele, in denen keine solche Geheimhaltungsinteressen verletzt sind.

aa) § 8 Abs 1 DSG 2000

> *Gemäß § 1 Abs 1 bestehende schutzwürdige Geheimhaltungsinteressen sind bei Verwendung nicht-sensibler Daten dann nicht verletzt, wenn*
>
> *1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder*
>
> *2. der Betroffene der Verwendung seiner Daten zugestimmt hat, wobei ein Widerruf jederzeit möglich ist und die Unzulässigkeit der weiteren Verwendung der Daten bewirkt, oder*
>
> *3. lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder*
>
> *4. überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern.*

Eine ausdrückliche gesetzliche Ermächtigung zur Datenverwendung – aus dem Gemeinschaftsrecht oder auch dem innerstaatlichen Recht[72] - muss jede ihrer Komponenten erfassen und auch die zugelassenen Daten ausdrücklich bezeichnen. So müssen **dem Gesetz die Datenarten, Betroffenen- und Empfängerkreise zu entnehmen sein**. Dies erfordert ein hohes Reglungsniveau und detaillierte Angaben. Wird dieses nicht erreicht, muss sich die Datenverwendung auf § 8 Abs 3 Z 1 DSG 2000 stützen.[73]

Eine **erteilte Zustimmung** kann **nicht rückwirkend widerrufen werden**, weshalb eine bereits erfolgte Datenverwendung durch den Widerruf nicht unzulässig wird.[74]

Demonstrative Beispiele für zweifelsfrei überwiegende berechtigte Interessen eines Auftraggebers oder Dritten gibt § 8 Abs 3 DSG 2000. Nicht genannte Sachverhalte sind unter Heranziehung der genannten Tatbestände zu beurteilen.

---

[72] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 45.
[73] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 138.
[74] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 46.

bb) § 8 Abs 2 DSG 2000

> *Bei der Verwendung von zulässigerweise veröffentlichten Daten oder von nur indirekt personenbezogenen Daten gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt. Das Recht, gegen die Verwendung solcher Daten gemäß § 28 DSG 2000 Widerspruch zu erheben, bleibt unberührt.*

Die Gefahr der Verletzung schutzwürdiger Geheimhaltungsinteressen ist in diesen Fällen nicht mehr gegeben oder stark reduziert, weshalb kein Geheimhaltungsanspruch mehr besteht. Dies entspricht § 1 Abs 1 letzter Satz DSG 2000, der das Bestehen eines Geheimhaltungsinteresses schon bei einer **allgemeinen Verfügbarkeit der Daten** verneint und so über § 8 Abs 2 DSG 2000 hinausgeht. **Unerheblich** ist dagegen, **wer die Veröffentlichung durchgeführt hat**.[75]

Dennoch ist bei allen Datenanwendungen, die solche Daten enthalten zu fragen, ob sie ausschließlich veröffentlichte Daten oder nicht auch zusätzliche, durch Auswertung der veröffentlichten Daten gewonnene Daten enthalten, die ihrerseits noch nicht veröffentlicht wurden.[76]

Fraglich ist, wie bei indirekt personenbezogenen Daten die Legitimation zur Erhebung des Widerspruches überprüft werden soll.[77]

cc) § 8 Abs 3 DSG 2000

> *Schutzwürdige Geheimhaltungsinteressen sind aus dem Grunde des § 8 Abs 1 Z 4 DSG 2000 insbesondere dann nicht verletzt, wenn die Verwendung der Daten*
>
> *1. für einen Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder*
>
> *2. durch Auftraggeber des öffentlichen Bereichs in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder*
>
> *3. zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder*
>
> *4. zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich ist oder*
>
> *5. zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder*
>
> *6. ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat.*

---

[75] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 140.
[76] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 70.
[77] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 48.

Es handelt sich hierbei um eine **demonstrative Aufzählung zulässiger Eingriffe** im Sinne des § 1 Abs 2 DSG 2000. Die Aufzählung beschränkt sich auf Falltypen, bei welchen die **Verletzung schutzwürdiger Geheimhaltungsinteressen immer auszuschließen ist**. Nicht aufgenommen in die Aufzählung wurden daher Verwendungskonstellationen, in denen im Einzelfall eine Beurteilung notwendig ist.[78]

Verwaltungsökonomische Gründe rechtfertigen bereits dann die automationsunterstützte Verwendung der Daten, wenn sie wesentlich zur Erfüllung der Vollzugsaufgabe benötigt werden.

Die Verpflichtung zur **Amtshilfe** betrifft die Pflicht zur Datenübermittlung, die allerdings nur auf Ersuchen erfolgen darf.[79] Auf internationaler Ebene ist auf das Auslieferungs- und Rechtshilfegesetz und das Polizeikooperationsgesetz zu verweisen.

Da die Datenverwendung zur Erfüllung der **vertraglichen Verpflichtung** erforderlich sein muss, reicht ein bloßes Nützlichsein nicht aus, die Erforderlichkeit zur Erfüllung einer Nebenvereinbarung dagegen schon.

Die **Rechtsansprüche** des Auftraggebers können sowohl solche des Öffentlichen als auch des Privatrechts sein.[80]

dd) § 8 Abs 4 DSG 2000

> *Die Verwendung von 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 verstößt – unbeschadet der Bestimmungen des § 8 Abs 2 DSG 2000 – nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn*
>
> *1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten sowohl im öffentlichen als auch im privaten Bereich besteht oder*
>
> *2. die Verwendung derartiger Daten für Auftraggeber des öffentlichen Bereichs eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder*
>
> *3. sich sonst im privaten Bereich 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.*

---

[78] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 137.
[79] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 47.
[80] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 139.

Strafrechtsbezogene Daten sind zwar keine sensible Daten, werden aber ihre Nähe gerückt. Die Verarbeitung muss daher möglichst beschränkt bleiben.[81]

Erfasst sind nicht nur Daten über Verurteilte sondern auch über Tatverdächtige, Beschuldigte und Angeklagte. Es **kommt nicht darauf an, ob alle strafrechtlichen Voraussetzungen** für eine Verurteilung **vorliegen** oder etwa der Betroffene wegen Schuldunfähigkeit nicht verurteilt werden kann.

Der private Auftraggeber darf strafrechtsbezogene Daten nur verwenden, wenn es ihm möglich ist, bei ihrer Handhabung auf die **Betroffeneninteressen besonders Bedacht zu nehmen** – so zB durch besonders vertrauliche Behandlung oder möglichst kurze Verarbeitungsdauer. Berechtigte Interessen des Auftraggebers werden aber bspw bei der Anwerbung für bestimmte berufliche Tätigkeiten, die eine besondere Vertrauenswürdigkeit des Bewerbers und daher den Nachweis seiner Unbescholtenheit fordern, bestehen.

Eine **Zustimmungsmöglichkeit des Betroffenen** zur Verwendung seiner strafrechtsbezogenen Daten ist **nicht ausdrücklich vorgesehen**. Ihre Zulässigkeit wird aber aus § 1 Abs 2 DSG 2000 abzuleiten sein.[82]

b) Sensible Daten - § 9 DSG 2000

In § 9 DSG 2000 sind die neben dem **grundsätzlichen Verwendungsverbot** zulässigen Verwendungsfälle sensibler Daten in Form eines **taxativen Katalogs** geregelt.

> *Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung sensibler Daten ausschließlich dann nicht verletzt, wenn*
>
> *1. der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder*
>
> *2. die Daten in nur indirekt personenbezogener Form verwendet werden oder*
>
> *3. sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen, oder*
>
> *4. die Verwendung durch Auftraggeber des öffentlichen Bereichs in Erfüllung ihrer Verpflichtung zur Amtshilfe geschieht oder*
>
> *5. Daten verwendet werden, die ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand haben, oder*
>
> *6. 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, oder*
>
> *7. die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder*

---

[81] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 70.

[82] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 141.

8. die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder

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

10. Daten für private Zwecke gemäß § 45 oder für wissenschaftliche Forschung oder Statistik gemäß § 46 oder zur Benachrichtigung oder Befragung des Betroffenen gemäß § 47 verwendet werden oder

11. die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers auf dem Gebiet des Arbeits- oder Dienstrechts Rechnung zu tragen, und sie nach besonderen Rechtsvorschriften zulässig ist, wobei die dem Betriebsrat nach dem Arbeitsverfassungsgesetz zustehenden Befugnisse zur Datenverwendung unberührt bleiben, oder

12. die Daten zum Zweck der Gesundheitsvorsorge, der medizinischen Diagnostik, der Gesundheitsversorgung oder –behandlung oder für die Verwaltung von Gesundheitsdiensten erforderlich ist, und die Verwendung dieser Daten durch ärztliches Personal oder sonstige Personen erfolgt, die einer entsprechenden Geheimhaltungspflicht unterliegen, oder

13. nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten und es sich hierbei um Daten von Mitgliedern, Förderern oder sonstigen Personen handelt, die regelmäßig ihr Interesse für den Tätigkeitszweck der Vereinigung bekundet haben; diese Daten dürfen, sofern sich aus gesetzlichen Vorschriften nichts anderes ergibt, nur mit Zustimmung der Betroffenen an Dritte weitergegeben werden.

Im Gegensatz zu § 8 DSG 2000 muss die **Veröffentlichung der Daten** nach Z 1 **durch den Betroffenen selbst** erfolgt sein. Dies muss auch außer Zweifel stehen. Sie kann in öffentlichen Registern, Teilnehmerverzeichnissen, durch Presseaussendungen oder im Internet erfolgen.[83]

Eine **gesetzliche Ermächtigung oder Verpflichtung** nach Z 3 muss die Art der sensiblen Daten und Umstände ihrer Verwendung nicht ausdrücklich festlegen, wie etwa in § 8 Abs 1 Z 1 DSG 2000. Entscheidend ist lediglich, ob aus der Rechtsvorschrift die Verwendung sensibler personenbezogener Daten bei ihrem Vollzug und ihre Erforderlichkeit im konkreten Fall zur Erfüllung der bestimmten gesetzlich übertragenen Aufgaben abgeleitet werden kann. Zu den wichtigen **öffentlichen Interessen** zählt in diesem Zusammenhang bspw die Aufsicht über bestimmte Wirtschaftszweige, wie etwa die Banken- oder

[83] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 144.

Versicherungsaufsicht. Gesetze, die die Verwendung von Daten für Zwecke einer besonderen Wirtschaftsaufsicht vorsehen, erfüllen somit ein wichtiges öffentliches Interesse.[84] Der Erwägungsgrund 34 der EG-Datenschutzrichtlinie, 95/46/EG, sieht ein wichtiges öffentliches Interesse auch in der Gewährung von sozialer Sicherheit - hinsichtlich der Sicherung von Qualität und Wirtschaftlichkeit der Verfahren zur Abrechnung von Leistungen in den sozialen Krankenversicherungssystemen - weiters von wissenschaftlicher Forschung und öffentlicher Statistik.

Die **Einwilligung** nach Z 6 muss ausdrücklich erteilt werden und den Anforderungen des § 4 Z 14 DSG 2000 entsprechen.[85]

Während vor der Verwendung sensibler Daten im **lebenswichtigen Interesse** des Betroffenen nach Z 7 zu prüfen ist, ob nicht seine Zustimmung eingeholt werden kann, entfällt diese Vorprüfung bei der Datenverwendung im lebenswichtigen Interesse eines Dritten nach Z 8.[86]

Nach Z 9 ist die Verwendung sensibler Daten zur **Rechtsverteidigung** - sowohl hinsichtlich des Öffentlichen als auch des Privatrechts - bereits im Vorfeld einer gerichtlichen Auseinandersetzung zulässig.[87]

Die **arbeits- oder dienstrechtlichen Rechte und Pflichten des Auftraggebers** können sich aus Einzelverträgen, kollektivvertraglichen bzw betrieblichen Vereinbarungen oder einzelstaatlichen oder gemeinschaftlichen Rechtsvorschriften ergeben. Die Zulässigkeit der Datenverwendung muss vergleichbar Z 3 aus besonderen Rechtsvorschriften abgeleitet werden können.[88]

Die Regelung der Z 12 erfasst grundsätzlich die Verwendung von **Gesundheitsdaten** und anderen sensiblen Daten, sofern diese unmittelbar mit den genannten medizinischen Fachaufgaben zusammenhängen. Der Gesundheitsversorgung dienen auch Apotheken, Patientendateien dienen der Verwaltung von Gesundheitsdiensten.

Eine Vereinigung iSd Z 13 ist nicht nur ein **ideeller Verein**, sondern auch eine andere **Organisation, soferne sie nicht auf Gewinn gerichtet ist**. Abzustellen ist daher auf die Verfolgung von Profitinteressen. In Betracht zu ziehen sind auch Kapitalgesellschaften, die ideelle Zwecke verfolgen, Parteien nach dem Parteiengesetz, gesetzlich anerkannte Kirchen und Religionsgesellschaften und religiöse Bekenntnisgemeinschaften. Ihr Tätigkeitszweck grenzt die zulässigerweise verwendbaren sensiblen Daten ab. Für Übermittlungen ist in diesem Zusammenhang die Einwilligung der Betroffenen nötig. Die organisationsinterne Datenverwendung ist dagegen auch ohne eine solche zulässig.[89]

---

[84] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 72.
[85] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 52.
[86] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 145.
[87] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 143.
[88] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 146.
[89] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 53.

D. § 7 Abs 2 DSG 2000

Daten dürfen nur übermittelt werden, wenn

1. sie aus einer gemäß § 7 Abs 1 DSG 2000 zulässigen Datenanwendung stammen und

2. der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis – soweit diese nicht außer Zweifel steht – im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und

3. durch Zweck und Inhalt der Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

1. § 7 Abs 2 Z 1 DSG 2000

Stammen die zu übermittelnden Daten gemäß § 7 Abs 1 und Abs 3 DSG 2000 aus einer zulässigen Datenanwendung, so ist auch ihre Übermittlung rechtmäßig. Sind die Daten **im Übermittlungszeitpunkt nicht rechtmäßig verarbeitet**, ist **jede Übermittlung rechtswidrig**.[90]

2. § 7 Abs 2 Z 2 DSG 2000

Der Übermittler hat bei Übermittlungen über Ersuchen zu beurteilen, ob das Informationsbedürfnis des Ersuchenden in dessen gesetzlichen Zuständigkeit oder rechtlichen Befugnis zur Verarbeitung der Daten im Hinblick auf den Übermittlungszweck Begründung findet. Ergibt sich dies nicht schon aus der Zweckangabe, so hat sie der Ersuchende glaubhaft zu machen.

Bei Übermittlungen ohne Ersuchen hingegen dürfen beim Übermittler keine Zweifel über das Vorliegen dieser Umstände bestehen.[91]

Anonyme Übermittlungen sind grundsätzlich unzulässig, da der Auftraggeber seine Identität in geeigneter Weise offen zu legen hat (vgl IV. E.). Den Betroffenen soll dadurch die Wahrung ihrer Rechte ermöglicht werden. In jenen Fällen, in denen keine Registernummer geführt wird, weil es sich nicht um meldepflichtige Datenanwendungen handelt, wird dies bedeuten müssen, dass Name und Anschrift des Auftraggebers anzuführen sind. Die bloße Verwendung von Postfächern oder Telefonnummern kann dagegen nicht ausreichen.[92] Lediglich wenn berechtigte Gründe für die Geheimhaltung der übermittelnden Stelle die Interessen der Betroffenen auf Ausübung ihrer Rechte nach dem DSG 2000 überwiegen, sind anonyme Übermittlungen zulässig.[93]

---

[90] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 134.
[91] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 134.
[92] *Jahnel*, Das Datenschutzgesetz 2000, WBl 2000, 49.
[93] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 135.

3. § 7 Abs 2 Z 3 DSG 2000

Unter Zugrundelegung von Zweck und Inhalt der Übermittlung ist abschließend eine Interessensabwägung hinsichtlich der schutzwürdigen Geheimhaltungsinteressen des Betroffenen vorzunehmen (vgl IV. C. 2.).

E. Die Informationspflicht des Auftraggebers

Um dem Betroffenen die Wahrnehmung seiner Rechte zu erleichtern und zur Beachtung der Grundsätze der Datenverarbeitung nach Treu und Glauben, trifft den Auftraggeber die Informationspflicht nach § 24 DSG 2000, die spezielle Regelungen für die Übermittlung von Daten beinhaltet. Je nach konkreter Ausgestaltung der Datenübermittlung ist einerseits eine Erweiterung andererseits eine Einschränkung der Informationspflicht vorgesehen.

Er hat dieser **Informationspflicht aus eigenem** nachzukommen, ohne dass der Betroffene darum ersuchen muss.[94] Der **Betroffene hat keinen durchsetzbaren Rechtsanspruch** auf die Erfüllung der Informationspflicht.[95]

Sie darf nicht als Verdoppelung der Meldepflicht in dem Sinn verstanden werden, dass eine zweiten Meldung an den Betroffenen zu erfolgen hat. Der Betroffene soll lediglich darauf hingewiesen werden, dass seine Daten von einem bestimmten Auftraggeber für einen bestimmten Zweck verarbeitet werden sollen.[96]

Oft ist die Beurteilung eines komplexen Sachverhaltes nötig, um den richtigen Umfang der Information festzulegen. Es kann daher sinnvoll sein, ihr Ausmaß in einzelnen typischen Situationen durch Verhaltensregeln nach § 6 Abs 4 DSG 2000 zu klären (vgl IV. B. 1.).[97]

1. § 24 Abs 1 DSG 2000

> *Der Auftraggeber einer Datenanwendung hat aus Anlass der Ermittlung von Daten die Betroffenen in geeigneter Weise*
>
> *1. über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und*
>
> *2. über Namen und Adresse des Auftraggebers, zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen.*

Ob der Betroffene über diese Information bereits verfügt, ist in der **konkreten jeweiligen Situation** zu überprüfen.[98] Die Mitteilung der

---

[94] *Ghali*, Datenschutz (1999), 176.
[95] *Holoubek/Potacs*, Öffentliches Wirtschaftsrecht Band 1, 2002, 264.
[96] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 91.
[97] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 194.
[98] *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 91

Information in geeigneter Weise setzt **keine bestimmte Form** voraus. Sie hat schriftlich oder mündlich **anlässlich der Datenermittlung** zu erfolgen. Auf den Zeitpunkt der Datenspeicherung kommt es dagegen nicht an.[99]

2. § 24 Abs 2 DSG 2000

Über Abs 1 hinausgehende Informationen sind in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist; dies gilt insbesondere dann, wenn

1. gegen eine beabsichtigte Verarbeitung oder Übermittlung von Daten ein Widerspruchsrecht des Betroffenen gemäß § 28 besteht oder

2. es für den Betroffenen nach den Umständen des Falles nicht klar erkennbar ist, ob er zur Beantwortung der an ihn gestellten Fragen rechtlich verpflichtet ist, oder

3. Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne dass dies gesetzlich vorgesehen ist.

Eine **über Zweck, Name und Adresse des Auftraggebers hinausgehende Information** des Betroffenen ist **bei der Übermittlung von Daten** notwendig, wenn dies **für eine Verarbeitung nach Treu und Glauben erforderlich ist** und dem Betroffenen gegen die Übermittlung ein **Widerspruchsrecht nach § 28 DSG 2000 zusteht**, wonach jeder Betroffene das Recht hat, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen, Widerspruch zu erheben, sofern die Datenverwendung nicht gesetzlich vorgesehen ist.

Das Widerspruchsrecht hängt grundsätzlich von der **subjektiven Situation des Betroffenen** ab. Seine überwiegenden schutzwürdigen Interessen müssen sich aus einer besonderen, individuellen Situation ergeben.[100] Das kann dazu führen, dass der Auftraggeber über das Bestehen eines Widerspruchsrechtes informieren muss, ohne die spezielle Befindlichkeit des Betroffenen und somit die Berechtigung zum Widerspruch zu kennen.[101]

3. § 24 Abs 3 DSG 2000

Werden Daten nicht durch Befragung des Betroffenen, sondern durch Übermittlung von Daten aus anderen Aufgabengebieten desselben Auftraggebers oder aus Anwendungen anderer Auftraggeber ermittelt, darf die Information gemäß Abs. 1 entfallen, wenn

1. die Datenverwendung durch Gesetz oder Verordnung vorgesehen ist oder

---

[99] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 196.
[100] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 108.
[101] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 93.

2. die Information im Hinblick auf die mangelnde Erreichbarkeit von Betroffenen unmöglich ist oder

3. wenn sie angesichts der Unwahrscheinlichkeit einer Beeinträchtigung der Betroffenenrechte einerseits und der Kosten der Information aller Betroffenen andererseits einen unverhältnismäßigen Aufwand erfordert. Dies liegt insbesondere dann vor, wenn Daten für Zwecke der wissenschaftlichen Forschung oder Statistik gemäß § 46 oder Adressdaten im Rahmen des § 47 ermittelt werden und die Information des Betroffenen in diesen Bestimmungen nicht ausdrücklich vorgeschrieben ist. Der Bundeskanzler kann durch Verordnung weitere Fälle festlegen, in welchen die Pflicht zur Information entfällt.

Ausnahmsweise darf bei der Übermittlung von Daten die Informationspflicht entfallen.

Besteht eine **ausdrückliche gesetzliche Regelung einer Datenverwendung,** erübrigt sich eine gleichgerichtete Information des Betroffenen.[102]

Die **absolute Unmöglichkeit der Erreichbarkeit eines Betroffenen** wird nur in seltenen Fällen nachgewiesen werden können.[103] Seine Information ist aber insbesondere dann unmöglich, wenn der **Auftraggeber keine ausreichenden Informationsdaten hat**, um ihm die Information zukommen zu lassen. Es trifft ihn dadurch weder die Pflicht noch das Recht, die fehlenden Daten eigens für diesen Zweck zu erheben und zu verarbeiten, weil dadurch neue Risiken geschaffen würden.[104]

Auch nicht ausdrücklich geregelte Sachverhalte mangelnder Erreichbarkeit (Ansprechbarkeit) des Betroffenen wie zB bei der Ermittlung medizinischer Daten bei Bewusstlosigkeit des Patienten rechtfertigen bzw erfordern den Entfall der Informationspflicht.[105]

Die Mitteilung der Information darf schließlich auch entfallen, wenn einzelne Betroffene nur mit **unverhältnismäßigem Aufwand** erreicht werden können oder wenn die Ausforschung wegen der Größe des Betroffenenkreises nur mit unverhältnismäßigem Aufwand möglich wäre.[106]

Die Interessenabwägung zur Feststellung der Unverhältnismäßigkeit des Informationsaufwandes macht eine eindeutige Beurteilung des Bestehens der Informationspflicht im Einzelfall sehr schwierig.[107]

---

[102] *Holoubek/Potacs*, Öffentliches Wirtschaftsrecht Band 1, 2002, 264.
[103] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 267.
[104] *Ghali*, Datenschutz (1999), 177.
[105] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 94.
[106] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 267.
[107] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 94.

V. Die Einordnung des Data-Minings in das DSG 2000

Data-Mining-Prozesse arbeiten mit Informationen über natürliche und juristische Personen oder sonstige Personengemeinschaften. Ziel und Zweck ist die Auswertung von einem oder mehreren ursprünglich für einen ganz bestimmten Zweck angelegten Datenbeständen für einen neuen Zweck. Bisher unbekannte Beziehungen zwischen den Daten und verborgene Informationen sollen aufgedeckt und verwertet werden.

A. Qualifizierung der Daten

Das DSG 2000 erfasst uneingeschränkt automationsunterstützt verwendete Daten. Manuell verwendete Dateien gelten als solche, soweit sie für Zwecke solcher Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist.[108]

Soweit es sich bei den Daten, die die Basis für Data-Mining-Prozesse bilden, um **anonymisierte Daten** handelt, liegt bei ihrer Verwendung kein Tatbestand vor, der unter das Datenschutzrecht fällt. Anonymisierte Data-Mining-Prozesse sind daher auf den ersten Blick **datenschutzrechtlich unbedenklich**. Probleme können allerdings selbst in diesem Zusammenhang auftauchen, wenn Muster, die aus einem Data-Mining-Prozess stammen, auch ohne konkreten Personenbezug **aufgrund objektiver Kriterien zu Benachteiligungen führen**.[109] Nach § 49 DSG 2000 darf niemand einer automatisierten Einzelentscheidung unterworfen werden. Für derartige Entscheidungen könnten aber gerade auch die Ergebnisse eines anonymisierten Data-Mining-Prozesses zum Zweck der Bewertung einzelner Aspekte der Personen herangezogen werden.

Bilden **personenbezogene** oder auch nur **indirekt personenbezogene Daten** die Basis des Data-Mining-Prozesses, ist dagegen die erste Voraussetzung für die Anwendbarkeit des DSG 2000 erfüllt. Customer Relationship Management bspw wird nur aufgrund der Auswertung personenbezogener Daten möglich sein.

---

[108] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.
[109] http://www.akwien.at/396_11161.htm.

B. Der Auftraggeber

Wer im Einzelfall der Auftraggeber der Datenverarbeitung bzw des konkreten Data-Mining-Prozesses ist, ist aufgrund der Definition des § 4 Z 4 DSG 2000 zu prüfen. Wesentlich ist, dass jener Auftraggeber ist, der die Verarbeitung der Daten steuert, der die **tatsächliche Entscheidung** darüber trifft, Daten für einen bestimmten Zweck zu verarbeiten oder dies nicht zu tun, sei es unmittelbar, sei es unter Heranziehung eines Dienstleisters.

C. Verwendungskategorie der Daten

Ziel des Data-Minings ist die Erlangung neuer Erkenntnisse und neuen Wissens aus bestehenden Datenbanken. Die Daten werden zu diesem Zweck geordnet, verglichen, verknüpft, abgefragt, ausgegeben. Sie werden also jedenfalls „**verarbeitet**".

Diese Datenverarbeitung erfolgt aber zu einem ***neuen Zweck*** als die ursprüngliche Datenermittlung. Sowohl die als Basis dienenden Daten als auch die gewonnenen Erkenntnisse und Wissen sollen ökonomisch weiterführend genutzt werden. Dies kann nur durch ihre **„Weitergabe"** erfolgen – innerhalb der Organisation des Auftraggebers, der über die Ursprungsdatenbank verfügt, an außenstehende Dritte oder durch Veröffentlichung.

Die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister erfüllt die Voraussetzungen einer **Datenübermittlung** gemäß § 4 Z 12 DSG 2000. Gleiches gilt für die Verwendung der Daten für ein anderes Aufgabengebiet des Auftraggebers.

1. Andere Empfänger

Die Weitergabe von Daten im Konzern an rechtlich selbständige Tochterunternehmen stellt bspw eine Übermittlung dar.[110] Unstrittig ist dies auch bei völlig unabhängigen Dritten, die erst als Übermittlungsempfänger mit dem Auftraggeber, der über Erkenntnisse aus einer unter seiner Verantwortung geführten Datenanwendung verfügt, in Verbindung treten.

2. Andere Aufgabengebiete

Ein Aufgabengebiet ist eines von mehreren Tätigkeitsfeldern, das in seinem Umfang nach der Verkehrsauffassung geeignet ist, für sich allein den gesamten Geschäftsbereich eines Auftraggebers zu bilden (vgl. III. A. 9.).

---

[110] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.

Zur Frage der Ausgestaltung der **näheren Abhängigkeit von Tätigkeiten**, um sie als ein Aufgabengebiet qualifizieren zu können, existieren verschiedene Meinungen. Während eine Meinung[111] einen **engen tatsächlichen und wirtschaftlichen Zusammenhang** der Tätigkeiten fordert und als Beispiel für ein einheitliches Aufgabengebiet den Umfang einer Gewerbeberechtigung oder eines Kompetenztatbestandes im Sinne der Art 10 bis 15 B-VG nennt, ist nach anderer Meinung[112] auch noch bei einem zusammengehörenden Bündel von Gewerbeberechtigungen desselben Auftraggebers von einem Aufgabengebiet auszugehen. Dies wird damit begründet, dass nicht verlangt werden könne, dass in bestimmten Berufssparten, die etwa für den Verkauf und die Reparatur gesonderte Gewerbeberechtigungen benötigen, für die Verwaltung der Kundenadressen jeweils gesonderte Aufgabengebiete bestehen bzw getrennte Datenanwendungen einzurichten seien.

Meiner Meinung nach darf darin aber gerade kein Grund für die Einheitlichkeit der Aufgabengebiete liegen. Müssen die datenschutzrechtlichen Vorschriften hinsichtlich eines Aufgabengebietes und der dazu gehörenden Kundendatenbank eingehalten werden, kann es kein Problem sein, die Einhaltung dieser Vorschriften im gleichen Unternehmen auch hinsichtlich eines zweiten Aufgabengebietes und der dazu gehörenden Kundendatenbank zu gewährleisten. Ziel und Zweck des Datenschutzrechtes würden meiner Meinung nach sonst zu sehr verwässert. Im Vordergrund muss der Schutz des Betroffenen stehen.

Der Betroffene, der einem Rechtsträger Daten für einen bestimmten Tätigkeitsbereich anvertraut hat, muss grundsätzlich nicht damit rechnen, dass diese für Zwecke verwendet werden, die zum ursprünglichen Anlass in keinem engen wirtschaftlichen Zusammenhang stehen. Der Betroffene soll mangels besonderer Vereinbarung nicht gewärtigen müssen, dass diese Daten vornehmlich im Interesse eines Dritten verwendet werden. Vielmehr soll er bei der Ermittlung davon ausgehen können, dass die Daten nur für einen bestimmten Tätigkeitsbereich des Rechtsträgers Verwendung finden.[113] Die Beurteilung der Frage, ob ein enger wirtschaftlicher Zusammenhang zwischen dem Verwendungszweck nach der Übermittlung und dem Anlass des Anvertrauens besteht, muss stets für den Einzelfall anhand der **konkreten Vertragsbeziehung und ihrer wirtschaftlichen Implikationen** erfolgen. Auch unternehmensfremde Interessen an der anderweitigen Verwendung der Daten sind hierbei zu beachten.[114] Wie der OGH in diesem Zusammenhang bspw ausgesprochen hat, sind die Führung von Girokonten und der Abschluss von Bausparverträgen verschiedene „Aufgabengebiete“[115].

---

[111] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.

[112] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 32.

[113] OGH 25. Februar 1992, 4 Ob 114/91 = EDVuR 1992,91 = JBl 1992, 599 = ÖBl 1992, 21 = ÖJZ 1992/58 = RdW 1992, 210.

[114] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.

[115] OGH 25. Februar 1992, 4 Ob 114/91 = EDVuR 1992,91 = JBl 1992, 599 = ÖBl 1992, 21 = ÖJZ 1992/58 = RdW 1992, 210.

Sollen aus ursprünglich zu einem bestimmten Zweck erstellten Datenbanken neue, bisher unbekannte Erkenntnisse gewonnen werden, steht dieses Ziel zum ursprünglichen Anlass in keinem, jedenfalls in **keinem engen wirtschaftlichen Zusammenhang**. Jeder Zweckwechsel führt zur Qualifikation der Datenverwendung als Datenübermittlung. Da der Schutz des Einzelnen in seinem Grundrecht auf Datenschutz im Vordergrund steht, ist die Frage, ob es sich um einheitliche oder "andere" Aufgabengebiete des Auftraggebers handelt, meiner Meinung nach streng zu beurteilen. **Im Zweifel** sollte daher zum Schutz des Betroffenen vom **Vorliegen eines anderen Aufgabengebietes** ausgegangen werden.

Die Frage, ob der Betroffene bereits bei der ursprünglichen Datenermittlung über die später beabsichtigte Zugrundelegung dieser Daten in einem Data-Mining-Prozess informiert wurde, spielt bei der Prüfung der Rechtswirksamkeit seiner Zustimmung zur Übermittlung seiner Daten eine Rolle (vgl VI. D. 4.).

Aus diesen Gründen ist daher die **Zurverfügungstellung bestehender Datensammlungen als Basis für die Aufdeckung von verborgenen und unbekannten Beziehungen durch Data-Mining** unter dem Gesichtspunkt der **Datenübermittlung** zu prüfen.

VI. Die Anwendung des DSG 2000 auf Data-Mining

A. Die Informationspflicht des Auftraggebers § 24 DSG 2000

Bereits bei der Ermittlung der Daten hat der Auftraggeber seine **Informationspflicht** gegenüber den Betroffenen zu erfüllen. Die für die Datenübermittlung wesentlichen Erweiterungen und Einschränkungen der Informationspflicht in dieser Bestimmung sind zu beachten.

B. Die Zulässigkeit der Datenübermittlung § 7 Abs 2 DSG 2000

§ 7 Abs 2 DSG 2000 regelt die Voraussetzungen, unter denen ein Auftraggeber Daten aus einer unter seiner Verantwortung geführten zulässigen Datenanwendung übermitteln darf. Die Bestimmung verleiht **kein subjektives Recht** darauf, **Daten übermittelt zu erhalten**. Den Auftraggeber als Inhaber der Daten trifft die Verantwortung für den Vorgang der Übermittlung.[116]

Eine abschließende Antwort auf die Frage der Zulässigkeit von Data-Mining kann nicht gegeben werden. Es ist vielmehr in jedem konkreten Einzelfall eine Prüfung vorzunehmen, die zum Ergebnis der Zulässigkeit, aber auch der Unzulässigkeit gelangen kann.

Damit Daten zulässig übermittelt werden und so die Basis für Data-Mining-Prozesse bilden können, müssen die Voraussetzungen des § 7 Abs 2 DSG 2000 erfüllt sein. Die Frage, ob die gegenständlichen Daten aus einer **zulässigen Datenanwendung** stammen, ist anhand § 7 Abs 1 und Abs 3 DSG 2000 zu beantworten. Die Daten, die den Data-Mining-Prozessen zugrunde gelegt werden, sind das Ergebnis aus Datenverarbeitungen, die idR völlig unabhängig vom späteren Data-Mining-Prozess erfolgten. Die Zulässigkeit dieser Datenverarbeitungen ist im Einzelfall zu prüfen. Besonderes Augenmerk ist hierbei auf die schutzwürdigen Geheimhaltungsinteressen der Betroffenen zu legen. Auch für diese Datenverarbeitung haben der Grundsatz der Verhältnismäßigkeit sowie die Grundsätze der Datenverwendung nach § 6 DSG 2000 zu gelten.

Im nächsten Schritt hat der Empfänger dem Übermittelnden, der als Auftraggeber der zugrunde liegenden Datenverarbeitung über die Daten verfügt, seine ausreichende **gesetzliche Zuständigkeit oder rechtliche**

[116] DSK vom 4. Juni 2002, K120.673/003-DSK/2002.

Befugnis im Hinblick auf den Übermittlungszweck glaubhaft zu machen. Es existiert keine gesetzliche Bestimmung, die die Übermittlung von Daten zu Zwecken des Data-Minings vorsieht. Die rechtliche Befugnis dazu muss daher den im Einzelfall bestehenden Vereinbarungen – wie zB dem Gesellschaftsvertrag – entnommen werden. Durch den Zweck und den Inhalt der Übermittlung, die meiner Meinung nach zumindest nach den zu erwartenden Ergebnissen des Data-Mining-Prozesses konkretisiert werden müssen, um dem Betroffenen ausreichende Information gewähren zu können, dürfen die **schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden**. Hierfür kommen als wichtigste Ausschließungsgründe die Veröffentlichung der Daten, die Zustimmungserklärung der Betroffenen und die überwiegenden berechtigten Interessen des Auftraggebers oder eines Dritten in Betracht.

Auch für die Datenübermittlung selbst sind der Grundsatz der Verhältnismäßigkeit und die Grundsätze der Datenverwendung nach § 6 DSG 2000 einzuhalten.

Jene Punkte, die in diesem Prüfungsschema im Zusammenhang mit Data-Mining besonders streng zu prüfen sind bzw Probleme aufwerfen können, sollen im Folgenden aufgezeigt werden.

C. Gesetzliche Zuständigkeit oder rechtliche Befugnis des Auftraggebers bzw Empfängers

Der Auftraggeber der ursprünglichen Datenverarbeitung, aus der die Daten stammen, die nun dem Data-Mining-Prozess zugrunde gelegt werden sollen, darf diese nur nach seinen gesetzlichen Zuständigkeiten oder rechtlichen Befugnissen vornehmen. Der Empfänger hat seine gesetzliche Zuständigkeit oder rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft zu machen.

Die rechtlichen Befugnisse von Auftraggeber und Empfänger ergeben sich aus dem **Gesetz**, dem **Gesellschaftsvertrag** (Satzung, Statut, oä), damit zusammenhängend aus seiner **Rechtsform** und schließlich auch aus seiner **Gewerbeberechtigung**. Auch Einschränkungen ihrer Befugnisse können sich daraus ergeben, zB durch die Festlegung des Unternehmensgegenstandes im Gesellschaftsvertrag.

Tätigkeiten, die weder im Gesetz noch im Unternehmensgegenstand, im Gewerbeschein oder sonst gesondert Erwähnung finden, **für die Entfaltung seiner gewerblicher Tätigkeit** aber **erforderlich** sind, sind **vom Zweck eines gewerblich tätigen Unternehmens gedeckt**. Dazu gehören bspw die Beschaffung von Material, Beschäftigung von Arbeitskräften, etc.

Die Voraussetzung der gesetzlichen Zuständigkeit oder rechtlichen Befugnis des Auftraggebers ist daher erfüllt, wenn die Datenübermittlung mit

der Entfaltung einer zumindest **typischerweise dem rechtlich anerkannten Zweck des Übermittlers dienenden Tätigkeit zwangsläufig verbunden ist**. Dies gilt jedenfalls, soweit derartige Unternehmensfunktionen in der Rechtsordnung allgemein anerkannt sind (zB Buchführung, Personalverwaltung, Auslieferung usw).[117]

Im Fall der **Zustimmung des Betroffenen** oder bei Verwendung von zulässigerweise **veröffentlichtem Datenmaterial** wird man davon auszugehen haben, dass die **Berechtigung des Empfängers automatisch zugrunde zu legen** ist, um nicht jede Übermittlung an einen unbekannten Empfängerkreis (zB Internet) zu unterbinden.[118] Die Zustimmungserklärung hat aber dennoch den an sie gestellten Anforderungen zu entsprechen (vgl VI. C. 4.).

Für die Übermittlung von Daten zur Durchführung von Data-Mining-Prozessen besteht **keine ausdrückliche gesetzliche Ermächtigung.** Es finden sich keine bspw § 151 GewO oder §§ 66 Abs 6 Z 1 und 91 Abs 5 ÄrzteG 1998 vergleichbare Bestimmungen. Vielmehr sind im Einzelfall die Berechtigungen des beteiligten Auftraggebers und des Empfängers unter Berücksichtigung der konkreten Ausgestaltung der Situation zu prüfen.

D. Schutzwürdige Geheimhaltungsinteressen des Betroffenen

Sowohl nicht sensible als auch sensible Daten kommen als Basisdaten für die Durchführung eines Data-Mining-Prozesses in Frage. Im Einzelfall ist § 8 DSG 2000 oder § 9 DSG 2000 zur Überprüfung der Wahrung der schutzwürdigen Geheimhaltungsinteressen des Betroffenen heranzuziehen.

Nach § 7 Abs 2 Z 3 DSG 2000 ist unter **nochmaliger Heranziehung** der §§ 8 und 9 DSG 2000 eine **Abwägung hinsichtlich Zweck und Inhalt der Datenübermittlung durchzuführen**. Die Überprüfung nach § 7 Abs 1 DSG 2000, hier nach Zweck und Inhalt der Datenverarbeitung insgesamt, kann daher durchaus zu einem anderen Ergebnis führen als jene nach § 7 Abs 2 DSG 2000. Werden die Daten für ein anderes Aufgabengebiet des Auftraggebers übermittelt, sind unter den Interessen Dritter im gegebenen Zusammenhang die Interessen des Auftraggebers im jeweils anderen Aufgabengebiet zu verstehen.[119]

---

[117] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.
[118] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 42.
[119] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.

1. § 8 DSG 2000

Es besteht keine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Übermittlung von Daten zur Durchführung von Data-Mining-Prozessen. Es ist kein lebenswichtiges Interesse eines Betroffenen oder eines Dritten vorstellbar, das die Durchführung eines derartigen Prozesses erfordern könnte. Wäre das Data-Mining zur Erfüllung einer vertraglichen Verpflichtung zwischen Auftraggeber und Betroffenem erforderlich, ist dies meiner Meinung nach nur dann denkbar, wenn der Vertragsgegenstand selbst auf die Durchführung von Data-Mining-Prozessen lautet. Auch hinsichtlich der Verwendung von Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen und Unterlassungen ist das Vorliegen von schutzwürdigen Geheimhaltungsinteressen des Betroffenen zu bejahen, da es keine gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten für Data-Mining-Zwecke gibt, dies keine wesentliche Voraussetzung für Auftraggeber des öffentlichen Bereiches zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder sich sonst die Zulässigkeit der Verwendung dieser Daten ergibt. In diesem Zusammenhang ist nämlich nicht erkennbar, welches überwiegende Interesse der Auftraggeber an der Aufdeckung von bisher unbekannten Beziehungen haben könnte.

Schutzwürdige Geheimhaltungsinteressen können daher bei Verwendung nicht-sensibler Daten in Data-Mining-Prozessen lediglich bei der Verwendung von **veröffentlichten oder indirekt personenbezogenen Daten**, aufgrund der erteilten **Zustimmung des Betroffenen** zur Verwendung seiner Daten bzw bei Vorliegen **überwiegender berechtigter Interessen des Auftraggebers oder eines Dritten** nicht verletzt sein.

2. § 9 DSG 2000

Wie bereits erwähnt besteht keine gesetzliche Verpflichtung zur Datenübermittlung zum Zweck des Data-Minings. Die Amtshilfe kann nicht darin bestehen, Data-Mining-Prozesse durchzuführen, da nur bereits bekannte Tatsachen mitgeteilt werden sollen. Es ist keine öffentliche Funktion denkbar, die die Durchführung derartiger Prozesse erfordert. Weiters sind keine lebenswichtigen Interessen vorstellbar, die nur durch die Durchführung von Data-Mining-Prozessen gewahrt werden könnten. Soll der Data-Mining-Prozess zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers notwendig sein, ist fraglich um welche Rechtsansprüche es sich in diesem Fall handeln kann, wenn diese erst durch einen Prozess hervortreten, der bisher unbekannte Zusammenhänge aufdeckt. Es bestehen keine Rechte und Pflichten auf dem Gebiet des Arbeits- oder Dienstrechts, die Data-Mining-Prozesse erfordern, insbesondere sollten hier nur bereits bekannte Zusammenhänge bzw Tatsachen zur Kenntnis genommen werden. Es ist keine erlaubte Tätigkeit von nicht auf Gewinn gerichteten Vereinigungen denkbar, die auf die Durchführung von Data-Mining-Prozessen

zielt, da diese auf politische, philosophische, religiöse oder gewerkschaftliche Tätigkeiten beschränkt sind und ihnen nur die Verarbeitung von Daten, die „Rückschlüsse" auf die politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, erlaubt sind. Die Aufdeckung bisher verborgener Zusammenhänge kann darunter nicht subsumiert werden.

Schutzwürdige Geheimhaltungsinteressen können daher bei der Verwendung sensibler Daten in Data-Mining-Prozessen lediglich dann nicht verletzt sein, wenn der **Betroffene** die **Daten offenkundig selbst öffentlich gemacht hat** oder sie **nur in indirekt personenbezogener Form** verwendet werden, der Betroffene seine **Zustimmung zur Datenverwendung** erklärt hat, die **Voraussetzungen der §§ 45 – 47 DSG 2000** vorliegen und die Daten zum Zweck der **Gesundheitsvorsorge**, der medizinischen Diagnostik, der Gesundheitsversorgung oder –behandlung erforderlich sind und die Verwendung der Daten durch ärztliches Personal oder sonstige Personen erfolgt, die ja ihrerseits wiederum einer Verschwiegenheitspflicht unterliegen.

3. Veröffentlichte Daten § 8 Abs 2 oder § 9 Z 1 DSG 2000

Bei allen Datenanwendungen, die veröffentlichte Daten enthalten, ist die Frage zu stellen, ob sie ausschließlich solche enthalten oder nicht auch zusätzliche, durch Auswertung der veröffentlichten Daten gewonnene Daten enthalten sind, die ihrerseits noch nicht veröffentlicht sind. **Jede Aufbereitung veröffentlichter Daten** kann **neue – nicht veröffentlichte – Informationen liefern**. Deshalb kann nicht ausgeschlossen werden, dass in besonderen Konstellationen schutzwürdige Geheimhaltungsinteressen doch berührt werden.[120] In diesem Fall ist zu prüfen, ob die Datenverwendung unter einem anderen Gesichtspunkt gerechtfertigt werden kann.

4. Die Zustimmung des Betroffenen § 8 Abs 1 Z 2 oder § 9 Z 6 DSG 2000

Erforderlich ist eine Willensbekundung iSd § 4 Z 14 DSG 2000, die Gültigkeit besitzt und in Kenntnis der Sachlage für den konkreten Fall erfolgt. Mangels des Erfordernisses der Ausdrücklichkeit kann die Zustimmung hinsichtlich der Verwendung von nicht sensiblen Daten auch **konkludent** erfolgen. Bezüglich der Verwendung von sensiblen Daten ist dagegen eine **ausdrückliche** Zustimmungserklärung notwendig. **Unverzichtbar** ist aber die **Aufklärung** des Betroffenen hinsichtlich des ihm nach erteilter Zustimmung zur Verfügung stehenden **Widerrufsrechtes**.

In der Bitte des Betroffenen um Zusendung von Informationsmaterial, liegt keine Einwilligung in eine Verarbeitung seiner Daten zu anderen Zwecken, wohl aber eine **schlüssige Einwilligung zur zeitweisen Speicherung**.[121]

---

[120] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 137.
[121] *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 33.

Der Betroffene soll durch die Kenntnis der Sachlage die Möglichkeit haben, Gefahren und Vorteile der Verarbeitung ihn betreffender Daten zu beurteilen und seine Rechte auf Berichtigung und Löschung wahrzunehmen. Die dafür benötigte Information hat der Verantwortliche dem Betroffenen mitzuteilen. Im Sinne dieser Fallbezogenheit hat sich die Einwilligung auf eine **konkrete Verarbeitung von Daten über die betroffene Person durch einen bestimmten Verantwortlichen für bestimmte Zwecke** zu beziehen. Erforderlich ist daher eine spezifizierte Willensbekundung, die einen nach betroffenen Daten und Aktivitäten näher umrissenen Inhalt und Umfang hat. Auszugehen ist insoweit aber von einem beweglichen System, wonach die Anforderungen an die Bestimmtheit umso höher sind, je größer die Tragweite der Erklärung für die Rechte und Freiheiten des Betroffenen ist. Die Wirksamkeit der Zustimmung hängt maßgeblich davon ab, ob der Auftraggeber seinen **Informationspflichten** nachgekommen ist.[122]

a) § 6 Abs 3 KSchG

Der als lex specialis für Verbrauchergeschäfte geltende § 6 Abs 3 KSchG ist auch auf Sachverhalte mit datenschutzrechtlichem Inhalt anwendbar. KSchG und Datenschutzrecht können daher auf bestimmte Sachverhalte gleichzeitig Anwendung finden.

Eine **unauffällig im vorgedruckten Text vorhandene Zustimmungserklärung des Kunden** zur Verarbeitung und Weitergabe seiner Daten entspricht daher nicht dem Gesetz. Eine solche Erklärung muss vielmehr so beschaffen sein, dass an der Tatsache und dem Inhalt der Willenserklärung kein Zweifel besteht. Eine Klausel widerspricht § 6 Abs 3 KSchG, wenn entgegen dem nach objektiven Kriterien zu messenden Transparenzgebot nicht bestimmbar ist, welche Unternehmen derzeit und künftig einem Konzern zugehörig sind bzw sein werden und welchen Daten übermittelt werden sollen.[123]

Das in § 6 Abs 3 KSchG normierte Transparenzgebot ist bei einer dem Konsumenten abgeforderten **Zustimmungserklärung** zur Datenübermittlung nur dann erfüllt, wenn sie die **zu übermittelnden Datenarten, deren Empfänger und den Übermittlungszweck abschließend bezeichnet**. Dies gilt auch nach Inkrafttreten des DSG 2000.[124]

Das Transparenzgebot soll dem Betroffenen im Rahmen des Möglichen und Überschaubaren ermöglichen, sich zuverlässig über seine Rechte und Pflichten bei der Vertragsabwicklung zu informieren, damit er nicht von der Durchsetzung seiner Rechte abgehalten werden kann und ihm nicht unberechtigte Pflichten abverlangt werden. **Verwendete Klauseln** haben daher **stets klar und verständlich abgefasst** zu sein. Eine wirksame Zustimmung

---

[122] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.

[123] OGH 27. Jänner 1999, 7 Ob 170/98w - "Friends of Merkur" = ARD 5023/25/99 = ecolex 1999/182 = RdW 1999, 458.

[124] OGH 13. September 2001, 6 Ob 16/01y - "Mobilpoints" = ecolex 2002/35 (*Leitner*) = JBl 2002, 178 = RdW 2002/67.

kann nur vorliegen, wenn der **Betroffene weiß, welche seiner Daten zu welchem Zweck verwendet werden sollen**, weil er nur dann der Verwendung seiner Daten „in Kenntnis der Sachlage für den konkreten Fall“ zustimmen kann.[125]

Erfolgt die Zustimmung der betroffenen Personen aufgrund einer gemäß § 6 Abs 3 KSchG unwirksamen - weil unklaren - Vertragsklausel, ist sie ebenso unwirksam.

Dem Transparenzgebot entspringen als Einzelwirkungen das Gebot der Erkennbarkeit und Verständlichkeit, das Gebot, den anderen Vertragsteil auf bestimmte Rechtsfolgen hinzuweisen, das Bestimmtheitsgebot, das Gebot der Differenzierung, das Richtigkeitsgebot und das Gebot der Vollständigkeit.[126]

5. Überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten - § 8 Abs 1 Z 4 DSG 2000

Zur Klärung der Frage, ob überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten bestehen, ist eine umfassende Abwägung zwischen dem Verwendungsinteresse des Auftraggebers oder eines Dritten einerseits und den Geheimhaltungsinteressen des Betroffenen andererseits erforderlich. Das **Interesse des Auftraggebers** muss ein **berechtigtes**, dh **von der Rechtsordnung anerkanntes**, sein. Das Geheimhaltungsinteresse auf Seite des Betroffenen hängt maßgeblich vom Inhalt der zu verarbeitenden Daten ab.[127]

a) Die Interessenabwägung im Bereich des DSG 2000

Die Interessenabwägung nach dem DSG 2000 räumt den Rechten des Betroffenen grundsätzlich einen höheren Stellenwert ein als die EG-Datenschutzrichtlinie, 95/46/EG.[128]

Nur wenn der Zweck, zu dem die Speicherung erfolgt, mit der Belastung des Selbstbestimmungsrechtes des Einzelnen zu vereinbaren ist und nur soweit die erfassten Daten zu diesem Zweck erforderlich sind, ist die Speicherung von den Betroffenen hinzunehmen. Dieser **Grundsatz der Erforderlichkeit** lässt sich schon aus dem Verweis in § 1 Abs 2 DSG 2000 ableiten, wonach nur gesetzlich gedeckte notwendige Eingriffe erlaubt sind. Zur Wahrung berechtigter Interessen Dritter, die nur mit einem Eingriff in das Grundrecht auf Datenschutz verfolgt werden können, ist dieser lediglich in der **gelindesten Form** zulässig, sodass die Interessen des anderen noch gewahrt werden können, das Grundrecht des Betroffenen aber so weit als möglich unverletzt bleibt. Dem **Interesse am gefährdeten Gut sind stets die Interessen des**

---

[125] OGH 22. März 2001, 4 Ob 28/01y = ecolex 2001/147 (*Rabl*) = ÖBA 2001/977 (*Koziol*) = ÖBA 2002, 67 = RdW 2001/557.

[126] OGH 13. September 2001, 6 Ob 16/01y - "Mobilpoints" = ecolex 2002/35 (*Leitner*) = JBl 2002, 178 = RdW 2002/67.

[127] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.

[128] *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000), 139.

Handelnden und der Allgemeinheit gegenüberzustellen. Abzustellen ist dabei auf die Art des eingeschränkten Rechtes, die Schwere des Eingriffes, die Verhältnismäßigkeit zum verfolgten Zweck und den Grad der Schutzwürdigkeit dieses Interesses. Durch das Grundrecht auf Datenschutz sollen aber nicht die Interessen der Allgemeinheit aus Gründen des Datenschutzes nicht mehr verfolgt werden können.[129]

Der **Datenschutz hat** somit jedenfalls **bei Vorliegen eines öffentlichen Interesses in den Hintergrund zu treten**.

Das Grundrecht auf Datenschutz gilt aber auch für den Verkehr **zwischen Privaten**. Hier spricht im Zuge der Interessenabwägung die Vermutung **im Zweifel für die Schutzwürdigkeit**. Als berechtigte Interessen sind auch subjektive, auf gesetzlicher oder vertraglich (zB Franchise-Verträge) vereinbarter Grundlage beruhende Ansprüche anerkannt.[130]

E. Grundsatz der Verhältnismäßigkeit § 7 Abs 3 DSG 2000

Die Zulässigkeit einer Datenverwendung setzt voraus, dass die dadurch verursachten **Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß** und mit den **gelindesten zur Verfügung stehenden Mitteln** erfolgen und dass die Grundsätze des § 6 DSG 2000 eingehalten werden.

1. Festgelegte, eindeutige und rechtmäßige Zwecke und Wesentlichkeitsgrundsatz - § 6 Abs 1 Z 2 und Z 3 DSG 2000

Die Zweckfestlegung hat bereits für die Ermittlung der Daten zu erfolgen und erfordert einen **bewussten Akt des Auftraggebers**. Es reicht hierzu nicht aus, dass sie sich aus dem Gesamtzusammenhang der Datenverwendung irgendwie ergibt. Die Schriftlichkeit der Festlegung ist nicht, ihre Eindeutigkeit und Rechtmäßigkeit dagegen schon erforderlich. Zweifel, ob und in welchem Sinn der Auftraggeber den Zweck festgelegt hat, müssen ausgeschlossen werden können. Der Ermittlungszweck als **Primärzweck** muss **rechtmäßig und auf rechtmäßige Weise festgelegt worden sein**. Die Ermittlungsmaßnahme darf gerade im Hinblick auf den festgelegten Zweck rechtmäßig sein.

Der **Zweck der Übermittlung** durch den Auftraggeber ist im Rahmen der **rechtmäßigen Zwecke der Verarbeitung der erhaltenen Daten durch den Empfänger** gelegen.[131] Die Zulässigkeit der Datenübermittlung erfordert nicht, dass sie für die Tätigkeit unabdingbar ist, sondern dass sie eine

---

[129] OGH 12. März 1997, 6 Ob 2228/96 g = AnwBl 1997/7361 = JBl 1997, 516 = RdW 1997, 399.

[130] OGH 26. August 1999, 2 Ob 244/99 t = RdW 1999, 785 = RdW 2000/55.

[131] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.

„wesentliche Voraussetzung“ dafür bildet, die Tätigkeit also durch die übermittelten Daten in entscheidender Weise erleichtert wurde.[132]

Eine **Weiterverwendung von Daten** soll **nur zulässig** sein, wenn dies mit dem **ursprünglichen Ermittlungszweck „nicht unvereinbar“** ist. Diejenigen innerbetrieblichen Datenverwendungen, die der Aufrechterhaltung und Optimierung der Organisation (wie zB Rechnungswesen und Controlling) oder der Analyse und Planung dienen, sind nicht als eigener Verwendungszweck zu sehen, der mit dem Zweck der ursprünglichen Datenermittlung (zB im Rahmen des Abschlusses eines Handelsgeschäftes) unvereinbar ist.[133]

Die Ziele des Data-Minings gehen aber weit über die Optimierung der Organisation hinaus. Angestrebt wird die Optimierung im Hinblick auf den Unternehmensprofit oder die Kundenzufriedenheit. Nicht nur eine interne Optimierung der Organisation ist das erklärte Ziel, diese soll vielmehr nach außen treten und wirtschaftliche Wirkung zeigen.

Die Vorratsbeschaffung von Daten ist unzulässig.

Fraglich ist daher, ob die Aufdeckung von verborgenen und unbekannten Beziehungen ein eindeutiger und rechtmäßiger Zweck der Datenübermittlung ist. In dieser Allgemeinheit ist dies meiner Meinung nach nicht zu bejahen. Liegen dem Data-Mining Datenbestände zugrunde, die ursprünglich für keinen eindeutigen, rechtmäßigen und festgelegten Zweck ermittelt wurden, ist die Übermittlung dieser Daten jedenfalls unzulässig. Sollen Daten rechtmäßig weiterverwendet, in gegenständlichen Fall übermittelt, werden, darf dies nicht mit dem eindeutigen, rechtmäßigen und festgelegten Zweck der ursprünglichen Datenverarbeitung und auch nicht mit dem Zweck der Datenübermittlung unvereinbar sein. Dies kann meiner Meinung nach aber nur dann beurteilt werden, wenn zumindest konkrete Erwartungen bestehen, welche Ergebnisse der Data-Mining-Prozess liefern wird. Diese Erwartungen müssten sich aus den Daten, die die Basis für das Data-Mining bilden, ableiten lassen. Auch die beabsichtigte nachfolgende Verwendung der gewonnenen Erkenntnisse ist meiner Meinung nach in die Erwägungen unbedingt mit einzubeziehen.

Auch die Eindeutigkeit, Rechtmäßigkeit und Festlegung des Übermittlungszweckes sollten nach den durch den Data-Mining-Prozesses erwarteten Ergebnissen und deren beabsichtigter nachfolgenden Verwendung beurteilt werden. Auch ob die Daten für den Zweck der Datenanwendung wesentlich sind, ist unter diesen Gesichtspunkten zu prüfen, wird in Anbetracht der Zielsetzung des Data-Minings, aus bestehenden Datenbeständen neue Erkenntnis zu gewinnen, aber nicht verneint werden können. Der Zweck der Datenübermittlung ist daher insgesamt einer umfassenden Prüfung zu unterziehen.

---

[132] DSK vom 18. Mai 2000, 120.686/3-DSK/00.

[133] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.

2. Sachliche Richtigkeit - § 6 Abs 1 Z 4 DSG 2000

Den Auftraggeber trifft die konkrete Pflicht die Daten regelmäßig zu aktualisieren. Diese ist im Zusammenhang mit dem Verwendungszweck zu sehen, weshalb sich unterschiedlich strenge Anforderungen an die Aktualisierungspflicht ergeben können.[134] Im Interesse der Richtigkeit der aus Data-Mining-Prozessen zu erlangenden Ergebnisse ist von einer strengen Aktualisierungspflicht auszugehen.

3. Aufbewahrungsdauer - § 6 Abs 1 Z 5 DSG 2000

Die Vereinbarkeit der Bestimmung, dass **Daten nur solange in personenbezogener Form aufbewahrt** werden dürfen, als dies für die **Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich** ist, mit der für die Durchführung von Data-Mining-Prozessen notwendigen Speicherungsdauer ist zu prüfen, da die Gefahr besteht, Daten in Vorratshaltung auf lange Dauer abzuspeichern.

[134] *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861.

VII. Zusammenfassung

A. Die Entschließung der 59. Konferenz der Datenschutzbeauftragten des Bundes und der Länder vom 14./15. März 2000 (Deutschland)[135]

Nach der hierin festgelegten Definition des Begriffes „Data Mining" bietet es Werkzeuge, die die scheinbar zusammenhanglosen Daten nach noch nicht bekannten, wissenswerten Zusammenhängen durchsuchen, Daten aufspüren, kombinieren und neue Informationen zur Verfügung stellen. Diese Entwicklung schafft **neue Gefahren für das Grundrecht auf informationelle Selbstbestimmung** und für den **Schutz der Privatheit** zB durch die Erstellung von Persönlichkeitsprofilen, automatisierte Vorhersagen von Verhaltens- und Handlungsweisen, Manipulationsmöglichkeiten und zu lange Speicherungsdauer.

Die Konferenz der Datenschutzbeauftragten verweist darauf, dass nach dem grundrechtlichen Gebot der Zweckbindung personenbezogene Daten nur im Rahmen der gesetzlich zugelassenen Zwecke oder der gegenseitigen Vereinbarung verwendet werden dürfen. Die **personenbezogene Speicherung in einem Data Warehouse entfernt sich vom ursprünglichen Verwendungszweck** und stellt dadurch eine **Speicherung auf Vorrat ohne Zweckbindung** dar. Eine Zweckänderung ist aber nur mit Einwilligung der Betroffenen zulässig, die wiederum die Aufklärung über die Tragweite der Einwilligung voraussetzt. Die Einwilligung in unbestimmte und zeitlich unbegrenzte Zweckänderungen ist aus diesem Grund unwirksam.

Gestaltung und Auswahl von Datenverarbeitungs-Systemen sollen dafür Sorge zu tragen, keine oder so wenig personenbezogene Daten wie möglich zu verarbeiten, wobei **anonyme und pseudonyme Verfahren datenschutzrechtlich unbedenklich** sind. Die Verfahren haben für eine hinreichende Informationsmöglichkeit der Betroffenen zu sorgen, um jederzeit die Risiken abschätzen und ihre Rechte wahrnehmen zu können.

Nach der Europäischen Datenschutzrichtlinie hat grundsätzlich jede Person das Recht, **keiner belastenden automatisierten Einzelentscheidung unterworfen zu werden** (Art 15 EG-Datenschutzrichtlinie, 95/46/EG). **Data-Mining ist ein solches Instrument, das für automatisierte Einzelentscheidungen herangezogen werden kann.**

Die Hersteller und Anwender von Data Mining Verfahren sind daher dazu aufgerufen, jenen Programmen den Vorzug zu geben, die unter Einsatz von datenschutzfreundlichen Technologien die Speicherung von personenbezogenen Daten durch Anonymisierung oder Pseudonymisierung vermeiden.

---

[135] http://www.datenschutz-berlin.de/doc/de/konf/59/datawa.htm.

B. Die derzeitige Situation in Österreich

Den seit der Entwicklung des Data-Minings entstehenden rechtlichen Problemen, kann nach der derzeitigen Rechtslage aufgrund großer Auslegungsschwierigkeiten, die sich durch fehlende höchstgerichtliche Judikatur noch verschärfen, nur schwer Rechnung getragen werden.

Die rechtliche Beurteilung des Data-Mining-Prozesses muss daher dem konkreten Einzelfall vorbehalten bleiben. Allgemeingültige Aussagen sind zum derzeitigen Zeitpunkt nicht möglich, wie das folgende Beispiel verdeutlichen soll:

Eine natürliche oder juristische Person betreibt einen KFZ-Handel und eine KFZ-Werkstätte, für die sie in jeweils getrennten Datenbanken die Kundendaten erfasst, speichert, ordnet, abfragt, ausgibt usw. Es handelt sich dabei lediglich um nicht-sensible Daten. Geht man davon aus, dass es sich bei KFZ-Handel und KFZ-Werkstätte um **ein Aufgabengebiet** des Auftraggebers handelt und somit auch kein Zweckwechsel damit verbunden ist, wenn die Kundendaten des KFZ-Handels für Belange der KFZ-Werkstätte und umgekehrt verwendet werden, liegt keine Datenübermittlung vor. Bei Durchführung eines Data-Mining-Prozesses sind die für die Datenverarbeitung geltenden Bestimmungen zu befolgen. Ausgehend davon, dass es sich um **verschiedene Aufgabengebiete** handelt, müssen bei Datentransfers zwischen dem Bereich des KFZ-Handels und dem der KFZ-Werkstätte zur nachfolgenden Durchführung von Data-Mining-Prozessen die Bestimmungen der Datenübermittlung befolgt werden. Am wichtigsten ist dabei die Frage, ob durch die Übermittlung schutzwürdige Geheimhaltungsinteressen der Kunden verletzt werden. Liegt eine nach dem DSG 2000, bei Verbrauchern iSd KSchG auch nach § 6 Abs 3 KSchG, wirksame Zustimmungserklärung der Kunden vor oder handelt es sich um veröffentlichte oder nur indirekt personenbezogene Daten, so werden durch die Datenübermittlung keine schutzwürdigen Geheimhaltungsinteressen verletzt. Das Vorliegen der rechtlichen Befugnis des "Empfängers" ist in diesen Fällen zu bejahen. Bei Erfüllung der weiteren gesetzlichen Voraussetzungen der Datenübermittlung ist diese daher **zulässig** und die so übermittelten Daten dürfen einem Data-Mining-Prozess zugrundegelegt werden. Liegt dagegen keiner dieser Gründe für einen Ausschluss der Verletzung schutzwürdiger Geheimhaltungsinteressen des Betroffenen vor, bleibt zu prüfen, ob der Auftraggeber überwiegende berechtigte Interessen an der Übermittlung der Daten hat. Während der Kunde ein Interesse daran hat, seine Daten geheim zu halten, ist der Auftraggeber interessiert, die vorhandenen Kundendaten nach Zusammenhängen zu durchsuchen, die ihm bisher verborgen waren, durch die ihm aber eine Steigerung des Unternehmensprofits ermöglicht würde. Im Zweifel spricht die Vermutung für die Schutzwürdigkeit des Betroffenen. Die

Datenübermittlung wäre daher in diesem Fall wegen der Verletzung schutzwürdiger Geheimhaltungsinteressen des Betroffenen **unzulässig** und somit auch der auf dieser Datenbasis durchgeführte Data-Mining-Prozess.

Aufgezeigt können in einer allgemeinen rechtlichen Beurteilung des Data-Minings daher nur jene Punkte werden, die im Einzelfall besonders streng zu prüfen sind und Probleme aufwerfen können. Geäußert können nur Wünsche hinsichtlich einer möglichen neuen Gestaltung der Rechtslage werden, die dem Schutz des einzelnen Betroffenen Rechnung tragen würden.

Im konkreten Einzelfall ist besonderes Augenmerk auf die Zwecke zu legen, zu denen durch das Data-Mining neue Erkenntnisse gewonnen werden sollen. Es ist eine **strenge Zweckprüfung und Abwägung hinsichtlich der schutzwürdigen Geheimhaltungsinteressen der Betroffenen** durchzuführen.

Vorrangig obliegt es den derzeit im DSG 2000 vorgesehenen **Kontrollmechanismen** (insbesondere der Meldepflicht des Auftraggebers und dem daran anschließenden Prüfungsverfahren durch die Datenschutzkommission sowie deren sonstigen Befugnissen - §§ 17, 20 und 30 ff DSG 2000) dem Schutzes der Betroffenen gerecht zu werden, wobei die effektive Rechtsdurchsetzung im privaten Bereich durchaus verbessert werden könnte. Wünschenswert wäre in diesem Zusammenhang mE die Schaffung von **spezifischen Kontrollmöglichkeiten** für Data-Mining-Prozesse, nicht etwa nur durch eine besondere Meldepflicht vor Aufnahme der Tätigkeit sondern auch eine zusätzliche Mitteilung der gewonnenen Erkenntnisse an die Datenschutzkommission, der sodann deren Überprüfung im Hinblick auf die Wahrung der Rechte der Betroffenen obliegt. Vorstellbar wäre es auch, für jedes Data-Mining-Projekt einen von der Datenschutzkommission besonders beauftragen Mitarbeiter als „Projektprüfer“ direkt in das Projekt zu stellen.

Positiv auf die Situation der Betroffenen könnte sich aber auch die Schaffung von **Beschränkungen hinsichtlich der Verknüpfungs- oder Abfragemöglichkeiten** auswirken. Abfragen sollten nicht mehr in jede beliebige Richtung möglich sein, sondern von zusätzlichen Voraussetzungen abhängig gemacht werden, für die der Auftraggeber erneut seine Berechtigung und Qualifizierung darlegen muss.

Wünschenswert wäre überdies eine **konkrete Begrenzung der Nutzungsmöglichkeiten der vorhandenen Datenbestände**. Durch **Kopier-** und **Verwertungsverbote** sowie **Löschungsverpflichtungen** könnte diesen Erfordernissen entsprochen werden.

Die derzeitige Lage in Österreich ist relativ offen. Das Augenmerk ist auf den einzelnen Data-Mining-Prozess zu legen.

Grundsätzlich stehe ich den Möglichkeiten, die das Data-Mining eröffnet, zurückhaltend gegenüber. Werden bei seiner Durchführung die gesetzlichen Bestimmungen beachtet, ist natürlich nichts dagegen einzuwenden. Die Missbrauchsgefahr ist aber dennoch ständig präsent. Persönlich hoffe ich, dass das Data-Mining für Analysen, die im Interesse der Allgemeinheit liegen, angewendet werden mögen, wie zB im Bereich der medizinischen Forschung.

Abkürzungsverzeichnis

aA	=	anderer Ansicht
aaO	=	am angegebenen Ort
AB	=	Ausschussbericht
ABGB	=	Allgemeines bürgerliches Gesetzbuch, JGS 946/1811
abl	=	ablehnend
ABl	=	Amtsblatt der Europäischen Gemeinschaften
AGB	=	Allgemeine Geschäftsbedingungen
AnwBl	=	Österreichisches Anwaltsblatt
arg	=	argumento
BG	=	Bundesgesetz
BGBl	=	Bundesgesetzblatt
BGBlG	=	Bundesgesetz über das Bundesgesetzblatt 1996, BGBl 660/1996
BKA	=	Bundeskanzleramt, Bundeskriminalamt
BMF	=	Bundesministerium für Finanzen
BMI	=	Bundesministerium für Inneres
BMJ	=	Bundesministerium für Justiz
BMLV	=	Bundesministerium für Landesverteidigung
BMVIT	=	Bundesministerium für Verkehr, Innovation und Technologie
BlgNR	=	Beilage(-n) zu den stenographischen Protokollen des Nationalrates
BR	=	Bundesrat
bspw	=	beispielweise
B-VG	=	Bundesverfassungsgesetz 1920 idF v 1929
bzw	=	beziehungsweise
Datenschutz-RL	=	Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl L 201 vom 31.7.2002, 37
dh	=	das heißt
div	=	diverse
DSG 2000	=	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000), BGBl I 165/1999
DSG 1978	=	Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz), BGBl 565/1978
DSK	=	Datenschutzkommission
E	=	Entscheidung
EB	=	Erläuternde Bemerkungen
ecolex	=	Fachzeitschrift für Wirtschaftsrecht

EG-Datenschutz-RL	=	Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Abl L 281, 31 vom 23.11.1995
EGMR	=	Europäischer Gerichtshof für Menschenrechte
EGZPO	=	Einführungsgesetz zur Zivilprozessordnung, RGBl 112/1895
EfSlg	=	Ehe- und Familienrechtliche Entscheidungen des OGH
EMRK	=	Europäische Menschenrechtskonvention, BGBl 210/210
Entw	=	Entwurf
EO	=	Exekutionsordnung, RGBl 79/1896
ErgLfg	=	Ergänzungslieferung
ErwGr	=	Erwägungsgrund
et alt	=	und andere
etc	=	et cetera
EuGH	=	Gerichtshof der Europäischen Gemeinschaften
EuGI	=	Gericht der Europäischen Gemeinschaften I. Instanz
EuGRZ	=	Europäische Grundrechte Zeitschrift
EvBl	=	Evidenzblatt für Rechtsmittelentscheidungen (ÖJZ)
EWR	=	Europäischer Wirtschaftsraum
f, ff	=	folgende
FinStrG	=	Finanzstrafgesetz, BGBl 129/1958
FN	=	Fußnote
G	=	Gesetz
gem	=	gemäß
GewO	=	Gewerbeordnung 1994, BGBl 194/1994
GP	=	Gesetzgebungsperiode
Hrsg	=	Herausgeber
iaR	=	in aller Regel
idF	=	in der Fassung
idR	=	in der Regel
idS	=	in diesem Sinne
ieS	=	im engeren Sinn
insbes	=	insbesondere
InfoSoc-RL	=	Richtlinie 2001/29/EG vom 22. Mai 2001 zur Harmonisierung bestimmter Aspekte des Urheberrechts und der verwandten Schutzrechte in der Informationsgesellschaft (ABl L 167 v 22.6.2001, 10, berichtigt durch ABl L 6 v 10.1.2002, 71).
IP	=	Internet Protokoll
IPR	=	Internationales Privatrecht
iS	=	im Sinne
iSd	=	im Sinne des, - der
iSv	=	im Sinne von
iVm	=	in Verbindung mit
iwS	=	im weiteren Sinn

JA	=	Justizausschuss
JAP	=	Juristische Ausbildung und Praxisvorbereitung
JBl	=	Juristische Blätter
Jud	=	Judikatur
JurPC	=	JurPC, Internet-Zeitschrift für Rechtsinformatik
KSchG	=	Konsumentenschutzgesetz, BGBl. 140/1979
leg cit	=	legis citatae (der zitierten Vorschrift)
Lfg	=	Lieferung
Lit	=	Literatur
lit	=	litera
maW	=	mit anderen Worten
mE	=	meines Erachtens
mA	=	meiner Ansicht
MR	=	Zeitschrift für Medien und Recht
mwH	=	mit weiteren Hinweisen
mwN	=	mit weiteren Nachweisen
Nov	=	Novelle
NR	=	Nationalrat
NZ	=	Notariatszeitung
oa	=	oder ähnliches
OGH	=	Oberster Gerichtshof
OLG	=	Oberlandesgericht
ÖBl	=	Österreichische Blätter für gewerblichen Rechtsschutz und Urheberrecht
ÖJZ	=	Österreichische Juristen-Zeitung
ÖH	=	Österreichische Hochschülerschaft
ÖStZ	=	Österreichische Steuerzeitung
RdW	=	Österreichisches Recht der Wirtschaft
RGBl	=	Reichsgesetzblatt
RL	=	Richtlinie der Europäischen Gemeinschaften
Rs	=	Rechtsache
Rsp	=	Rechtsprechung
Rz	=	Randzahl
RV	=	Regierungsvorlage
S	=	Satz, Seite
Slg	=	Sammlung
sog	=	sogenannt, -e, -er, -es
StF	=	Stammfassung
StProt	=	stenographische(s) Protokoll(e)
stRsp	=	ständige Rechtsprechung
SZ	=	Entscheidungen des österreichischen Obersten Gerichtshofes in Zivilsachen

ua	=	und andere
udgl	=	und dergleichen
UrhG	=	Bundesgesetz über das Urheberrecht an Werken der Literatur und der Kunst und über verwandte Schutzrechte (Urheberrechtsgesetz), BGBl 111/1936
UrhG-Nov	=	Urheberrechtsgesetz-Novelle
URL	=	Uniform Resource Locator
uU	=	unter Umständen
UWG	=	Bundesgesetz gegen den unlauteren Wettbewerb, BGBl 448/1984
v	=	vom, von
va	=	vor allem
vgl	=	vergleiche
VO	=	Verordnung
VfGH	=	Verfassungsgerichtshof
VwGH	=	Verwaltungsgerichtshof
VStG	=	Verwaltungsstrafgesetz 1991, BGBl 52/1991
wbl	=	Wirtschaftsrechtliche Blätter
Z	=	Ziffer
zB	=	zum Beispiel
ZfRV	=	Zeitschrift für Rechtsvergleichung
zT	=	zum Teil

Literaturverzeichnis

Drobesch Heinz, Grosinger Walter, Das neue österreichische Datenschutzgesetz, Juridica Verlag, Wien, 2000.

Zitiert: *Drobesch/Grosinger*, Das neue österreichische Datenschutzgesetz (2000),

Duschanek Alfred, Datenschutzrecht, in: *Holoubek Michael/Potacs Michael*, Öffentliches Wirtschaftsrecht Band 1, Springer-Verlag, Wien, 2002.

Zitiert: *Holoubek/Potacs*, Öffentliches Wirtschaftsrecht Band 1, 2002,

Duschanek Alfred, Rosenmayr-Klemenz Claudia, Datenschutzgesetz 2000 – DSG 2000 Bundesgesetz über den Schutz personenbezogener Daten, Wirtschaftskammer Österreich, Wien, 2000.

Zitiert: *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000),

Ghali Yvonne, Datenschutz Rechtsgrundlagen, WEKA Verlag, Wien, 1999.

Zitiert: *Ghali*, Datenschutz (1999),

Grabenwarter Christoph, Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel, ÖJZ 2000, 861.

Zitiert: *Grabenwarter*, Kundendaten im Versandhandel, ÖJZ 2000, 861

Hansen Hans Robert, Gustaf Neumann, Wirtschaftsinformatik I, Grundlagen betrieblicher Informationsverarbeitung, Lucius & Lucius, Stuttgart, 2001[8].

Zitiert: *Hansen/Neumann*, Wirtschaftsinformatik I, 2001[8],

Heuer Andreas, Saake Gunter, Datenbanken Konzepte und Sprachen, mitp-Verlag, Bonn, 2000[2].

Zitiert: *Heuer/Saake*, Datenbanken, 2000[2],

Jahnel, Dietmar, Das Datenschutzgesetz 2000. Wichtige Neuerungen, wbl 2000, 49.

Zitiert: *Jahnel*, Das Datenschutzgesetz 2000, WBl 2000, 49

Jahnel Dietmar, Datenschutzrecht, in: *Jahnel Dietmar/Schramm Alfred/ Staudegger Elisabeth*, Informatikrecht, Springer-Verlag, Wien, 2003[2.]

Zitiert: *Jahnel/Schramm/Staudegger*, Informatikrecht (2003[2]),

Krahl Daniela, Windheuser Ulrich, Zick Friedrich-Karl, Data Mining Einsatz in der Praxis, Addison-Wesley, Bonn, 1998.

Zitiert: *Krahl/Windheuser/Zick*, Data Mining, 1998,

Mayer-Schönberger Viktor, Brandl Ernst O., Datenschutzgesetz 2000, Linde Verlag, Wien, 1999.

Zitiert: *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999),

Schweighofer Erich, Data Mining und Datenschutz am Beispiel Österreichs, DuD 21 (1997), 458 – 461.

Zitiert: *Schweighofer*, Data Mining und Datenschutz, DuD 21 (1997),

Sonstige Quellen

http://www.ai.univie.ac.at/oefai/ml/kdd/wasist.html
http://www.ai.univie.ac.at/oefai/ml/kdd/wi-ass.html
http://www.ai.univie.ac.at/oefai/ml/kdd/wi-eigensch.html
http://www.ai.univie.ac.at/oefai/ml/kdd/wi-grupp.html
http://www.ai.univie.ac.at/oefai/ml/kdd/wi-klass.html
http://www.ai.univie.ac.at/oefai/ml/kdd/wi-schritte.html

http://www.akwien.at/396_11161.htm

http://www.datenschutz-berlin.de/doc/de/konf/59/datawa.htm

http://futurezone.orf.at/futurezone.orf?read=detail&view=bw&id=180049&tmp=80570

http://www.the-data-mine.com/bin/view/Misc/DataMining

http://www.unet.univie.ac.at/~a9560254/pub/dm/

http://wwwai.wu-wien.ac.at/~koch/lehre/inf-sem-ws-00/nentwich/mining.pdf