

DAS DATEN- SCHUTZ- GESETZ 2000

Am 1. 1. 2000 ist ein neues Datenschutzgesetz (DSG 2000) in Kraft getreten. Durch das DSG 2000 wird zum einen die EU-Richtlinie zum Datenschutz (Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr) umgesetzt, zum anderen wurde versucht, den bei der bisherigen Vollziehung des geltenden Datenschutzes gewonnenen Erfahrungen Rechnung zu tragen.

Da durch das DSG 2000 der Datenschutz gegenüber der bisherigen Rechtslage nicht unwesentlich verstärkt wurde und auch das Datenschutzbewusstsein der Bevölkerung zugenommen hat, sollen die folgenden Ausführungen, ohne Anspruch auf Vollständigkeit, einen informativen Überblick über die wesentlichen Bestimmungen und wichtigsten Neuerungen des DSG 2000 geben.

SCHUTZBEREICH DES DSG 2000

Das DSG 2000 schützt **personenbezogene** Daten. Das sind alle Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Betroffene sind alle natürlichen und juristischen Personen sowie Personengemeinschaften, deren Daten verwendet werden.

Die Daten können sein:

DIREKT PERSONENBEZOGENE DATEN:

z. B.: Name, Geburtsdatum, Wohnanschrift usw.

INDIREKT PERSONENBEZOGENE DATEN:

Der Personenbezug der Daten ist so, dass die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht mehr bestimmt werden kann.

z. B.: verschlüsselte Daten, deren Verschlüsselungs-Code bei der

Verwendung nicht zugänglich ist (Sozialversicherungsnummer, Geheimtelefonnummer)

ZULÄSSIGERWEISE VERÖFFENTLICHTE DATEN:

z. B.: Firmenbuch, Grundbuch, Gewerberegister

Bei der Verwendung **indirekt personenbezogener Daten** und **zulässigerweise veröffentlichter Daten** gelten schutzwürdige Geheimhaltungsinteressen als nicht verletzt.

ANONYMISIERTE DATEN:

Es handelt sich um Daten, die niemand auf eine in ihrer Identität bestimmte Person zurückführen kann, da der Personenbezug fehlt. Diese Daten sind datenschutzrechtlich nicht relevant.

SENSIBLE DATEN:

Darunter versteht man besonders schutzwürdige Daten. Das sind Daten natürlicher Personen über ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit, Sexualleben.

MANUELL VERARBEITETE DATEN:

Das sind Daten, die nicht automationsunterstützt verarbeitet werden (z. B. Karteien, Handdateien). Diese Daten sind dann Datenanwendungen im Sinne des DSG, wenn sie für Zwecke von Angelegenheiten bestehen, in denen die Zuständigkeit zur Gesetzgebung Bundessache ist. Datenschutzregelungen für manuelle Dateien, die für Zwecke von Angelegenheiten bestehen, die in die Zuständigkeit der Landesgesetzgebung fallen (z. B. Naturschutz, Raumordnung, Baugesetz), müssen erst von den jeweiligen Bundesländern erlassen werden.

GRUNDRECHT AUF DATENSCHUTZ

So wie schon das DSG 1978 stellt auch das DSG 2000 ein Grundrecht auf Datenschutz als Verfassungsbestimmung voran.

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. Ein schutzwürdiges Interesse ist aus-

geschlossen, wenn Daten in Folge ihrer **allgemeinen Verfügbarkeit (veröffentlichte Daten)** oder **mangelnden Rückführbarkeit auf den Betroffenen (anonymisierte Daten)** einem Geheimhaltungsanspruch nicht zugänglich sind. Soweit die Verwendung von personenbezogenen Daten nicht im **lebensnotwendigen Interesse des Betroffenen** oder **mit seiner Zustimmung** erfolgt, sind Beschränkungen des Anspruches auf Geheimhaltung nur zur Wahrung überwiegender berechtigter Interessen eines anderen zulässig.

Wird ein solcher Eingriff durch eine staatliche Behörde vorgenommen, dann bedarf es dazu immer einer besonderen gesetzlichen Grundlage. Das Grundrecht auf Datenschutz garantiert darüber hinaus ein **Auskunftsrecht** (wer welche Daten über ihn verarbeitet, woher die Daten stammen, wozu sie verwendet werden und an wen sie übermittelt werden) sowie das Recht auf **Richtigstellung** unrichtiger Daten und **Löschung** unzulässigerweise verarbeiteter Daten.

Das betrifft sowohl die automationsunterstützte Verarbeitung als auch die Verarbeitung in manuell geführten Dateien.

EINFACHE GESETZLICHE BESTIMMUNGEN DES DSG

DEFINITIONEN

Im Vergleich zur bisherigen Rechtslage sind durch das DSG 2000 bei den Begriffsbestimmungen insbesondere folgende Neuerungen erwähnenswert:

SENSIBLE DATEN:

Darunter fallen, wie schon erwähnt, besonders schutzwürdige Daten; das sind Daten natürlicher Personen über rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit, Sexualleben.

Hinsichtlich der Zulässigkeit der Verwendung (Verarbeitung und Übermittlung) solcher Daten bestehen besonders strenge Regelungen (siehe später), außerdem sind sie grundsätzlich einer sogenannten Vorabkontrolle durch die Datenschutzkommission (DSK) unterworfen (siehe später).

AUFTRAGGEBER:

Das DSG 2000 definiert als Auftraggeber jene natürliche oder juristische Person oder Personengemeinschaft, die allein oder mit anderen gemeinsam die Entscheidung trifft, Daten für einen bestimmten Zweck zu verarbeiten, gleichgültig ob sie die Verarbeitung selbst durchführt oder dazu einen anderen (Dienstleister) dazu heranzieht.

Neu ist, dass nunmehr als Auftraggeber auch Personen gelten, die einem Dritten die Daten zur Herstellung eines von ihnen aufgetragenen Werkes überlassen, wobei der Auftragnehmer die Entscheidung trifft, diese Daten zu verarbeiten.

Damit ist etwa ein Unternehmer, der seinem Steuerberater den Auftrag zur Lohnverrechnung für seine Mitarbeiter erteilt, nunmehr Auftraggeber und zur Einhaltung der datenschutzrechtlichen Verpflichtungen verantwortlich; dies auch dann, wenn er gar nicht selbst den Auftrag zur automationsunterstützten Datenverarbeitung erteilt hat, sondern der Steuerberater über die Art der Verarbeitung autonom entschieden hat.

Eine Ausnahme besteht nur dann, wenn dem Auftragnehmer anlässlich der Auftragserteilung die Verarbeitung der überlassenen Daten untersagt wurde oder der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten aufgrund von Rechtsvorschriften, Ständesregeln oder Verhaltensregeln eigenverantwortlich zu treffen hat. In diesem Fall gilt der mit der Herstellung des Werkes Betraute als **Auftraggeber**.

DIENSTLEISTER:

Darunter versteht man alle natürlichen und juristischen Personen sowie Personengemeinschaften, die Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden.

DATENANWENDUNG:

Dieser Begriff ist an Stelle des Begriffes Datenverarbeitung getreten, wobei darunter die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert erfolgen (au-

tomationsunterstützte Datenanwendung).

Die Definition zielt zwar auf **automationsunterstützte** Verarbeitungen ab, gilt aber auch für rein **manuelle Datensammlungen**. **Manuelle Daten** sind Datenanwendungen im Sinne des DSG 2000, soweit die Zuständigkeit zur Gesetzgebung **Bundessache** ist. Die Meldepflicht (siehe später) besteht nur für solche Daten, deren Inhalt der **Vorabkontrolle** (siehe später) unterliegt. Der Vollzug bei manuellen Daten, die aufgrund von Landesgesetzen entstanden sind bzw. geführt werden, ist derzeit nicht geregelt.

VERWENDEN VON DATEN:

Jede Art der Handhabung einer Datenanwendung, sowohl das Verarbeiten von Daten als auch das Übermitteln von Daten.

INFORMATIONSVORBUNDENSYSTEM:

Die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber und die gemeinsame Benützung der Daten in der Art, dass jeder Auftraggeber auch auf jene Daten im System Zugriff hat, die von den anderen Auftraggebern dem System zur Verfügung gestellt wurden (z. B. Reservierungssysteme, Flugbuchungssysteme, Verbrechensbekämpfungssysteme).

Der Auftraggeber eines Informationsverbundsystems muss einen geeigneten **Betreiber** für das System bestellen.

Der Betreiber hat jeden Betroffenen auf Antrag binnen zwölf Wochen alle Auskünfte zu geben, die notwendig sind, um den für die Verarbeitung seiner Daten im System verantwortlichen Auftraggeber festzustellen.

Den Betreiber trifft auch die Verantwortung für die notwendigen Maßnahmen der Datensicherheit. Informationsverbundsysteme unterliegen auch der Vorabkontrolle (siehe später).

ZUSAMMENFASSUNG DER DATENANWENDUNGEN FÜR DEN ÖFFENTLICHEN UND PRIVATEN BEREICH

Das DSG 2000 trennt sich von der Zweiteilung des DSG 1978 in einen Abschnitt „öffentlicher Bereich“ und einen Abschnitt „privater Bereich“. Die Bestimmungen des DSG gelten nunmehr sowohl für Auftraggeber

des öffentlichen Bereiches als auch des privaten Bereiches, wobei für den öffentlichen Bereich vielfach Sonderbestimmungen vorgesehen sind.

Ein öffentlich rechtlicher Auftraggeber liegt vor, wenn er in Formen des öffentlichen Rechtes eingerichtet ist, Organ einer Gebietskörperschaft ist oder zwar in Formen des Privatrechtes eingerichtet ist, aber in Vollziehung der Gesetze tätig ist. Alle anderen Auftraggeber sind solche des privaten Bereiches.

VERWENDUNG VON DATEN (VERARBEITUNG UND ÜBERMITTLUNG)

GRUNDSÄTZE:

Daten dürfen nur nach **Treu und Glauben** und auf **rechtmäßige Weise** verwendet werden; sie dürfen nur für **festgelegte, eindeutige und rechtmäßige Zwecke** ermittelt werden.

Daten dürfen nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden. Eine Weiterverwendung für **wissenschaftliche** und **statistische Zwecke** ist unter den im DSG geregelten Voraussetzungen zulässig.

Die Daten müssen für den Zweck der Datenanwendung wesentlich sein und ihre Verwendung darf über diesen Zweck nicht hinausgehen; sie müssen so verwendet werden, dass sie **im Ergebnis sachlich richtig sind** und, **wenn nötig, auf den neuesten Stand gebracht sind**.

Eine Aufbewahrung in personenbezogener Form ist so lange erlaubt, als das für die Erreichung der Zwecke erforderlich ist.

Ausnahmen sind aufgrund gesetzlicher oder archivrechtlicher Vorschriften möglich.

Der Auftraggeber trägt bei jeder seiner Datenanwendungen die Verantwortung für die Einhaltung der Grundsätze betreffend die Verwendung von Daten; auch dann, wenn er für die Datenanwendung **Dienstleister** heranzieht.

Auftraggeber, die nicht im EU-Bereich angesiedelt sind, haben einen österreichischen Verantwortlichen zu benennen.

Zur näheren Festlegung, was in einzelnen Bereichen als **Verwendung von Daten nach Treu und Glauben** anzusehen ist, können für den privaten Bereich **gesetzliche Interessenvertretungen, sonstige Berufsverbände oder vergleichbare Einrichtungen** Verhaltensregeln ausarbeiten.

ZULÄSSIGKEIT DER VERWENDUNG VON DATEN:

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

Daten dürfen nur **übermittelt** werden, wenn sie aus einer zulässigen Datenanwendung stammen und der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis betreffend den Übermittlungszweck glaubhaft macht und durch Zweck und Inhalt der Übermittlung schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

Die Zulässigkeit einer Datenverwendung ist gegeben, wenn die dabei verursachten Eingriffe in das Grundrecht auf Datenschutz nur im erforderlichen Ausmaß und mit den geringsten zur Verfügung stehenden Mitteln erfolgen und die Grundsätze der Verwendung von Daten eingehalten werden.

WANN WERDEN SCHUTZWÜRDIGE GEHEIMHALTUNGSINTERESSEN NICHT VERLETZT:

BEI VERWENDUNG NICHT SENSIBLER DATEN, WENN

- eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung der Daten besteht oder
- der Betroffene der Verwendung seiner Daten zugestimmt hat; **Widerruf** ist jederzeit möglich, oder
- lebenswichtige Interessen des Betroffenen die Verwendung erfordern oder
- überwiegend berechnete Interessen des Auftraggebers oder eines Dritten die Verwendung erfordern, insbesondere dann, wenn die Verwendung der Daten
 - für einen Auftraggeber des **öffentlichen Bereiches** eine wesentliche Voraussetzung für die Wahrnehmung einer ihm gesetzlich übertragenen Aufgabe ist oder
 - durch Auftraggeber des **öffentlichen Bereiches** in Erfüllung der Verpflichtung zur Amtshilfe geschieht oder
 - zur Wahrung lebenswichtiger Interessen eines Dritten erforderlich ist oder
 - zur Erfüllung einer vertraglichen

Verpflichtung zwischen Auftraggeber und Betroffenen erforderlich ist oder

- zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
- ausschließlich die Ausübung einer öffentlichen Funktion durch den Betroffenen zum Gegenstand hat
- zulässigerweise veröffentlichte Daten oder indirekt personenbezogene Daten (Recht auf **Widerruf** – siehe später) verwendet werden
- die Verwendung von Daten über
 - gerichtlich oder verwaltungsbehördlich strafbare Handlungen oder Unterlassungen
 - den Verdacht der Begehung von Straftaten
 - strafrechtliche Verurteilungen
 - vorbeugende Maßnahmen verstößt dann nicht gegen schutzwürdige Geheimhaltungsinteressen, wenn
 - eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung dieser Daten besteht oder
 - die Verwendung der Daten für Auftraggeber des öffentlichen Bereiches eine wesentliche Voraussetzung zur Wahrnehmung einer ihnen gesetzlich übertragenen Aufgabe ist oder
 - sich die Zulässigkeit der Verwendung aus gesetzlichen Sorgfaltspflichten oder sonstigen berechtigten, die Geheimhaltungsinteressen des Betroffenen überwiegenden Interessen des Auftraggebers ergibt.

BEI VERWENDUNG SENSIBLER DATEN, WENN

- der Betroffene die Daten offenkundig selbst öffentlich gemacht hat oder
- die Daten in nur indirekt personenbezogener Form verwendet werden oder
- sich die Ermächtigung oder Verpflichtung zur Verwendung aus gesetzlichen Vorschriften ergibt, soweit diese der Wahrung eines wichtigen öffentlichen Interesses dienen (Mitteilung an die EU-Kommission)
- die Verwendung durch Auftraggeber des **öffentlichen Bereiches** im Rahmen der Amtshilfe geschieht oder
- Daten verwendet werden, die ausschließlich die Ausübung einer öf-

fentlichen Funktion durch den Betroffenen zum Gegenstand haben oder

- der Betroffene seine Zustimmung ausdrücklich erteilt hat; **Widerruf** ist jederzeit möglich, oder
- die Verarbeitung oder Übermittlung zur Wahrung lebenswichtiger Interessen des Betroffenen notwendig ist und seine Zustimmung nicht rechtzeitig eingeholt werden kann oder
- die Verwendung der Daten zur Wahrung lebenswichtiger Interessen eines anderen notwendig ist oder
- die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden oder
- Daten für **private Zwecke** oder für wissenschaftliche Forschung oder Statistik oder zur Benachrichtigung oder Befragung des Betroffenen verwendet werden oder
- die Verwendung erforderlich ist, um den Rechten und Pflichten des Auftraggebers nach Arbeits- oder Dienstrecht Rechnung zu tragen; Befugnisse des Betriebsrates bleiben unberührt oder
- die Daten für Gesundheitsvorsorge, medizinische Diagnostik, Gesundheitsversorgung oder -behandlung oder Verwaltung von Gesundheitsdiensten erforderlich sind und die Verwendung durch ärztliches Personal oder Personen erfolgt, die der Geheimhaltungspflicht unterliegen oder
- nicht auf Gewinn gerichtete Vereinigungen mit politischem, philosophischem, religiösem oder gewerkschaftlichem Tätigkeitszweck Daten, die Rückschlüsse auf politische Meinung oder weltanschauliche Überzeugung natürlicher Personen zulassen, im Rahmen ihrer erlaubten Tätigkeit verarbeiten; es muss sich dabei um Daten von Mitgliedern, Förderern oder sonstigen Personen handeln, 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.

HERANZIEHUNG EINES DIENSTLEISTERS

Auftraggeber dürfen bei ihren Datenanwendungen Dienstleister in An-

spruch nehmen; der Dienstleister muss eine ausreichende Gewähr für eine rechtmäßige und sichere Datenverwendung bieten; der Auftraggeber hat mit dem Dienstleister die dafür notwendigen Vereinbarungen zu treffen und sich von ihrer Einhaltung zu überzeugen.

PFLICHTEN DES DIENSTLEISTERS:

Er hat, unabhängig von vertraglichen Vereinbarungen, die Daten ausschließlich im Rahmen der Aufträge des Auftraggebers zu verwenden (die Übermittlung der verwendeten Daten ohne Auftrag ist verboten) und alle erforderlichen Datensicherheitsmaßnahmen (siehe später) zu treffen. Für die Dienstleistung dürfen nur solche Mitarbeiter herangezogen werden, die sich dem Dienstleister gegenüber zur Einhaltung des Datenheimnisses verpflichtet haben oder einer gesetzlichen Verschwiegenheitspflicht unterliegen.

Weitere Dienstleister dürfen nur mit Billigung des Auftraggebers herangezogen werden.

Der Dienstleister hat die notwendigen organisatorischen und technischen Voraussetzungen im Einvernehmen mit dem Auftraggeber für die Erfüllung der Auskunft-, Richtigstellungs- und Löschungspflichten des Auftraggebers zu schaffen und nach Beendigung der Dienstleistung entweder alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, an den Auftraggeber zu übergeben oder in seinem Auftrag aufzubewahren oder sie zu vernichten.

Alle Informationen, die zur Kontrolle der Einhaltung dieser Verpflichtungen notwendig sind, sind dem Auftraggeber zur Verfügung zu stellen.

DATENSICHERHEIT

DATENSICHERHEITSMASSNAHMEN:

Für alle Organisationseinheiten eines Auftraggebers oder Dienstleisters, die Daten verwenden, sind Maßnahmen zur Datensicherheit zu treffen. Nach Art der verwendeten Daten, Umfang und Zweck der Verwendung und unter Bedachtnahme auf den Stand der technischen Möglichkeiten und die wirtschaftliche Vertretbarkeit ist sicherzustellen, dass die Daten vor zufälliger oder unrechtmäßiger Zerstörung und vor Verlust geschützt sind und ihre Verwendung ordnungsgemäß erfolgt und Unbefugten nicht zugänglich werden.

FOLGENDE DATENSICHERUNGSMASSNAHMEN KOMMEN INSBESONDERE IN FRAGE:

- Festlegung der Aufgabenverteilung bei der Datenverwendung zwischen den Organisationseinheiten und den Mitarbeitern
 - Bindung der Verwendung von Daten an gültige Aufträge der anordnungsbefugten Organisationseinheiten und Mitarbeiter
 - Belehrung der Mitarbeiter über Datenschutz- und Datensicherheitsvorschriften
 - Regelung der Zutrittsberechtigung zu den Räumlichkeiten des Dienstleisters oder Auftraggebers
 - Regelung der Zugriffsberechtigung auf Daten und Programme
 - Regelung des Schutzes der Datenträger vor Einsicht und Verwendung durch Unbefugte
 - Festlegung der Berechtigung zum Betrieb der Datenverarbeitungsgeräte
 - Absicherung jedes Gerätes durch Vorkehrungen bei den eingesetzten Maschinen und Programmen gegen unbefugte Inbetriebnahme
 - Führen eines Protokolls, um die tatsächlich durchgeführten Verwendungsvorgänge, insbesondere Änderungen, Abfragen und Übermittlungen, auf ihre Zulässigkeit nachzuvollziehen
 - Führen einer Dokumentation über die getroffenen Maßnahmen zum Zweck der Erleichterung der Kontrolle und Beweissicherung
- Protokoll- und Dokumentationsdaten sind **drei Jahre** aufzubewahren. Abweichungen sind möglich, wenn der Datenbestand zulässigerweise früher gelöscht oder länger aufbewahrt wird.

Datensicherheitsvorschriften sind so zu erlassen und zur Verfügung zu halten, dass sich die Mitarbeiter über die für sie geltenden Regelungen jederzeit informieren können. Keiner Protokollierung bedürfen Übermittlungen, die in einer Standardverordnung bzw. Musterverordnung (siehe später) vorgesehen sind. Nicht registrierte Übermittlungen aus Datenanwendungen, die einer Verpflichtung zur Auskunftserteilung (siehe später) unterliegen, sind so zu protokollieren, dass dem Betroffenen Auskunft gegeben werden kann.

DATENGEHEIMNIS

Auftraggeber, Dienstleister und deren Mitarbeiter (Arbeitnehmer, Dienstnehmer, Personen in einem

arbeiterähnlichen – dienstnehmerähnlichen Verhältnis) haben Daten aus Datenanwendungen, die ihnen ausschließlich aufgrund ihrer berufsmäßigen Beschäftigung anvertraut wurden oder zugänglich geworden sind, unbeschadet sonstiger Verschwiegenheitspflichten geheim zu halten, außer es besteht ein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten. Mitarbeiter dürfen Daten nur aufgrund einer ausdrücklichen Anordnung ihres Arbeitgebers übermitteln. Auftraggeber und Dienstleister haben ihre Mitarbeiter vertraglich zu verpflichten, dass diese Daten aus Datenanwendungen nur aufgrund von Anordnungen übermitteln und das Datengeheimnis auch nach Beendigung des Arbeitsverhältnisses einhalten werden.

Auftraggeber und Dienstleister dürfen Anordnungen zur Übermittlung von Daten nur erteilen, wenn dies gesetzlich zulässig ist und haben die von der Anordnung betroffenen Mitarbeiter über die geltenden Übermittlungsanordnungen und über die Folgen einer Verletzung des Datenheimnisses zu belehren. Mitarbeitern dürfen aus einer Verweigerung der Befolgung einer Anordnung zur Datenübermittlung wegen Verstoßes gegen das DSGVO keine Nachteile erwachsen.

Must er

VERPFLICHTUNGSERKLÄRUNG GEM. § 15 DSGVO 2000

Ich verpflichte mich, das Datengeheimnis gemäß den Bestimmungen des DSGVO 2000 zu wahren, insbesondere personenbezogene Daten aus Datenanwendungen, die mir zugänglich geworden sind oder die mir aufgrund meiner berufsmäßigen Beschäftigung anvertraut wurden, unbeschadet sonstiger gesetzlicher Verschwiegenheitspflichten geheim zu halten, soweit kein rechtlich zulässiger Grund für eine Übermittlung der anvertrauten oder zugänglich gewordenen Daten besteht.

Mir ist bekannt, dass es insbesondere untersagt ist, unbefugten Personen oder unzuständigen Stellen Daten zu übermitteln oder auf welche Weise immer Kenntnis über Daten zu verschaffen oder diese sonst missbräuchlich zu verwenden. Vor allem verpflichte ich mich, Daten nur auf-

grund einer ausdrücklichen Anordnung zu übermitteln.

Ebenso verpflichte ich mich, das Datengeheimnis auch nach Beendigung meines Auftragsverhältnisses bedingungslos einzuhalten und nehme zur Kenntnis, dass ein Verstoß dagegen (verwaltungs-)strafrechtliche Folgen nach sich ziehen kann und allenfalls schadenersatzrechtliche Konsequenzen nach sich zieht.

Selbstverständlich sind von dieser Verpflichtung auch meine Dienstnehmer sowie alle Personen, die zu mir in einem arbeitsähnlichen bzw. dienstnehmerähnlichen Verhältnis stehen, erfasst.

DATENVERKEHR MIT DEM AUSLAND

Soweit der Datenverkehr mit dem Ausland nicht **genehmigungsfrei** ist, hat der Auftraggeber vor der Übermittlung oder Überlassung von Daten in das Ausland die Genehmigung der Datenschutzkommission einzuholen.

ÜBERMITTLUNGEN UND ÜBERLASSUNGEN VON DATEN IN DAS AUSLAND SIND GENEHMIGUNGSFREI

- wenn diese an Empfänger in Mitgliedstaaten der Europäischen Union oder an Empfänger in Drittstaaten mit angemessenem Datenschutz erfolgen; aufgrund der Verordnung des Bundeskanzlers, BGBl. 1999 II/521 (DatenschutzangemessenheitsVO) derzeit lediglich Schweiz und Ungarn.
- wenn die Daten im Inland zulässigerweise veröffentlicht wurden;
- wenn die Daten für den Empfänger nur indirekt personenbezogen sind;
- wenn der Datenverkehr in Rechtsvorschriften vorgesehen ist (diese müssen Gesetzesrang haben und unmittelbar anwendbar sein);
- wenn die Daten aus Datenanwendungen für private Zwecke übermittelt werden; d. h. die Daten wurden für ausschließlich persönliche oder familiäre Tätigkeiten verarbeitet und wurden vom Betroffenen selbst mitgeteilt oder sind sonst rechtmäßigerweise zugekommen. Die Übermittlung solcher Daten für andere Zwecke bedarf der Zustimmung des Betroffenen, außer es ist gesetzlich etwas anderes vorgesehen;
- wenn die Daten für publizistische

Zwecke übermittelt werden;

- wenn der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung gegeben hat;
- wenn ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten in das Ausland erfüllt werden kann;
- wenn die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden;
- wenn die Übermittlung oder Überlassung in einer Standardverordnung oder Musterverordnung ausdrücklich angeführt ist (siehe später);
- wenn es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt;
- wenn der Datenverkehr aus Datenanwendungen erfolgt, die von der Meldepflicht ausgenommen sind; das sind Datenanwendungen für Zwecke des Schutzes der verfassungsmäßigen Einrichtungen der Republik Österreich, der Sicherung der Einsatzbereitschaft des Bundesheeres, der Sicherstellung der umfassenden Landesverteidigung, des Schutzes wichtiger außenpolitischer, wirtschaftlicher oder finanzieller Interessen der Republik Österreich oder der Europäischen Union, der Vorbeugung, Verhinderung oder Verfolgung von Straftaten.

PUBLIZITÄT VON DATENANWENDUNGEN

MELDEPFLICHT DES AUFTRAGGEBERS:

Jeder Auftraggeber hat vor Aufnahme einer Datenanwendung eine **Meldung** an die Datenschutzkommission zum Zweck der Registrierung im Datenverarbeitungsregister zu erstatten. Ausnahme:

- Es handelt sich um Datenanwendungen, die **nicht meldepflichtig** sind,
- weil sie ausschließlich veröffentlichte Daten enthalten,
 - die Führung von Registern oder Verzeichnissen zum Inhalt haben, die von Gesetzes wegen öffentlich einsehbar sind,
 - nur indirekt bezogene Daten enthalten,
 - von natürlichen Personen aus-

schließlich für persönliche oder familiäre Tätigkeiten vorgenommen werden (Für ausschließlich persönliche oder familiäre Tätigkeiten dürfen natürliche Personen Daten verarbeiten, wenn sie ihnen vom Betroffenen selbst mitgeteilt wurden oder ihnen sonst rechtmäßigerweise zugekommen sind. Diese Daten dürfen, soweit gesetzlich nichts anderes vorgesehen ist, für andere Zwecke nur mit Zustimmung des Betroffenen übermittelt werden.),

- für publizistische Zwecke vorgenommen werden,
- einer Standardverordnung entsprechen.

Durch Verordnung des Bundeskanzlers können Typen von Datenanwendungen und Übermittlungen aus diesen zu **Standardanwendungen** erklärt werden.

Voraussetzung:

Sie müssen von einer großen Anzahl von Auftraggebern in gleichartiger Weise vorgenommen werden und angesichts des Verwendungszweckes und der verarbeiteten Datenarten, muss die Gefährdung schutzwürdiger Geheimhaltungsinteressen der Betroffenen unwahrscheinlich sein.

WELCHE DATENANWENDUNGEN UNTERLIEGEN EINER VEREINFACHTEN MELDUNG:

Durch Verordnung des Bundeskanzlers können **Musteranwendungen** festgelegt werden.

Voraussetzung:

Eine größere Anzahl von Auftraggebern hat gleichartige Datenanwendung vorzunehmen und die Voraussetzungen für die Erklärung zur Standardanwendung liegen nicht vor. Für eine Übergangszeit bis längstens **30. 6. 2000** gelten die in der bisherigen Standardverordnung (BGBl. 1987/261) geregelten Datenverarbeitungen als Musteranwendungen im Sinne des DSG 2000. Spätestens ab diesem Zeitpunkt muss eine neue Standard- und Musterverordnung in Kraft treten (die Wirtschaftskammer Steiermark wird davon zeitgerecht informieren).

WANN KANN DIE VERARBEITUNG AUFGENOMMEN WERDEN:

Der Vollbetrieb darf unmittelbar nach Abgabe der Meldung aufgenommen werden.

Bestimmte Arten von Datenanwendungen dürfen aber erst – sofern sie nicht einer Musteranwendung ent-

sprechen – nach ihrer Prüfung durch die Datenschutzkommission aufgenommen werden. Das ist die sogenannte **Vorabkontrolle**. Es handelt sich dabei um Datenanwendungen, die sensible bzw. strafrechtlich relevante Daten enthalten, die Auskunftserteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben bzw. in Form eines Informationsverbundsystems durchgeführt werden sollen.

MELDUNGEN AN DAS DATENVERARBEITUNGSREGISTER:

Eingerichtet bei der Datenschutzkommission (DSK) 1010 Wien, Bäckerstraße 20, Tel. 01/513 26 77-0. Die Meldungen sind mittels Formblättern durchzuführen, die beim Datenverarbeitungsregister erhältlich sind. Sie sind auch über Internet abrufbar (www.austria.gv.at/regierung/VD/V3dok.htm#DVR). Eine Meldung ist auch auf elektronischem Weg möglich: E-Mail: dvr-post@oestat.gv.at. Alle Eingaben sind von Bundesstempelgebühren und Bundesabgaben befreit. Jeder Auftraggeber bekommt bei der erstmaligen Registrierung eine Datenverarbeitungsregisternummer (DVR-Nr.) zugeteilt, die er auf allen Schriftstücken oder sonstigen Mitteilungen (z. B. E-Mail) an die Betroffenen anzugeben hat.

INFORMATIONSPFLICHT DES AUFTRAGGEBERS

Die aufgrund der Datenschutzrichtlinie erforderliche Informationspflicht des Auftraggebers stellt eine der wesentlichsten Neuerungen des DSG 2000 dar.

Aus Anlass der Übermittlung von Daten hat der Auftraggeber einer Datenanwendung die Betroffenen in geeigneter Weise zu informieren; und zwar über den Zweck der Datenanwendung, für die die Daten ermittelt werden sowie über Name und Adresse des Auftraggebers, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen. Darüber hinausgehende Informationen sind dann zu geben, wenn das für eine Verarbeitung nach **Treu und Glauben** erforderlich ist.

Dies ist insbesondere dann der Fall, wenn gegen die beabsichtigte Verarbeitung oder Übermittlung von Daten ein **Widerspruchsrecht** des Betroffenen besteht (siehe später) oder

es für den Betroffenen nicht klar erkennbar ist, ob er zur Beantwortung der gestellten Fragen verpflichtet ist oder Daten in einem Informationsverbundsystem verarbeitet werden sollen, ohne dass dies gesetzlich vorgesehen ist.

Bei Datenanwendungen, die nicht meldepflichtig sind, entfällt die Informationspflicht.

PFLICHT ZUR OFFENLEGUNG DER IDENTITÄT DES AUFTRAGGEBERS

Bei Übermittlungen und Mitteilungen an Betroffene hat der Auftraggeber seine Identität in geeigneter Weise offenzulegen, um dem Betroffenen die Verfolgung seiner Rechte zu ermöglichen.

Bei **meldepflichtigen** Datenanwendungen ist in Mitteilungen an Betroffene die **Registernummer** des Auftraggebers anzuführen.

RECHTE DES BETROFFENEN

Das DSG nennt als Rechte des Betroffenen ausdrücklich das Auskunftsrecht, das Recht auf Richtigstellung oder Löschung sowie das Widerspruchsrecht.

AUSKUNFTSRECHT:

Auf schriftliches Verlangen des Betroffenen und unter Nachweis seiner Identität hat der Auftraggeber dem Betroffenen binnen acht Wochen Auskunft über die zu seiner Person verarbeiteten Daten zu geben; mit Zustimmung des Betroffenen genügt auch ein mündliches Auskunftsbegehren.

Die Auskunft hat anzuführen:

- die verarbeiteten Daten
- die verfügbaren Informationen über ihre Herkunft
- allfällige Empfänger oder Empfängerkreise von Übermittlungen
- den Zweck der Datenverwendung
- die Rechtsgrundlagen der Datenverwendung in allgemein verständlicher Form
- auf Verlangen des Betroffenen auch Namen und Adresse von Dienstleistern

Wenn der Betroffene zustimmt, ist auch eine mündliche Auskunft mit der Möglichkeit der Einsichtnahme bzw. Abschrift oder Ablichtung möglich.

Für Zwecke der Auskunftserteilung sind **nicht** registrierte Übermittlungen entsprechend zu protokollieren. Übermittlungen, die in der Standard- oder Musterverordnung angeführt

sind, bedürfen keiner Protokollierung.

Die Auskunft ist nicht zu erteilen, wenn dies zum Schutz des Betroffenen aus besonderen Gründen notwendig ist bzw. wenn dem überwiegende berechnete Interessen des Auftraggebers oder eines Dritten oder überwiegende öffentliche Interessen entgegenstehen. Über Befragen hat der Betroffene am Auskunftsverfahren im zumutbaren Ausmaß mitzuwirken, um un gerechtfertigten und unverhältnismäßigen Aufwand beim Auftraggeber zu vermeiden.

Die Frist zur Auskunftserteilung beträgt acht Wochen.

Die Auskunft ist unentgeltlich zu erteilen, wenn sie den aktuellen Datenbestand einer Datenanwendung betrifft und der Betroffene im laufenden Jahr noch kein Auskunftsersuchen an den Auftraggeber zum selben Aufgabengebiet gestellt hat. In allen anderen Fällen kann ein **pauschalierter Kostenersatz von 260 Schilling**, der bei tatsächlich erwachsenen höheren Kosten höher sein kann, verlangt werden.

Das Recht auf Auskunft kann mittels Beschwerde an die Datenschutzkommission durchgesetzt werden. Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb von vier Monaten und bei einer Beschwerde an die DSK bis zum rechtskräftigen Abschluss des Verfahrens nicht vernichten.

RECHT AUF RICHTIGSTELLUNG ODER LÖSCHUNG:

Jeder Auftraggeber hat unrichtige oder entgegen den Bestimmungen des DSG verarbeitete Daten richtig zu stellen oder zu löschen; entweder aus eigenem, sobald ihm die Unrichtigkeit oder Unzulässigkeit ihrer Verarbeitung bekannt geworden ist, oder auf begründeten Antrag des Betroffenen innerhalb von acht Wochen.

Der Pflicht zur Richtigstellung unterliegen nur solche Daten, deren Richtigkeit für den Zweck der Datenanwendung von Bedeutung ist.

Die Unvollständigkeit von Daten bewirkt dann einen Berichtigungsanspruch, wenn sich daraus die Unrichtigkeit der Gesamtinformation ergibt.

Werden Daten für den Zweck der Datenanwendung nicht mehr benötigt, gelten sie als unzulässig

verarbeitete Daten und sind zu löschen, außer ihre Archivierung ist rechtlich zulässig und der Zugang zu den Daten ist besonders geschützt. Der Beweis der Richtigkeit der Daten obliegt dem Auftraggeber, außer die Daten wurden ausschließlich aufgrund von Angaben des Betroffenen ermittelt.

WIDERSPRUCHSRECHT:

Soweit die Verwendung von Daten nicht gesetzlich vorgesehen ist, hat jeder Betroffene das Recht, gegen die Verwendung seiner Daten wegen Verletzung überwiegender schutzwürdiger Geheimhaltungsinteressen beim Auftraggeber der Datenanwendung **Widerspruch** zu erheben. Der Auftraggeber hat bei Vorliegen dieser Voraussetzungen die Daten des Betroffenen binnen **acht Wochen** aus seiner Datenanwendung zu löschen und allfällige Übermittlungen zu unterlassen. Gegen eine **nicht gesetzlich** angeordnete Aufnahme in eine öffentlich zugängliche Datei kann der Betroffene jederzeit auch ohne Begründung seines Begehrens **Widerspruch** erheben. Die Daten sind binnen acht Wochen zu löschen.

RECHTSSCHUTZEINRICHTUNGEN

Zur Durchsetzung von Datenschutzansprüchen sieht das DSG 2000 folgende Rechtsschutzeinrichtungen vor:

DATENSCHUTZKOMMISSION:

Kontrollbefugnisse:

Jedermann kann sich wegen einer behaupteten Verletzung seiner Rechte oder ihn betreffender Pflichten durch einen Auftraggeber bzw. Dienstleister mit einer Eingabe an die DSK wenden. Die DSK kann bei begründetem Verdacht auf Verletzung dieser Rechte und Pflichten Datenanwendungen überprüfen; Datenanwendungen, die der Vorabkontrolle unterliegen, dürfen auch ohne Vorliegen eines solchen Verdachtes überprüft werden.

Beschwerde an die DSK:

Die DSK ist auf Antrag des Betroffenen zuständig für Entscheidungen über behauptete Verletzungen des **Rechtes auf Auskunft** (sowohl für Auftraggeber des öffentlichen als auch des privaten Bereiches). Bei Verletzung der Rechte eines Betroffenen auf **Geheimhaltung, Rich-**

tigstellung oder Löschung entscheidet die DSK nur dann, wenn der Betroffene seine Beschwerde gegen einen Auftraggeber des **öffentlichen Bereiches** richtet, der nicht als Organ der Gesetzgebung oder Gerichtsbarkeit tätig ist.

ANRUFUNG DER GERICHTE:

Ansprüche gegen Auftraggeber des **privaten Bereiches** wegen Verletzung der Rechte des Betroffenen auf Geheimhaltung, Richtigstellung, Löschung sind auf dem Zivilrechtsweg geltend zu machen. Bei Verwendung von Daten entgegen den Bestimmungen des DSG hat der Betroffene Anspruch auf Unterlassung und Beseitigung des dem DSG widersprechenden Zustandes. Zur Sicherung der Ansprüche auf Unterlassung können einstweilige Verfügungen erlassen werden. Zuständig ist das Landesgericht, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat oder das Landesgericht, in dessen Sprengel der Auftraggeber oder Dienstleister seinen gewöhnlichen Aufenthalt oder Sitz hat.

SCHADENERSATZ:

Bei schuldhafter Verwendung von Daten durch einen Auftraggeber oder Dienstleister ist dem Betroffenen der Ersatz des erlittenen Schadens nach den Bestimmungen des ABGB zu leisten. Bei schwerwiegender rechtswidriger Datenverwendung, die mit Tatbeständen vergleichbar ist, die nach dem Mediengesetz zum Schadenersatz verpflichtet, ist auch der **immaterielle Schaden** (angemessene Entschädigung für die erlittene Kränkung) zu ersetzen; die Voraussetzungen und die Höhe der Entschädigung richten sich nach den Bestimmungen des Mediengesetzes.

STRAFBESTIMMUNGEN

DATENANWENDUNGEN IN GEWINN- ODER SCHÄDIGUNGS-ABSICHT:

Wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich aufgrund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich gemacht worden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder

veröffentlicht, obwohl der Betroffene an den Daten ein schutzwürdiges Geheimhaltungsinteresse hat, ist vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen. Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

VERWALTUNGSSTRAF-BESTIMMUNG:

Eine Verwaltungsübertretung, die mit **Geldstrafe bis zu 260.000 Schilling** zu ahnden ist, begeht, wer

- sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft
- einen erkennbar widerrechtlichen Zugang vorsätzlich aufrecht erhält
- Daten vorsätzlich in Verletzung des Datengeheimnisses übermittelt
- Daten, die für wissenschaftliche Forschung und Statistik oder im Rahmen der Zurverfügungstellung von Adressen anvertraut wurden, vorsätzlich für andere Zwecke verwendet
- Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht
- Daten unzulässigerweise vorsätzlich löscht

Ab dem Zeitpunkt der Kenntnis von einem Auskunftsverlangen darf der Auftraggeber Daten über den Betroffenen innerhalb eines Zeitraumes von vier Monaten, im Fall der Erhebung einer Beschwerde an die DSK bis zum rechtskräftigen Abschluss des Verfahrens nicht vernichten.

Eine Verwaltungsübertretung, die mit **Geldstrafe bis zu 130.000 Schilling** zu ahnden ist, begeht, wer

- Daten ermittelt, verarbeitet oder übermittelt, ohne die Meldepflicht erfüllt zu haben;
- Daten ins Ausland übermittelt oder überlässt, ohne die Genehmigung der DSK eingeholt zu haben;
- Offenlegungs- und Informationspflichten verletzt;
- erforderliche Sicherheitsmaßnahmen gröblich außer Acht lässt.

Der Versuch ist strafbar.

Der **Verfall** von Datenträgern und Programmen kann ausgesprochen werden, wenn diese Gegenstände mit einer Verwaltungsübertretung in Zusammenhang stehen.

Zuständig ist die Bezirksverwaltungsbehörde, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat.

BESONDERE VERWENDUNGSZWECKE VON DATEN

PRIVATE ZWECKE:

Für ausschließlich persönliche oder familiäre Tätigkeiten dürfen natürliche Personen Daten verarbeiten. Voraussetzung ist, dass ihnen diese Daten vom Betroffenen selbst mitgeteilt wurden oder sonst auf rechtmäßige Weise zugekommen sind. Für andere Zwecke dürfen diese Daten nur mit Zustimmung des Betroffenen übermittelt werden.

WISSENSCHAFTLICHE FORSCHUNG UND STATISTIK:

Für Zwecke wissenschaftlicher oder statistischer Untersuchungen, die keine personenbezogenen Ergebnisse zum Ziel haben, darf der Auftraggeber der Untersuchung alle Daten verwenden, die öffentlich zugänglich sind oder für andere Untersuchungen oder andere Zwecke zulässigerweise ermittelt wurden oder für den Auftraggeber nur indirekt personenbezogen sind. Für andere Datenanwendungen dürfen Daten für Zwecke wissenschaftlicher Forschung und Statistik nur verwendet werden, wenn besondere gesetzliche Vorschriften das zulassen oder der Betroffene zustimmt oder eine Genehmigung der DSK vorliegt. Der direkte Personenbezug ist unverzüglich zu verschlüsseln, wenn bei der Arbeit auch mit nur indirekt personenbezogenen Daten das Auslangen gefunden werden kann. Ist der Personenbezug der Daten für die wissenschaftliche oder statistische Arbeit nicht mehr notwendig, ist er gänzlich zu beseitigen.

ZURVERFÜGUNGSTELLUNG VON ADRESSEN ZUR BENACHRICHTIGUNG UND BEFRAGUNG VON BETROFFENEN:

Die Übermittlung von Adressdaten eines bestimmten Kreises von Betroffenen zum Zweck ihrer Benachrichtigung oder Befragung bedarf, soweit gesetzlich nicht ausdrücklich anderes bestimmt ist (z. B. § 268 GewO 1994, hinsichtlich der Adressenverlage und Direktwerbeunternehmen), der **Zustimmung** der Betroffenen. Diese Zustimmung kann ausnahmsweise entfallen, wenn aufgrund der Auswahlkriterien und des Gegenstandes der Benachrichtigung oder Befragung eine Beeinträchtigung der Geheimhaltungsinteressen der Betroffenen unwahrscheinlich ist und Daten desselben Auftraggebers ver-

wendet werden oder bei einer beabsichtigten Übermittlung der Adressdaten an Dritte an der Benachrichtigung oder Befragung ein öffentliches Interesse besteht oder wenn der Betroffene nach entsprechender Information keinen Widerspruch gegen die Übermittlung erhoben hat.

Bei Nichtvorliegen dieser Voraussetzungen ist eine Übermittlung der Adressdaten auch mit Genehmigung der DSK zulässig (bei einem wichtigen Interesse des Betroffenen selbst, bei wichtigem öffentlichem Benachrichtigungs- oder Befragungsinteresse sowie zur Befragung der Betroffenen für wissenschaftliche oder statistische Zwecke).

Die übermittelten Adressdaten dürfen ausschließlich nur für den genehmigten Zweck verwendet werden.

Sie sind zu löschen, wenn sie für die Benachrichtigung oder Befragung nicht mehr benötigt werden.

AUTOMATISIERTE EINZELENTSCHEIDUNGEN:

Durch diese Neuregelung soll verhindert werden, dass wertende Entscheidungen, die einzelne Aspekte von Personen betreffen, ausschließlich aufgrund eines automatisiert ablaufenden Computerprogramms vorgenommen werden.

Demzufolge darf niemand einer für ihn rechtliche Folgen nach sich ziehenden oder einer ihn erheblich beeinträchtigenden Entscheidung unterworfen werden, die ausschließlich aufgrund einer automationsunterstützten Verarbeitung von Daten zum Zweck einzelner Aspekte seiner Person ergeht (wie z. B. berufliche Leistungsfähigkeit, Kreditwürdigkeit, Zuverlässigkeit, Verhalten).

INFORMATIONSVORBUND-SYSTEME:

Obwohl dies von der Datenschutzrichtlinie nicht vorgegeben ist, enthält das DSG 2000 besondere Vorschriften für die Verarbeitung von Daten in Form eines „Informationsverbundsystems“. Ein solches Informationsverbundsystem liegt vor, wenn alle Teilnehmer die ihnen in einem bestimmten Bereich vorliegende Information in das System einspeichern und alle Auftraggeber auch auf jene Daten im System Zugriff haben, die von den anderen Teilnehmern dem System zur Verfügung gestellt wurden. Beispiele für derartige Systeme finden sich etwa

im Tourismusbereich (Flugreservierung, Zimmervermittlung) oder auch in der öffentlichen Verwaltung (Informationsverbundsysteme zur Verbrechensbekämpfung). Das DSG 2000 betrachtet diese Systeme als datenschutzrechtlich besonders heikel und sieht daher die Vorabkontrolle durch die Datenschutzkommission für sie vor. Die Datenschutzkommission kann in diesem Bereich auch besondere Auflagen für den Betrieb verfügen. Für Informationsverbundsysteme, die nicht gesetzlich vorgesehen sind, ist eine erweiterte Informationspflicht des Auftraggebers vorgesehen.

Für jedes Informationsverbundsystem ist ein Betreiber zu bestellen, der alle Auskünfte zu geben hat, die notwendig sind, um den für die Verarbeitung der Daten des Betroffenen im System verantwortlichen Auftraggeber festzustellen und der für die Datensicherheit im System verantwortlich ist.

INKRAFTTRETEN, ÜBERGANGSREGELN

Das DSG 2000 ist am **1. 1. 2000** in Kraft getreten.

Alle Meldungen und Registrierungen, die noch aufgrund der Rechtslage nach dem DSG 1978 vorgenommen wurden, gelten weiter, es sei denn, sie sind wegen Entfalls von Meldepflichten gegenstandslos geworden.

Neu zu beantragen – und zwar vor dem 1. 1. 2003 – sind Genehmigungen für den Datenverkehr mit dem Ausland.

Manuelle Datenanwendungen, die neu aufgenommen werden, sind sofort zu melden.

Manuelle Datenanwendungen, die bereits zum Zeitpunkt des Inkrafttretens des DSG bestanden haben, sind bis spätestens 1. 1. 2003 zu melden.

Für weitere Auskünfte steht die Abteilung für Rechtspolitik der Wirtschaftskammer Steiermark, Tel. 0 31 6/601-665, gerne zur Verfügung.