Version 4.10.2001

Das Datenschutzgesetz 2000 - Eine Herausforderung für den Kaufhausdetektiv

"Die Berufsdetektive sind in der Aufklärung von Betrugsfällen, Diebstählen und Betriebsspionage tätig. Sie spüren Schuldner und abgängige Jugendliche auf, überprüfen Dienstnehmer, beschaffen Beweismittel in Zivil- und Strafprozessen und klären Verschuldensfragen bei Ehescheidungen sowie Verleumdungen. Ein weiterer Bereich ist der Personenschutz sowie Sicherheitsanalysen und -konzepte."[1]

Wie diese - unvollständige - Aufzählung der Tätigkeitsbereiche[2] nahe legt, beauftragen Rechtsanwälte, Unternehmer und Privatpersonen aus den verschiedensten Gründen Berufsdetektive[3]. Dem Detektiv stehen bei seiner Tätigkeit im Vergleich zu anderen Staatsbürgern keine Sonderrechte zu, er hat bei der Ausübung seines Gewerbes mannigfaltige gesetzliche Vorschriften zu befolgen. Besondere Beachtung soll im Folgenden der mitunter schwierigen Einhaltung des Datenschutzgesetzes[4] bei der Beobachtung von Kunden durch Detektive in Geschäftslokalen gewidmet werden. Die dabei zu beachtenden Grundsätze gelten auch für andere Tätigkeitsbereiche von Berufsdetektiven sinngemäß.

Beobachtung von Kunden im Geschäftslokal:

Abgesehen von Wien, wo in der Vorweihnachtszeit Kriminalbeamte sporadisch in Einkaufszentren, großen Kaufhäusern, Einkaufspassagen und den bekannten Einkaufsstrassen Kaufhaus- und Taschendiebstähle zu verhindern suchen, gibt es meines Wissens in keinem weiteren Bundesland präventive Unterstützung von Unternehmen durch die Sicherheitsbehörden. Dies erscheint auf Grund des damit verbundenen Personalaufwandes und der Kosten vor allem in

[1] Aus Facts Spezial, "Detektive: Bodyguards & Ermittlungsprofis" der Allgemeinen Fachgruppe des Gewerbes der Wirtschaftskammer Wien, 1030 Wien, Rudolf-Sallinger-Platz 1, Tel.: 51450/2203.

[2] Gemäß § 249 Abs. 1 GewO sind Berufsdetektive befugt, Auskünfte über Privatverhältnisse zu erteilen, Erhebungen über strafbare Handlungen vorzunehmen, Beweismittel für Zwecke eines gerichtlichen oder verwaltungsbehördlichen Verfahrens zu beschaffen, verschollene oder sich verborgen haltende Personen, Schreiber oder Absender anonymer Briefe, Urheber oder Verbreiter von Verleumdungen, Verdächtigungen oder Beleidigungen auszuforschen, die Treue von Arbeitnehmern zu beobachten und zu kontrollieren, Kunden in Geschäftslokalen zu beobachten und Personen zu schützen.

[3] § 253 GewO normiert die Bezeichnung "Berufsdetektiv" und schließt den Gebrauch anderer Berufsbezeichnungen und auch zustehender Amtstitel bei der Gewerbeausübung aus.

[4] Bundesgesetz über den Schutz personenbezogener Daten (Datenschutzgesetz 2000 - DSG 2000), BGBl. 1999/165.

Zeiten der Budgetkonsolidierung durchaus verständlich, stellt für betroffene Unternehmen jedoch eine nicht zu unterschätzende Herausforderung dar.

Während Taschendiebstähle dem Image eines Einkaufszentrums schaden und dadurch einkaufslustige Kunden abschrecken, stellen Ladendiebstähle für das betroffene Unternehmen eine positive Vermögensschädigungen dar. Um den Schwund an Ware möglichst gering zu halten, werden umfangreiche Sicherheitskonzepte ausgearbeitet, deren Ziel die Verhinderung der unbefugten Aneignung von Ware durch "Kunden" ist. So wird Handelsware mechanisch gesichert und/oder mit elektronischen Alarmetiketten versehen. Da sich in der Vergangenheit jedoch gezeigt hat, dass marktübliche Sicherungssystem von Profis relativ einfach und schnell deaktiviert bzw. umgangen werden können, engagieren gefährdete Unternehmen zusätzlich Berufsdetektive.[5]

Aufgabe des Berufsdetektivs ist dabei die Beobachtung von Kunden im Geschäftslokal.[6] Dafür installieren Detektive unter anderem stecknadelgroße Kameras in den Verkaufsräumen und beobachten Kunden über Monitors oder tarnen sich als einkaufende Kunden. Ziel dieser Aktivitäten ist es, einen Dieb[7] auf frischer Tat zu ertappen und sein Entkommen mit der Ware zu verhindern. Üblicherweise beobachtet der Detektiv den Verdächtigen bei der "Ansichnahme"[8] der Ware und dem Passieren der Kassa ohne zu bezahlen. Zwischen Kassa und Ausgang nimmt der Detektiv unter Vorweisung seines Ausweises eine Anhaltung nach § 86 Abs. 2 StPO[9] vor. Zur Vermeidung von Aufsehen wird er den Verdächtigen ersuchen, mit in ein Besprechungszimmer zu kommen, wo dieser aufgefordert wird, die Ware herauszugeben. Anschließend kommt es zur Aufnahme der Personaldaten des Verdächtigen.

---

[5] Der Detektiv wird dabei als selbständiger Unternehmer tätig; "Detektive" im Angestelltenverhältnis kommen recht selten vor.

[6] Siehe dazu § 249 Abs. 1 Z. 6 GewO.

[7] Als einschlägige Straftatbestände kommen §§ 127 ff StGB (Diebstahl), § 141 StGB (Entwendung) in Frage.

[8] Auf die unterschiedlichen Meinungen bezüglich des Zeitpunkts des Gewahrsambruchs kann hier nicht eingegangen werden.

[9] § 86 Abs. 2 StPO lautet: "Liegen hinreichende Gründe für die Annahme vor, dass eine Person eine mit gerichtlicher Strafe bedrohte Handlung ausführe, unmittelbar vorher ausgeführt habe, oder dass nach ihr wegen einer solchen Handlung gefahndet werde, so ist jedermann berechtigt, diese Person auf angemessene Weise anzuhalten. Er ist jedoch verpflichtet, die Anhaltung unverzüglich dem nächsten Sicherheitsorgan anzuzeigen."

An dieser Stelle ergeben sich die ersten datenschutzrechtlichen Anknüpfungspunkte.[10] Ist der Detektiv berechtigt, die Vorlage eines Personalausweises, Führerscheines u.ä. zu verlangen, kann sich der Verdächtige generell weigern Angaben zu seiner Identität zu machen und ist der Detektiv befugt, Erhebungen zur Identitätsfeststellung einzuleiten?

Feststellung der Identität:

Der Detektiv möchte die Identität des Verdächtigen festzustellen. Dazu ist er meist auf Grund des Vertragsverhältnisses mit seinem Auftraggeber (z.B. Kaufhausbetreiber)[11] verpflichtet. Wer die Praxis kennt, weiß, dass die Identitätsfeststellung sinnvollerweise durch Einsichtnahme in einen amtlichen Lichtbildausweis des Verdächtigen geschieht.

"Verlangt" der Detektiv die Vorlage eines Ausweises, wird das als Frage nach den Personaldaten des Betroffenen zu qualifizieren sein. Dies erscheint insofern unproblematisch, als es kein ausdrückliches Verbot gibt, diese konkrete Frage zu stellen.[12]

Auch wenn es zulässig ist, einen Verdächtigen nach seiner Identität zu fragen, bedeutet das nicht, dass dieser eine (wahrheitsgemäße) Antwort geben müsste. Weigert sich der Gefragte seine Identität preiszugeben, wird der Detektiv keine direkte Möglichkeit haben, dem zu begegnen. Im Ergebnis wird er nur die Sicherheitsbehörde verständigen können.

Da der Detektiv die Möglichkeit (bei Vorliegen einer Anhaltung nach § 86 Abs. 2 StPO sogar die Verpflichtung) hat, die Sicherheitsbehörde zu verständigen, welche die Identität des Verdächtigen feststellt und eine Anzeige

[10] "Datenschutz" meint den Schutz von Menschen vor den Folgen missbräuchlicher Datenverwendung, nicht den Schutz von Daten. Bezüglich der Entstehung des mittlerweile eingeführten, missverständlichen Begriffs vgl. *Cas/Peissl*, Beeinträchtigung der Privatsphäre in Österreich (Studie des Instituts für Technikfolgenabschätzung im Auftrag der Bundesarbeitskammer für Arbeiter und Angestellte (2000), 5).

[11] Weiters treten vielfach Betreiber von Einkaufszentren und Unternehmervereinigungen in Einkaufsstraßen und -passagen als Auftraggeber von Berufsdetektiven auf.

[12] Eine derartige Beschränkung des Fragerechts wird vielfach im Arbeitsrecht unter Hinweis auf die Fürsorgepflicht des Arbeitgebers im Verhältnis zum (potentiellen) Arbeitnehmer angenom-

aufnimmt, wird sich in der Praxis ein ertappter Ladendieb vermutlich nur in Ausnahmefällen tatsächlich weigern, seine Identität preiszugeben. Dies deshalb, weil ein gerichtliches Strafverfahren - außer bei Strafunmündigen[13] - wohl unausweichlich wären. Ist der Ladendieb hingegen kooperativ, kann dies durchaus dazu führen, dass von der Erstattung einer Anzeige Abstand genommen wird.[14]

Eigene Erkundungen des Detektivs mit dem Ziel, die Identität einer Person festzustellen, werden wohl nur in seltenen Fällen wirtschaftlich sinnvoll sein, so etwa dann, wenn diese Person einen beachtlichen Schaden verursacht hat,[15] jedoch nicht angehalten werden konnte, oder noch vor Aufnahme der Personalien flüchtet.

Die grundsätzliche Befugnis, die Identität eines Verdächtigen zu ermitteln, ergibt sich aus § 249 Abs. 1 Z. 3 GewO, wonach die Beschaffung von Beweismitteln für Zwecke eines gerichtlichen oder verwaltungsbehördlichen Verfahrens Berufsdetektiven vorbehalten ist.[16] Zwar handelt es sich bei Diebstahl und Sachbeschädigung um Tatbestände nach dem Strafgesetzbuch, woraus sich ein staatlicher Strafanspruch[17] ergibt, jedoch differenziert die Gewerbeordnung hier nicht zwischen Zivil- und Strafverfahren. Es ist somit durchaus zulässig, dass ein Detektiv Beweismittel für ein Strafverfahren erhebt, auch wenn er damit keine Entlastung des Beschuldigten zu erreichen sucht. Die detektivischen Standesregeln[18], nach welchen die Durchführung von Ermittlungen stets ein

---

men (siehe z.B. *Löschnigg* in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht (2000), 149 f). Unmündige betreffend ist kein Frageverbot normiert.

[13] Siehe dazu § 4 JGG, BGBl. Nr. 599/1988.

[14] So sehen Detektive üblicherweise bei der Betretung von Kindern und unmündigen Minderjährigen - ausgenommen bei Bandendiebstahl und bewusster Ausnützung der Strafunmündigkeit - von der Erstattung einer Anzeige ab. Mündige Minderjährige und Personen über 65 Jahre werden vielfach erst bei Erreichung eines branchenabhängigen Mindestwarenwertes zur Anzeige gebracht.

[15] z.B. Diebstahl von Schmuck, hochwertigen Kosmetika, Sachschaden durch Zerstörung von Warenpräsentationsvitrinen etc..

[16] Bezüglich der Befugnis von Sicherheitsbehörden personenbezogene Daten zu ermitteln (allgemein zu verwenden), siehe § 51 ff SPG.

[17] Beim Diebstahl nach § 127 ff StGB und der Sachbeschädigung nach § 125 f StGB handelt es sich um Offizialdelikte, die Entwendung (§ 141 StGB) ist hingegen ein Ermächtigungsdelikt, was bedeutet, dass der Täter nur mit Ermächtigung des Verletzen zu verfolgen ist. Bei der Entwendung ist das staatliche Strafverfolgungsrecht somit von der Erteilung der genannten Ermächtigung abhängig.

[18] Verbindliche Standesregeln wurden bisher weder in Verordnungswege erlassen, noch gibt es Empfehlungen der zuständigen Allgemeinen Fachgruppe Wien des Gewerbes der Wirtschafts-

berechtigtes Interesse des Auftraggebers voraussetzen, erscheinen nicht verletzt, da sich dieser nach § 47 StPO als Privatbeteiligter dem Strafverfahren anschließen kann, um seine zivilrechtlichen Ansprüche[19] geltend zu machen.

Der im Verfassungsrang stehende, mit unmittelbarer Drittwirkung[20] ausgestattete § 1 Abs. 1 DSG bestimmt jedoch, dass jedermann[21], insbesondere auch im Hinblick auf die Achtung seines Privat- und Familienlebens, Anspruch auf Geheimhaltung der ihn betreffenden personenbezogenen Daten hat, soweit daran ein schutzwürdiges Geheimhaltungsinteresse besteht.[22]

Personenbezogene Daten sind nach der Legaldefinition § 4 Z. 1 DSG solche, die Angaben über Betroffene[23], deren Identität bestimmt oder bestimmbar ist, machen. Bei Name, Geburtsdatum, Wohnadresse, Beruf etc. handelt es sich somit um (direkt)[24] personenbezogene Daten nach obiger Definition.

Das Grundrecht auf Datenschutz[25] schützt nicht nur vor Weitergabe personenbezogener Daten, sondern bereits vor deren Ermittlung.[26] Im Hinblick auf den

---

kammer Wien oder eines Detektivverbandes. Bei den Standesregeln handelt es sich somit um einen "allgemeinen Branchenkonsens".

[19] Dabei ist vor allem an den Schaden durch gestohlene oder beschädigte Ware und Einrichtung, aber auch an die konkreten Kosten der Beobachtung und Verfolgung des nunmehr Angeklagten durch den Detektiv zu denken, welche der Auftraggeber auf Grund der vertraglichen Vereinbarung vorerst zu tragen hat. Bezüglich der Ersatzfähigkeit von Überwachungskosten vgl. *Thiele*, Ersatz von Detektivkosten, RdW 1999, 769.

[20] Das Recht auf Datenschutz wendet sich nicht nur gegen staatliche Organe, sondern gilt auch für Rechtsbeziehungen von Privaten untereinander.

[21] Ein "Jedermannsrecht" schützt jede natürliche und juristische Person, unabhängig von der Staatsbürgerschaft. Bei juristischen Personen sind auch Wirtschaftsdaten geschützt (vgl. *Jahnel*, in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht (2000), 166).

[22] Vgl. auch Art. 8 Abs. 2 EMRK, BGBl. Nr. 210/1958.

[23] "Betroffener" ist gemäß § 4 Z. 3 DSG jede vom Auftraggeber (Z 4) verschiedene natürliche oder juristische Person oder Personengemeinschaft, deren Daten verwendet (Z 8) werden.
Wie *Duschanek*, ZfV 2000/1303 ausführt, geht das DSG 2000 mit der Einbeziehung juristischer Personen über Art. 2 lit a DSRL hinaus; doch erlaubt Erwägungsgrund 24 der DSRL den Mitgliedsstaaten auch die Erlassung von Datenschutzvorschriften zum Schutz juristischer Personen.

[24] Im Gegensatz zu den "indirekt personenbezogenen Daten", bei welchen der Personenbezug verschlüsselt ist, so dass der Verwender der Daten ohne Hilfe des Schlüsselinhabers mit vernünftigem Aufwand, insbesondere mit rechtlich zulässigen Mitteln, nicht im Stande ist, die Daten wieder konkreten Personen zuzuordnen. Von den indirekt personenbezogenen Daten sind "anonymisierte Daten" zu unterscheiden, bei denen es keinen Personenbezug gibt und welche von niemanden auf eine bestimmte Person zurückgeführt werden können. Anonymisierte Daten unterliegen nicht dem Datenschutzgesetz. (vgl. RV 1613 Anmerkung zu § 4 Z. 7).

[25] Wie *Jahnel* in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht (2000), 159 ff, ausführt, gibt es kein einheitliches Grundrecht auf Datenschutz, das Grundrecht auf Datenschutz besteht tatsächlich aus mehreren, unterschiedlichen Rechten, nämlich dem Recht auf Geheimhaltung personenbezogener Daten (§ 1 Abs. 1), dem Recht auf Auskunft (§ 1 Abs. 3 Z. 1), dem Recht

Stufenbau der Rechtsordnung, nach welcher Verfassungsbestimmungen einfachgesetzlichen Regelungen derogieren, könnte vordergründig argumentiert werden, der Detektiv sei trotz der (einfachgesetzlichen) Ermächtigung des § 249 GewO nicht befugt, die Identität des Verdächtigen zu erheben. Wie bereits angedeutet, besteht der Anspruch auf Geheimhaltung von personenbezogenen Daten jedoch nicht uneingeschränkt, sondern nur so weit, als ein schutzwürdiges Interesse des Betroffenen besteht.

Bezüglich des Vorliegens eines schutzwürdigen Interesses normiert § 1 Abs. 2 DSG als zulässige Ausnahme vom Geheimhaltungsschutz neben dem Vorliegen lebenswichtiger Interessen des Betroffenen und seiner Zustimmung zur Verwendung der Daten auch die Notwendigkeit zur Wahrung überwiegender berechtigter Interessen eines anderen[27] und führt die zu beachtenden Parameter für jene Eingriffe in das Grundrecht, die durch den hoheitlich auftretenden Staat erfolgen, nachfolgend aus. Bei Eingriffen hingegen, die nicht durch den "Staat", sondern durch einen privatrechtlich tätigen Detektiv erfolgen, bietet Abs. 2 lex.cit. keine näheren Anhaltspunkte dafür, wann ein berechtigtes Informationsinteresse eines anderen vorliegt, welches das schutzwürdige Geheimhaltungsinteresse des Betroffenen überwiegt. Diesbezüglich sind die einfachgesetzlichen Ausführungsbestimmungen zum Grundrecht, und zwar die §§ 8, 9 DSG, heranzuziehen.

Zulässigkeit der Datenermittlung:

Unter "Verwendung von Daten" ist gemäß § 4 Z. 8 DSG jede Art der Handhabung von Daten einer Datenverarbeitung, also sowohl das Verarbeiten (Z. 9) als auch das Übermitteln (Z. 12) zu verstehen.[28] § 4 Z. 9 DSG definiert das "Verar-

---

auf Richtigstellung unrichtiger Daten (§ 1 Abs. 3 Z. 2) und dem Recht auf Löschung unzulässigerweise verarbeiteter Daten (§ 1 Abs. 3 Z. 2).
Diese weiteren Rechte werden mitunter auch als "Begleitgrundrechte" bezeichnet, die der Durchsetzung des Grundrechts auf Geheimhaltung dienen.

[26] 1613 der Beilagen zu den stenographischen Protokollen des Nationalrates XX. GP, Erläuterungen zur Regierungsvorlage zu § 1 DSG: "Das Grundrecht auf Datenschutz bewirkt einen Anspruch auf Geheimhaltung personenbezogener Daten. Darunter ist der Schutz des Betroffenen vor Ermittlung seiner Daten und der Schutz vor der Weitergabe der über ihn ermittelten Daten zu verstehen."

[27] Als "anderer" gilt jede vom Betroffenen verschiedene natürliche oder juristische Person.

[28] Da § 6 Abs. 1 Z. 1 DSG festlegt, dass Daten nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden dürfen, sind davon alle Verarbeitungsschritte umfasst.

beiten von Daten" als Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten oder jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittelns von Daten. § 4 Z. 10 DSG definiert das Ermitteln von Daten umfassend als "das Erheben von Daten in der Absicht, sie in einer Datenanwendung zu verwenden".[29]

Wird die Identität einer Person ermittelt, handelt es sich demgemäss nur dann um eine Verwendung von Daten iS. § 4 Z. 8 DSG, wenn die Daten zumindest teilweise automationsunterstützt, also maschinell und programmgesteuert gehandhabt werden. Eine traditionelle, nicht automationsunterstützte Recherche fällt somit nicht unter die genannte Bestimmung.[30]

Bei der Prüfung der Zulässigkeit der Ermittlung von Daten sind zunächst die allgemeinen Grundsätze nach § 6 DSG zu beachten, § 7 enthält die Regeln für die Beurteilung der Zulässigkeit einer konkreten Datenanwendung, wobei zwischen Verarbeiten (Abs. 1) und Übermitteln (Abs. 2) unterschieden wird. Im Ergebnis ist somit eine zweistufige Zulässigkeitsprüfung durchzuführen. Zuerst ist der Zweck der Datenverarbeitung zu überprüfen und dann, ob schutzwürdige Geheimhaltungsinteressen des Betroffenen verletzt werden, wobei zwischen "nicht-sensiblen Daten" (§ 8) und "sensiblen Daten" (§ 9) unterschieden wird.

Treu und Glauben:

Gemäß § 6 Abs. 1 DSG dürfen Daten nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden. Zur Festlegung dessen, was als Verwendung von Daten nach Treu und Glauben anzusehen ist, sind gesetzliche Interessenvertretungen, sonstige Berufsverbände und vergleichbare Einrichtungen befugt, Verhaltensregeln auszuarbeiten, welche nach einer Begutachtung

[29] Dabei ist es unwesentlich, ob die Daten mit oder ohne Mitwirkung des Betroffenen erhoben bzw. auf sonstige Art beschafft werden. Ausschlaggebend ist, ob die ermittelten Daten der Erreichung eines berechtigten Zwecks dienen.

[30] § 58 DSG normiert jedoch, dass manuell geführte Dateien für Zwecke in denen die Gesetzgebung Bundessache ist, als Datenanwendungen iS. § 4 Z. 7 DSG gelten, wobei eine Meldepflicht nur für jene Dateien besteht, deren Inhalt gemäß § 18 Abs. 2 DSG der Vorabkontrolle unterliegt. (Zum Begriff der Datei siehe § 4 Z. 6 DSG).

durch den Bundeskanzler veröffentlicht werden dürfen.[31] Derartige, rechtlich unverbindliche Verhaltensregeln[32] wurden bisher weder von der Wirtschaftskammerorganisation, noch von einem der nationalen Detektivverbände[33] oder einer vergleichbaren Einrichtung veröffentlicht. Es gibt somit derzeit keine Verhaltensregeln iS. § 6 Abs. 4 DSG.

Weiters ist zu beachten, dass Daten ausschließlich für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise weiterverwendet werden dürfen. Sie müssen für den Zweck der Datenanwendung wesentlich sein und dürfen über diesen nicht hinausgehen. Sie müssen sachlich richtig sein und dürfen nur so lange in personenbezogener Form aufbewahrt werden, wie dies für die Erreichung der Zwecke, für die sie ermittelt wurden, erforderlich ist.[34]

Bei der Prüfung der Zulässigkeit einer konkreten Datenverarbeitung ist nach § 7 DSG vorzugehen.

Zweck der Datenverarbeitung:

Gemäß § 7 DSG dürfen Daten nur verarbeitet werden, soweit der 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 rechtliche Befugnis eines Detektivs, Daten zu ermitteln,[35] ergibt sich aus § 249 GewO und stellt einen berechtigten Zweck der Datenverarbeitung dar.[36]

---

[31] Nach *Drobesch/Grosinger*, das neue österreichische Datenschutzrecht (2000), 132, ist die Rechtsnatur der Verhaltensregeln fraglich. Die Autoren verweisen a.a.O. auf *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000, 24, wonach Verhaltensregeln am ehesten mit ÖNormen zu vergleichen sind.

[32] Verhaltensregeln haben als "soft-law" keinen verbindlichen Charakter, wären aber bei der freiwilligen Befolgung durch die Mehrzahl der Detektivunternehmen ein wertvolles Mittel für die effektive Verwirklichung des Datenschutzes (vgl. RV-Erläuterungen zu § 6 DSG).

[33] Österreichischer Detektivverband, Berufsdetektivverband.

[34] Vgl. *Jahnel* in Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht (2000), 169.

[35] "Ermittlung" als Unterfall der Verarbeitung.

[36] In diesem Sinne auch *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 25, mit Hinweis auf *Dohr/Pollirer/Weiss*, Datenschutzgesetz (1988) Anm. 6 zu § 17 DSG.

Auftraggeber, Dienstleister:
Diffiziler ist die Feststellung, ob Detektiv oder Kaufhausbetreiber als Auftraggeber iS. § 7 Abs. 1 DSG zu qualifizieren ist. Die Unterscheidung zwischen datenschutzrechtlichem Auftraggeber und Dienstleister ist insofern von großer Relevanz, als den Auftraggeber eine Reihe von Pflichten trifft.[37] Demgegenüber trägt der Dienstleister eine vergleichsweise geringe Verantwortung.[38]

Nach dem Wortlaut des Gesetzes muss auf Seiten des Auftraggebers eine gesetzlichen Zuständigkeit oder rechtlichen Befugnis vorliegen, Daten zu ermitteln. Nach *Drobesch/Grosinger* kommt es für die Qualifikation als Auftraggeber ausschließlich auf faktische Umstände, nämlich die Entscheidung zur Datenverarbeitung, nicht aber auf Fragen der rechtlichen Zulässigkeit der Verarbeitung an.[39]

Gemäß § 4 Z. 4 DSG sind Auftraggeber natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, wenn sie allein oder gemeinsam mit anderen die Entscheidung getroffen haben, Daten für einen bestimmten Zweck zu verarbeiten (Z. 9), und zwar 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 oder hat der Auftragnehmer die Entscheidung über die Art und Weise der Verwendung, insbesondere die Vornahme einer Verarbeitung der überlassenen Daten, auf Grund von Rechtsvorschriften, Standesregeln oder Verhal-

[37] Der datenschutzrechtliche Auftraggeber hat die DVRNr. zu führen (ausgenommen davon sind die in der Anlage I der "Standard- und Musterverordnung", BGBl. II Nr. 201/00, aufgezählten Datenanwendungen. Bezüglich der in Anlage II der Verordnung aufgezählten "Musteranwendungen" besteht lediglich eine vereinfachte Meldepflicht), ist Ansprechpartner und Verantwortlicher für die Beachtung der Rechte Betroffener und weiters der verwaltungsstrafrechtlich primär Verantwortliche.
[38] Z.B. Verantwortung für Datensicherheitsmaßnahmen (§ 14) und Einhaltung des Datengeheimnisses (§ 15).
[39] *Drobesch/Grosinger*, das neue österreichische Datenschutzrecht (2000), 120.

tensregeln gemäß § 6 Abs. 4 eigenverantwortlich zu treffen, so gilt der mit der Herstellung des Werkes Betraute als datenschutzrechtlicher Auftraggeber.

Bei "Dienstleistern" handelt es sich gemäß § 4 Z. 5 DSG hingegen um natürliche oder juristische Personen, Personengemeinschaften oder Organe einer Gebietskörperschaft beziehungsweise die Geschäftsapparate solcher Organe, welche Daten, die ihnen zur Herstellung eines aufgetragenen Werkes überlassen wurden, verwenden.

Vorweg ist bei der Auslegung obiger Bestimmungen zu beachten, dass "Auftraggeber" iS. des Datenschutzrechts als eigenständiger Rechtsbegriff zu verstehen ist, welcher unabhängig von der zivilrechtlichen Terminologie des Auftragvertrages besteht.[40]

Nach *Jahnel* wollte der Gesetzgeber mit der Legaldefinition des Auftraggebers "... jedenfalls zum Ausdruck bringen, dass Träger der datenschutzrechtlichen Pflichten sein soll, wer die Verfügungsbefugnis über den EDV-Einsatz hat. Diese hat derjenige, der den Auftrag zur Datenverarbeitung erteilt oder der (als Auftragnehmer) über die Verwendung der Daten eigenverantwortlich entscheidet ("Herr der Datenverarbeitung")."[41] *Mayer-Schönberger/Brandl*[42] erklären die Zurechnung des Einsatzes von EDV durch einen mit einem Werk Beauftragten an den Werk-Auftragserteiler damit, dass heute der Einsatz von EDV grundsätzlich zu vermuten sei, wenn ein Werk unter Benützung von Daten zu erbringen ist.

Die Definition des Auftraggebers umfasst jedoch nicht ausdrücklich auch jene Fälle, in welchen ein zivilrechtlicher Auftraggeber dem mit der Herstellung eines Werkes Betrauten keine Daten überlässt, sondern dieser auftragsgemäß selbst ermittelt, wie dies bei Detektiven meist der Fall sein wird. Nach der von *Duschanek/Rosenmayr-Klemenz* vertretenen Ansicht muss es sich im Sinne der

[40] Vgl. z.B. *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000 (2000), 28.
[41] In Jahnel/Schramm/Staudegger (Hrsg), Informatikrecht, 164.
[42] In Datenschutzgesetz 2000 (1999), 62.

allgemeinen Definition des Auftraggebers (§ 4 Z. 4 1. Satz) auch dabei um ein Dienstleistungsverhältnis handeln.[43]

Dies wird auf jene Fälle zutreffen, in welchen dem Detektiv von seinem Auftraggeber die jeweils zu setzenden Schritte hinreichend bestimmt vorgegeben werden und er tatsächlich ausschließlich "auftragsgemäß" ermittelt. Hat der Detektiv hingegen den Auftrag einen Sachverhalt aufzuklären und trifft er als "Ermittlungsprofi" selbständig die Entscheidung darüber, welche Daten konkret zu ermitteln sind und wie dabei vorzugehen ist, kommt ihm Auftraggebereigenschaft iS. der genannten Bestimmung zu. Diese Sicht trägt auch dem Umstand Rechnung, dass der Auftraggeber unter anderem verpflichtet ist, die Zulässigkeit der Datenverwendung sicherzustellen. Wäre der zivilrechtliche Auftraggeber auch Auftraggeber im datenschutzrechtlichen Sinn, müsste er die Verantwortung für die Einhaltung aller Pflichten nach dem DSG tragen, ohne auf die EDV seines Auftragnehmers (Detektiv) Einfluss nehmen zu können.[44] Im Ergebnis erstreckte sich seine datenschutzrechtliche Verantwortung auf Tätigkeiten, die er wegen fehlender Gewerbeberechtigung gar nicht selbst ausüben darf, wodurch auch die Wahrung des gebotenen Datenschutzes in Frage gestellt wäre.[45]

Zusammenfassend ist ein Detektiv betreffend der Daten, die ihm von seinem Auftraggeber überlassen werden, bzw. welche er auftragsgemäß ermittelt, Dienstleister iS. des DSG. Bezüglich jener Daten, die er selbständig ermittelt, wird er hingegen als Auftraggeber zu betrachten sein. Was jedoch in jenen Fällen gelten soll, in denen der Detektiv Daten vom Auftraggeber erhält, aus welchen er durch Bewertung, Analyse und Verknüpfung neue Informationen zieht und diese mit weiteren Rechercheergebnissen kombiniert, kann anhand des Gesetzes nicht beantwortet und wohl nur durch Wertung im Einzelfall gelöst werden. Für diese Fälle böte sich die Möglichkeit, die Auftraggebereigenschaft in Verhaltensregeln gemäß § 6 Abs. 4 DSG festzulegen.

---

[43] *Duschanek/Rosenmayr-Klemenz,* Datenschutzgesetz 2000 (2000), 30.

[44] Die wesentlichen Pflichten eines Auftraggebers nach dem DSG sind: Registrierung der Datenanwendung, Angabe der Registernummer bzw. Offenlegung der Identität, Verantwortung für die Zulässigkeit der Datenverwendung, Vorkehrungen zur Datensicherheit, Verpflichtung der Mitarbeiter auf das Datengeheimnis, Informationspflichten, Auskunftspflicht, Richtigstellung unrichtiger Daten, Löschung unzulässig verarbeiteter oder nicht mehr gebrauchter Daten. (Vgl. *Jahnel*, Datenschutzrecht (FN 2) 176).

[45] In diesem Sinne auch *Duschanek/Rosenmayr-Klemenz,* Datenschutzgesetz 2000 (2000), 29.

Selbst in den Fällen, in den der Berufsdetektiv unstrittig als Dienstleister zu qualifizieren ist, kann eine Datenermittlung, welche er für seinen Auftraggeber durchführt, zulässig sein, denn das Vorliegen eines berechtigenden Zwecks ist unter Heranziehung der gesamten Rechtsordnung zu beurteilen.[46] Der berechtigte Zweck ergibt sich demnach aus Gesetz, dem Gesellschaftsvertrag und insbesondere aus der Gewerbeberechtigung.[47] Darüber hinaus sind Tätigkeiten, die für die Entfaltung gewerblicher Tätigkeit notwendig sind, vom Zweck eines gewerblich tätigen Unternehmens gedeckt.[48]

Benötigt ein Kaufhausbetreiber die Identitätsdaten eines Verdächtigen zur Geltendmachung seiner Ersatzforderungen gegen diesen, ist eine Datenermittlung durch ihn - unter Zuhilfenahme eines Berufsdetektivs als Dienstleister - somit trotz des Wortlautes von § 7 Abs.1 DSG nach dem bisher Gesagten zulässig.

Schutzwürdige Geheimhaltungsinteressen:

Weiters ist das Vorliegen eines schutzwürdigen Geheimhaltungsinteresses des Betroffenen, insbesondere im Hinblick auf die Achtung seines Privat- und Familienlebens zu prüfen. Beschränkungen dieses Rechts sind nur zur Wahrung berechtigter Interessen eines anderen oder auf Grund von Gesetzen zulässig, die überdies aus den in Art. 8 Abs. 2 EMRK als Ausnahmen zum Schutz des Privat- und Familienlebens genannten Gründen notwendig sein müssen, zulässig.[49]

Bei der konkreten Interessenabwägung, welche nicht-sensible Daten betreffend nach § 8 und sensible Daten betreffend nach § 9 DSG vorgenommen wird, ist zunächst die Schutzwürdigkeit des Interesses des Betroffenen zu beurteilen.

---

[46] Siehe bereits DSK 12.4.1984, ZfVBDat 1986/3/4.

[47] Vgl. *Duschanek*, Geheimnisschutz und Datenschutz, in *Ruppe* (Hrsg), Geheimnisschutz im Wirtschaftsleben (1986), 307.

[48] *Grabenwarter*, Datenschutzrechtliche Anforderungen an den Umgang mit Kundendaten im Versandhandel, OJZ 2000, 861 ff.

[49] Wie *Mayer-Schönberger*, Information und Recht (2001), 46, mit Hinweis auf VfGH 30.9.1989, JBl 1990, 445, ausführt, muss das entgegengesetzte Recht gesetzlich vorgesehen sein und eine Maßnahme darstellen, die in einer demokratischen Gesellschaft für die nationale Sicherheit, die öffentliche Ruhe und Ordnung, das wirtschaftliche Wohlergehen des Landes, die Verteidigung der Ordnung und zur Verhinderung von strafbaren Handlungen, zum Schutz der Gesundheit und der Moral oder zum Schutz der Rechte und Freiheiten anderer notwendig ist.

Diese ist nicht nach rein subjektiven Kriterien zu beurteilen, sondern nach objektiven Maßstäben. Es kommt darauf an, "ob bei einer Durchschnittsbetrachtung ein schutzwürdiges Geheimhaltungsinteresse einer Datenermittlung oder Datenübermittlung entgegensteht.[50] Liegt ein Geheimhaltungsinteresse vor, ist dieses in einem weiteren Prüfungsschritt gegen das Interesse eines anderen auf Informationszugang abzuwägen, wobei im Zweifel der Vertraulichkeit der Vorrang einzuräumen ist.[51]

Exkurs: Sensible Daten, nicht-sensible Daten:

Unter sensiblen Daten (besonders schutzwürdigen Daten) werden jene Daten natürlicher Personen verstanden, welche ihre rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit oder ihr Sexualleben betreffen (§ 4 Z. 2 DSG). Diese taxative Aufzählung erfolgte in wörtlicher Umsetzung des Art. 8 Abs. 1 DSRL[52], wobei deren abschließender Charakter auch Kritik in der Literatur gefunden hat.[53]

Für die Beurteilung, ob ein sensibles Datum vorliegt, kommt es somit ausschließlich darauf an, ob das jeweilige Datum unter eine der genannten Datenkategorien fällt, nicht hingegen darauf, ob der konkrete Informationsgehalt ein Diskriminierungsrisiko für den Betroffenen darstellt. Weiters ist es unerheblich, ob die Daten den sensiblen Informationsgehalt unmittelbar oder nur mittelbar (z.B. Angaben über die Einnahme bestimmter Medikamente) darstellen. Daten, bei denen man nur mit einer statistischen Wahrscheinlichkeit auf sensible Angaben im Sinne von Z. 2 schließen kann, (z.B. Namen, Geburts- oder Wohnort), fallen nicht unter die Begriffsdefinition, weil sie keine sichere Erkenntnis über das Vorliegen einer sensiblen Information liefern können.[54]

---

[50] *Mayer-Schönberger*, Information und Recht (2001), 46, mit Hinweis auf die hL und DSK 13.10.1993, 120.434 (Bescheid), ZfVBDat 1994/5.
[51] Vgl. *Mayer-Schönberger*, Information und Recht (2001), 46.
[52] Vgl. *Mayer-Schönberger/Brandl*, Datenschutzgesetz 2000 (1999), 61; *Duschanek/Rosenmayr-Klemenz,* Datenschutzgesetz 2000 (2000), 26 ff; *Drobesch/Grosinger*, das neue österreichische Datenschutzrecht (2000), 118 f.
[53] *Drobesch/Grosinger*, 118, mit Hinweis auf *Damann/Simitis*, EG-Datenschutzrichtlinie 160 ff.
[54] So *Drobesch/Grosinger*, 118.

Keine sensiblen Daten sind weiters Daten über die Vermögensverhältnisse einer Person, Angaben über deren Staatsangehörigkeit, Geschlecht und strafrechtliche Verurteilungen, wobei strafrechtsbezogene Daten durch Art. 8 Abs. 5 DSRL jedoch in die Nähe sensibler Daten gerückt werden.[55]

Schutzwürdige Geheimhaltungsinteressen werden bei der Verwendung nichtsensibler Daten gemäß § 8 Abs. 1 DSG 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 könnte in der Gewerbeberechtigung des Detektivs, nach welcher er befugt ist, die Identität einer Person zu ermitteln, erblickt werden. Bei der Auslegung der genannten Bestimmung ist jedoch zu berücksichtigen, dass diese inhaltlich unverändert von § 6 1. Tatbestand DSG 1978[56] übernommen wurde und die Materialien zum DSG 1978 ebenso wie mehrere Rundschreiben des BKA-VD fordern, dass eine ausdrückliche gesetzliche Ermächtigung jede der Komponenten einer Datenverarbeitung erfassen und auch die zugelassenen Daten ausdrücklich bezeichnen muss.[57] Nach den weiteren Ausführungen von *Drobesch/Grosinger* an der genannten Stelle müssen dem Gesetz neben der Datenart auch der Betroffenen- und Empfängerkreis zu entnehmen sein. Dadurch werde ein sehr hohes Regelungsniveau gefordert, welches meines Erachtens § 249 GewO nicht erfüllen kann.

[55] Wenn *Drobesch/Grosinger*, 119, auch psychologische Daten generell als nicht-sensible Daten qualifizieren, kann dem insofern nicht gefolgt werden, als es sich dabei vielfach um gesundheitsbezogene und somit sensible Daten handelt.
[56] BGBl. Nr. 565/1978 aufgehoben durch BGBl. I Nr. 165/1999.
[57] *Drobesch/Grosinger*, 138, mit Hinweis auf EB zur RV 1975 zu § 6 und BKA-VD, GZ 810.099/1-V/1a/85.

Abgesehen von der Zustimmung des Betroffenen zur Verwendung seiner Daten oder dem Vorliegen lebenswichtiger Interessen, können auch überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten die Verwendung rechtfertigen.

Ein überwiegendes berechtigtes Interesse iS. § 8 Abs. 1 Z. 4 DSG ist insbesondere dann anzunehmen, wenn die Verwendung[58] zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einer Behörde[59] notwendig ist und die Daten rechtmäßig ermittelt[60] worden sind (§ 8 Abs. 3 Z 5).

Strafrechtsbezogene Daten sind zwar keine sensiblen Daten, werden jedoch durch Art. 8 Abs. 5 DSRL in deren Nähe gerückt. Nach § 8 Abs. 4 DSG verstößt 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 - unbeschadet der Bestimmungen des Abs. 2 - nur dann nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen, wenn

1. eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung solcher Daten 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 die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteres-

---

[58] Wohl auch die Übermittlung.

[59] "Behörde" wird als Überbegriff für Gerichte und Verwaltungsbehörden zu verstehen sein. Die DSRL spricht hingegen von Rechtsansprüchen vor "Gericht", was iS. der EuGH-Judikatur als Tribunal zu verstehen ist.

[60] *Kilches*, Datenschutzgesetz 2000, Selbstbestimmter Datenschutz, MR 1999, 261: "Die Judikatur sämtlicher österreichische Höchstgerichte lehnt ein Beweisverwertungsverbot ab. Der Europäische Gerichtshof für Menschenrechte hat zu dieser Frage im Rahmen des Fair Trial Gebotes (Art. 6 EMRK) bislang nicht ausdrücklich Stellung genommen. Werden im Verfahren Daten vorgelegt, die rechtswidrig ermittelt wurden, stellt sich die Frage, ob dann lediglich die Verwaltungsstrafbestimmungen des DSG 2000 greifen oder die Beweis (gemeint wohl "Beweise", Anm. des Autors) nicht beachtet werden dürfen. Möglicherweise muss hier zwischen einfacher rechtswidriger Datenerhebung und qualifiziertem Datenverstoß in der Rechtsfolge differenziert werden. Regierungsvorlage und Richtlinie schweigen zu dieser Frage."

sen 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 dem Datenschutzgesetz gewährleistet.

Eine ausdrückliche gesetzliche Ermächtigung oder Verpflichtung zur Verwendung von Daten iS. Z. 1 liegt wiederum nur dann vor, wenn diese jede der Komponenten der Datenverarbeitung erfasst und auch die zugelassenen Daten ausdrücklich bezeichnet.[61] Für den Tätigkeitsbereich der Berufsdetektive sind keine derartigen gesetzlichen Ermächtigungen oder Verpflichtungen ersichtlich. Da sich § 8 Abs. 4 Z. 2 DSG ausschließlich auf Datenanwendungen im öffentlichen Bereich bezieht, kann dieser Tatbestand in gegebenen Zusammenhang außer Betracht bleiben.
Z. 3 lex.cit. normiert, dass sich die Zulässigkeit der Verwendung von strafrechtsbezogenen Daten auch aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergeben kann, wenn die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach dem Datenschutzgesetz gewährleistet. Die Verpflichtung zur Gewährleistung der Wahrung der Interessen der Betroffenen durch Art und Weise der Datenverwendung hat nach *Drobesch/Grosinger*[62] zur Folge, dass ein privater Auftraggeber strafrechtsbezogene Daten nur dann verwenden darf, wenn es ihm möglich ist, beim Umgang mit den Daten auf die Betroffeneninteressen (Achtung des Privatlebens, Erwerbsfreiheit) besonders Bedacht zu nehmen, z.B. durch besonders vertrauliche Behandlung oder möglichst kurze Bearbeitungsdauer.

Für den konkreten Fall eines durch einen Ladendiebstahl geschädigten Kaufhauses kann somit davon ausgegangen werden, dass eine Identitätsermittlung des unbekannten Täters zum alleinigen Zweck der Geltendmachung von Ersatzforderungen nicht gegen schutzwürdigen Geheimhaltungsinteressen verstößt.

---

[61] In diesem Sinne *Drobesch/Grosinger*, 141, mit Hinweis auf deren Anmerkungen zu § 8 Abs.1 Z. 1 DSG, 138.
[62] *Drobesch/Grosinger*, 141.

Die Datenermittlung selbst kann auf verschiedene Art und Weise erfolgen. So wird ein Detektiv eigene Erkundungen[63] durchführen, öffentlich zugängliche Quellen ausschöpfen und möglicherweise auch Daten aus anderen (legalen) Quellen beziehen.

Eigene Erkundungen:

Abhängig vom jeweiligen Sachverhalt ist die Kreativität des Detektivs gefordert, Wege zu finden, die Identität eines unbekannten Täters zu ermitteln. Möglicherweise gibt es eine Personenbeschreibung oder es liegt gar ein Foto aus einer Überwachungskamera vor, wodurch beispielsweise die Befragung von Auskunftspersonen[64] in Tatortnähe zielführend sein kann. Die rechtliche Befugnis eines Detektivs, die Identität einer Person auf diese Art zu ermitteln, ergibt sich, wie bereits ausgeführt, aus § 249 GewO. Auch schutzwürdige Geheimhaltungsinteressen des Betroffenen werden nicht verletzt.

Öffentlich zugängliche Quellen:

Ein schutzwürdiges Geheimhaltungsinteresse des Betroffenen gilt nach § 8 Abs. 2 DSG auch dann als nicht verletzt, wenn dabei ausschließlich zulässigerweise veröffentlichte Daten verwendet werden. Dabei handelt es sich vor allem um Daten, die in öffentlich zugänglichen Registern abgefragt werden können. Eine Ermittlung von Daten aus dem öffentlichen Telefonbuch, Grundbuch, Firmenbuch, Gewerberegister, Mitglieder und Funktionärsdatenverwaltung der Wirtschaftskammerorganisation, Ediktedatei, Melderegister, Personenstandsbücher[65], Unionsbürgerevidenz, Wählerevidenz, Europa-Wählerevidenz, Kraftfahrzeug-Zulassungsevidenz, etc. ist somit datenschutzrechtlich unproblematisch.[66] Daten über gerichtlich oder verwaltungsbehördlich strafbare Handlungen finden sich allerdings nicht in öffentlich zugängliches Registern.

---

[63] Üblicherweise als Recherche, Ermittlung oder Erhebung bezeichnet.

[64] z.B. Passanten an Autobusstation vor dem Tatort, Mitarbeiter in umliegenden Geschäften, etc.

[65] Geburten-, Ehe- und Sterbebuch (siehe Personenstandsgesetz (PStG), BGBl. Nr. 60/1983.).

[66] Auskünfte aus dem Zentralen Melderegister, den Personenstandsbüchern, der Mitglieder- und Funktionärsdatenverwaltung der Wirtschaftskammerorganisation und der Kraftfahrzeug-Zulassungsevidenz setzen die Glaubhaftmachung eines rechtlichen Interesses durch den Aus-

Weiters wird bei Daten, die vom Betroffenen selbst - oder mit seiner Zustimmung von einem Dritten - z.B. im Internet, veröffentlicht wurden, ein schutzwürdiges Geheimhaltungsinteresse nicht verletzt. Zusatzinformationen, die durch Auswertung von veröffentlichten Daten erzielt werden und ihrerseits nicht öffentlich zugänglich sind, können hingegen sehr wohl das schutzwürdige Geheimhaltungsinteresse eines Betroffenen verletzen.

Befragung des Betroffenen:

Vielfach wird sich ein Fall nicht allein durch Befragungen von Auskunftspersonen und Recherche in öffentlichen Datenregistern aufklären lassen. Es stellt sich dann die Frage, wie die noch fehlenden Informationen beschafft werden können. Ein probates Mittel, welches allerdings eine professionelle Vorgangsweise vom Berufsdetektiv verlangt, ist die verdeckte Befragung eines Verdächtigen unter Verwendung einer sogenannten Legende. Dem Betroffenen wird dabei vorgegaukelt, seine Antworten auf die an ihn gerichteten Fragen würden einem anderen Zweck dienen, als dies tatsächlich der Fall ist.

Eine derartige Vorgangsweise könnte dem Grundsatz, nach welchem Daten nur nach "Treu und Glauben" verwendet werden dürfen, widersprechen, da der Betroffene über seine Rechte nicht irregeführt oder im Unklarem gelassen werden darf.

Da die Identität einer verdächtigen Person neben den näheren Umständen der Tat für den eindeutig festgelegten und rechtmäßigen Zweck der Einleitung eines Strafverfahrens (unter Anschluss des Geschädigten als Privatbeteiligter) notwendig und wesentlich ist, kann in ihrer Ermittlung meines Erachtens kein Verstoß gegen die Grundsätze des § 6 DSG gesehen werden. Die verdeckte Befragung des Betroffenen durch den Detektiv ist somit zulässig.

---

kunftswerber voraus. Liegt ein solches vor, wird das schutzwürdige Geheimhaltungsinteresse des Betroffenen nicht verletzt.

Sonstige Quellen:

Jedenfalls unzulässig ist die Abfrage von behördeninternen Datenanwendungen wie beispielsweise des EKIS[67] durch Berufsdetektive. Derartige Vorgehensweisen haben bereits strafrechtliche Verurteilungen von Detektiven, wie auch ihrer Helfer, den unmittelbar tätigen Beamten des Innenministeriums bewirkt.[68] Von diesen rechtswidrigen Methoden soll hier nicht die Rede sein.

Daten aus firmeninternem Register:

Detektive verkaufen Wissen über Fakten und Zusammenhänge. Die Versuchung umfangreiche Datensammlungen anzulegen, um sie im Bedarfsfall zu benutzen, liegt somit nahe. Dies ist so lange unproblematisch, als nicht personenbezogene Daten nutzbar gemacht werden. Können Daten einer firmeninternen Datenanwendung hingegen auf konkrete Personen rückgeführt werden, ist eine Abfrage nur zulässig, wenn die Datenanwendung an sich zulässig ist (siehe unten).

Daten von anderen Detektiven:

Denkbar ist weiters, dass die benötigten Daten von einem anderen Detektiv zur Verfügung gestellt werden. Ermittelt dieser als Subunternehmer des beauftragten Detektivs, ist er befugt, Daten zu ermitteln und an seinen Auftraggeber zu übermitteln. Der beauftragende Detektiv seinerseits wird die Daten bei Vorliegen der zuvor beschriebenen Voraussetzungen an seinen Auftraggeber übermitteln.

Davon ist der Fall zu unterscheiden, in welchem der "Subdetektiv"[69] die benötigten Daten nicht anlassbezogen ermittelt, sondern bereits verwendet. Bezieht ein

---

[67] "EKIS": Elektronisches Kriminalpolizeiliches Informationssystem.
Nach der von ORF ON Futurezone (http://futurezone.orf.at) durchgeführten und am 10.10.2000 veröffentlichten Recherche beinhaltet der "kriminalpolizeilichen Aktenindex", welcher einen Teil des EKIS bildet, "...jede Anzeige einer Sicherheitsbehörde an eine Behörde der Strafjustiz auf Grund eines strafrechtlich relevanten Tatbestands mit Ausnahme von Fahrlässigkeitsdelikten.". Dieser Index basiere nach Auskunft des Leiters der EDV-Zentrale im Innenministerium, Nikolaus Schwab, auf § 57 Abs. 1 Z. 6 SPG.

[68] Siehe dazu *Maier*, Der Detektiv-Report, Wien 2001, ISBN 3-8000-3821-8, 145 ff.

[69] Der Auftraggeber beauftragt den Detektiv mit der Erbringung eines Werkes, nämlich mit der Ermittlung in einer bestimmten Angelegenheit. Der Detektiv ist als Werkunternehmer befugt, sich bei der Erbringung seiner Leistung Subunternehmer zu bedienen, welche jedoch in kein Rechtsverhältnis mit dem Auftraggeber treten.

Detektiv von anderen Detektiven personenbezogene Daten, stellt dies eine Übermittlung von Daten im Sinne des DSG dar, deren Zulässigkeit nach § 7 Abs. 2 DSG zu prüfen ist.

Nach § 7 Abs. 2 DSG dürfen Daten nur übermittelt werden, wenn
1. sie aus einer gemäß Abs. 1 lex.cit. 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.

Die Zulässigkeit der Datenübermittlung setzt voraus, dass die Daten im Übermittlungszeitpunkt rechtmäßig verarbeitet werden.[70] Eine rechtmäßige Verarbeitung ist nicht gegeben, wenn Daten entgegen den allgemeinen Grundsätzen des § 6 DSG verwendet werden. Gemäß diesen Grundsätzen sind personenbezogene Daten zu löschen, wenn sie für die Zwecke, für die sie ermittelt wurden, nicht mehr erforderlich sind.[71] Eine Übermittlung derartiger Daten durch einen Detektiv an einen anderen ist somit ausgeschlossen, wenn es sich um Daten handelt, welche für die Aufklärung eines anderen Sachverhaltes ermittelt wurden. Wurden die Daten hingegen für die allgemeine Verwendung in einer zulässigen Datenanwendung (siehe unten) ermittelt, ist ihre Übermittlung durch den Betreiber der Datenanwendung[72] bei Vorliegen der weiterer Voraussetzung des § 7 Abs. 2 DSG zulässig. Der anfragende Berufsdetektiv wird dem Berufskollegen seine rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft machen können, es bleibt somit zu untersuchen, ob die schutzwürdigen Geheimhaltungsinteressen des Betroffenen durch Zweck und Inhalt der Übermittlung verletzt werden.

[70] Vgl. *Drobesch/Grosinger*, 134, Rz. 3.
[71] § 6 Abs. 1 Z. 5 DSG.
[72] Nur ein datenschutzrechtlicher Auftraggeber darf Daten an einen Dritten weitergeben, dem Dienstleister ist dies ohne Auftrag des Auftraggebers gemäß § 11 Abs. 1 Z. 1 DSG verboten.

Das Geheimhaltungsinteresse des Betroffenen wird nicht verletzt, wenn ein überwiegendes berechtigtes Interesse an der Übermittlung auf Seiten des Datenempfängers vorliegt. Ein überwiegendes berechtigtes Interesse iS. § 8 Abs. 1 Z. 4 DSG ist insbesondere dann anzunehmen, wenn die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor einem Gericht oder einer Verwaltungsbehörde notwendig ist und die Daten rechtmäßig ermittelt worden sind (§ 8 Abs. 3 Z. 5).

Bezüglich sensibler Daten (siehe § 4 Z. 2 DSG) besteht hingegen ein grundsätzliches Verarbeitungsverbot, wovon § 9 DSG Ausnahmen normiert. So wird das schutzwürdige Geheimhaltungsinteresse eines Betroffenen wiederum nicht verletzt, wenn die Verwendung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen des Auftraggebers vor der Behörde notwendig ist und die Daten rechtmäßig ermittelt wurden. Die in einem Strafverfahren geltend zu machenden Ersatzansprüche des geschädigten Kaufhausbetreibers sind als solche Rechtsansprüche zu qualifizieren, weshalb auch deren Verwendung zulässig ist.

Informationspflicht, Verschwiegenheitspflicht:

Informationspflicht nach DSG:

Ermittelt der Detektiv Daten einer Person, so trifft den Auftraggeber[73] grundsätzlich eine aktive Informationspflicht. Nach § 24 Abs. 1 DSG ist der Betroffene aus Anlass der Ermittlung der Daten in geeigneter Weise über den Zweck der Anwendung, für die die Daten ermittelt werden und über Name und Adresse des Auftraggebers zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen.

Diese Informationspflicht besteht jedoch nur für Datenanwendungen. Eine solche liegt vor, wenn zumindest teilweise automationsunterstützte, also maschinell und programmgesteuerte Verwendungsschritte durchgeführt werden.

[73] Datenschutzrechtlicher Auftraggeber: Wurden dem Detektiv Daten vom zivilrechtlichen Auftraggeber überlassen, so ist dieser auch der datenschutzrechtliche Auftraggeber. Für Daten, die der Detektiv aus eigenem ermittelt und verarbeitet, ist er selbst als datenschutzrechtlicher Auftraggeber anzusehen.

Gemäß § 24 Abs. 3 DSG besteht weiters keine Informationspflicht bei jenen Datenanwendungen, die gemäß § 17 Abs. 2 und 3 nicht meldepflichtig sind. § 17 Abs. 3 Z 5 DSG nimmt Datenanwendungen von der Meldepflicht aus, die der Vorbeugung, Verhinderung oder Verfolgung von Straftaten dienen, soweit dies zur Verwirklichung des Zweckes der Datenanwendung notwendig ist. Nach der von *Drobesch/Grosinger*[74] vertretenen Ansicht sind unter "Vorbeugung, Verhinderung oder Verfolgung von Straftaten" die sicherheitspolizeilichen Angaben der §§ 21 bis 26 Sicherheitspolizeigesetz angesprochen. Demnach werden die strafpolizeilichen Aufgaben erfasst, die von den Strafjustizbehörden und den Sicherheitsbehörden im Dienst der Strafjustiz (Kriminalpolizei) besorgt werden. Folgt man dieser Auffassung, ist der im privaten Bereich tätige Detektiv nicht berechtigt, die Information des Betroffen zu unterlassen.

Vielfach wird sowohl der Detektiv als auch sein zivilrechtlicher Auftraggeber "damit leben können", dass der Betroffene über die Vornahme von Ermittlungen zu informieren ist. Es sind jedoch durchaus Fallkonstellationen denkbar, in welchen die Erhebungen gefährdet und das Ergebnis durch eine vorzeitige Information ad Absurdum geführt wird. Dem könnte im Einzelfall dadurch begegnet werden, dass der Detektiv die Verwendung einer Datenanwendung vermeidet. Da der Begriff der "Datenanwendung" jedoch nicht auf die Strukturiertheit einer Datei abzielt, sind sogar Textverarbeitungen davon erfasst.[75] Der Detektiv müsste somit ohne EDV-Unterstützung ermitteln und seinen Bericht ohne Textverarbeitungsprogramm verfassen, damit keine Informationspflicht entsteht.

---

[74] das neue österreichische Datenschutzgesetz, 179. Neben einer systematischen Interpretation der genannten Bestimmung unterstreicht mE die Tatsache, dass bei der Begehung einer strafbaren Handlung ausschließlich dem Staat ein Strafanspruch gegen den Täter zusteht, die Richtigkeit dieser Sichtweise. Ein Geschädigter macht auch im Adhäsionsverfahren nach der Strafproszessordnung einen zivilrechtlichen Schadenersatzanspruch geltend.

[75] AB zu § 17 DSG: " Die automationsunterstützte Erstellung und Archivierung von nicht strukturierten Texten (Textverarbeitung) kann angesichts der Definition des Begriffs "Verarbeitung personenbezogener Daten in der RL 95/46/EG von der Meldepflicht gemäß § 17 DSG nicht generell ausgenommen werden. Um die Durchführbarkeit dieser Pflicht zu erleichtern, ist beabsichtigt, durch Verordnung eine Musteranwendung für Textverarbeitung (einschließlich Archivierung) zu schaffen." In diese Richtung auch *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000, 24.

Verschwiegenheitspflicht nach GewO:

Gemäß § 252 Abs. 1 DSG sind Berufsdetektive zur Verschwiegenheit über die ihnen anvertrauten Angelegenheiten verpflichtet. Auf Grund dieser Bestimmung ist es dem Detektiv verboten, den Betroffenen über den Auftrag zu informieren. Fraglich ist in diesem Zusammenhang allerdings, was unter "anvertrauten Angelegenheiten" zu verstehen ist und ob auch Daten, die der Detektiv selbst erhebt, davon umfasst sind. Als datenschutzrechtlichen Auftraggeber könnten den Detektiv die Informationspflichten nach § 24 DSG treffen, wobei er das Spannungsverhältnis zwischen der gewerberechtlich normierten Verschwiegenheitspflicht und der datenschutzrechtlichen Informationspflicht möglicherweise dadurch lösen könnte, dass er dem Betroffenen nur allgemein mitteilt, er habe den Auftrag, Beweise zu erheben. Neben einer Gefährdung der Erhebungen ist jedoch unklar, ob eine derartige Vorgangsweise dem Grundsatz, nach welchem Daten nur nach "Treu und Glauben" verwendet werden dürfen, entspricht, da der Betroffene über seine Rechte nicht irregeführt oder im Unklarem gelassen werden darf.

Auch wenn der Betroffene kein durchsetzbares subjektives Recht auf Information hat, kann die Nichteinhaltung der Informationspflicht gemäß § 52 Abs. 2 DSG eine Verwaltungsstrafe bis zu S 130.000,- nach sich ziehen. Ein Verstoß gegen die Verschwiegenheitspflicht nach § 252 GewO kann eine Verwaltungsstrafe bis zu S 30.000,- nach sich ziehen (§ 367 Z. 49 GewO).

In der Branche wird die Verschwiegenheitspflicht bisher extensiv ausgelegt, so dass ein Detektiv - abgesehen von gesetzlich normierten Ausnahmen iS. § 252 Abs. 2 GewO[76] - keinerlei Informationen über einen Auftrag geben, ja nicht einmal dessen Existenz bestätigen bzw. verneinen darf. Weiters ist davon auszugehen, dass ihn eine aktive Geheimhaltungspflicht trifft, weshalb er Daten vor dem Zugriff Dritter wirksam zu schützen hat.

[76] § 252 Abs. 2 GewO lautet: "Inwieweit die Gewerbetreibenden von der Verpflichtung zur Ablegung eines Zeugnisses, zur Einsichtgewährung in Geschäftspapiere oder zur Erteilung von Auskünften über die ihnen in Ausübung des Berufes bekannt gewordenen Umstände in gerichtlichen oder verwaltungsbehördlichen Verfahren befreit sind, richtet sich nach den bezüglichen Rechtsvorschriften."

Im Hinblick auf das Wesen detektivischer Arbeitsmethoden, welche von der Rechtsordnung seit geraumer Zeit anerkannt werden[77], wird man meines Erachtens die gesetzliche Vorgabe des Datenschutzgesetzes aber auch in der Weise auslegen können, dass es ausreichend ist, wenn der Betroffene von den Ermittlungen erst nach deren Abschluss unterrichtet wird und beispielsweise im Rahmen eines folgenden Gerichtsverfahrens die Möglichkeit hat, Einsicht in die Daten zu nehmen. Diese Wertung scheint mit dem Grundgedanken des Rechts des Betroffenen auf Auskunft vereinbar, nach welchem einem Auskunftsbegehren nicht zu entsprechen ist, wenn überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten der Auskunfterteilung entgegenstehen. § 26 Abs. 2 DSG beinhaltet weiters eine demonstrative Aufzählung überwiegender öffentlicher Interessen und führt unter anderem die Vorbeugung, Verhinderung oder Verfolgung von Straftaten an. Entgegen der zu § 17 Abs. 3 Z. 5 DSG ausgeführten Meinung, bin ich hier der Ansicht, dass sich das überwiegende berechtigte Interesse des Auftraggebers oder eines Dritten auch aus der "Verfolgung von Straftaten" ergeben kann, weshalb eine Informationspflicht bzw. Auskunftspflicht, soweit dadurch der Erfolg der Ermittlungen gefährdet werden würde, (vorläufig) nicht besteht.

Selbst bei Ablehnung dieser Auslegung wird man die Geltendmachung von Ersatzforderungen als überwiegende berechtigte Interessen des Auftraggebers an der vorläufigen Geheimhaltung der Erhebungen werten müssen.

Betrieb einer Datei (ehemals) verdächtiger Personen:

Manche Detektive machen die Erstattung einer Anzeige auch davon abhängig, ob der Verdächtige bereits einmal bei einer einschlägigen Straftat ertappt wurde. Dabei kommt es durchaus vor, dass der Detektiv den Verdächtigen aus der Vergangenheit persönlich kennt. Im gegebenen Zusammenhang interessieren

[77] Vgl. Verordnung der Minister des Handels und des Innern vom 19. April 1904, betreffend die Einreihung des Betriebes von Privatdetektivunternehmen unter die konzessionierten Gewerbe, Reichsgesetzblatt für die im Reichsrate vertretenen Königreiche und Länder, XXII. Stück, Ausgegeben und versendet am 27. April 1904.

jedoch interne Register, welche von manchen auf die Kaufhausüberwachung spezialisierten Detekteien geführt werden bzw. wurden.[78]

Eine strukturierte Sammlung von Daten, die nach zumindest einem Suchkriterium zugänglich ist, stellt eine "Datei" iS. § 4 Z. 6 DSG dar. Das Grundrecht auf Geheimhaltung erfasst alle personenbezogenen Daten, also auch konventionell verarbeitete, unabhängig davon, ob sie in einer Datei strukturiert gesammelt werden oder nicht.[79] Es ist somit unerheblich, ob Daten aus einer händisch geführten Kartei, Liste, Register udg. oder einer computergestützte Datenanwendung stammen.[80]

Die Führung einer firmeninternen Datei mit ehemals verdächtigten Personen ist nur dann sinnvoll, wenn der Berufsdetektiv die sich darin befindenden Datensätze auch abgerufen kann. Die Zulässigkeit der Datenabfrage setzt voraus, dass diese Daten rechtmäßig verarbeitet werden, also rechtmäßig erhoben wurden und auch nachträglich kein Löschungstatbestand eingetreten ist.

Abgesehen vom recht seltenen Fall, dass eine Person die Zustimmung[81] zur Speicherung ihrer Daten in einer "Verdächtigendatei" erteilt, müssen Daten grundsätzlich nach Zweckerreichung gelöscht werden.

Ist der Detektiv Dienstleister, hat er gemäß § 11 Abs. 1 Z. 5 DSG nach Beendigung der Dienstleistung alle Verarbeitungsergebnisse und Unterlagen, die Daten enthalten, dem Auftraggeber zu übergeben oder in dessen Auftrag für ihn weiter aufzubewahren oder zu vernichten. Abhängig vom jeweiligen Sachverhalt kann der Zeitpunkt des tatsächlichen Abschlusses der Dienstleistung durchaus variieren. So könnte diese bereits mit der Übermittlung des Datenver-

[78] Siehe z.B. *Pokorny*, Detektive in Österreich, ihre Fälle, Methoden, Erfolge (ISBN 3-901090-00-2), 104, mit Nennung der Detektivagentur Pöchhacker Ges.m.b.H, Wien. (Ob das genannte Unternehmen nach wie vor eine entsprechende Datenanwendung unterhält, wurde nicht ermittelt).

[79] *Drobesch/Grosinger*, das neue österreichische Datenschutzrecht (2000), 98.

[80] Bei computergestützten Datenanwendungen handelt es sich nicht nur um spezielle Datenbanken, selbst die weltweit verbreiteten Textverarbeitungsprogramme wie z.B. Microsoft Word erlauben ein strukturiertes Suchen nach im Text vorkommenden Begriffen (z.B. Namen).

[81] § 4 Z. 14 DSG definiert die "Zustimmung" als die gültige, insbesondere ohne Zwang abgegebene Willenserklärung des Betroffenen, dass er in Kenntnis der Sachlage für den konkreten Fall in die Verwendung seiner Daten einwilligt. Liegt eine derartige Zustimmung vor, verstößt eine Datenverwendung nicht gegen schutzwürdige Geheimhaltungsinteressen des Betroffenen.

arbeitungsergebnisses an den Auftraggeber abschlossen sein oder aber erst geraume Zeit nach Rechnungslegung, wenn feststeht, dass der Detektiv die Daten auch nicht mehr als Grundlage für eine mit seinem Auftrag in Zusammenhang stehende Zeugenaussage vor einer Behörde benötigt.

Bezüglich Daten, welcher der Detektiv Auftraggeber ist, richtet sich seine Löschungspflicht nach § 27 DSG. Demnach gelten Daten als unzulässig verarbeitet und sind zu löschen, sobald sie für den Zweck der (ursprünglich zulässigen) Datenanwendung nicht mehr benötigt werden. Diese Löschungsverpflichtung besteht nicht, wenn die Datenarchivierung rechtlich zulässig ist und der Zugang zu diesen Daten besonders geschützt ist.[82]

Personenbezogene Daten können im Einzelfall somit zulässigerweise über erhebliche Zeiträume gespeichert bleiben. Ihre Weiterverwendung für einen anderen Zweck ist - abgesehen von wissenschaftlichen und statistischen Zwecken - nur zulässig, wenn eine Übermittlung der Daten für diesen Zweck zulässig ist (§ 27 Abs. 1 Z. 2 DSG).

Gemäß § 7 Abs. 2 DSG ist eine Datenübermittlung erlaubt, wenn die Daten aus einer zulässigen Datenanwendung stammen, der Empfänger dem Übermittelnden seine ausreichende gesetzliche Zuständigkeit oder rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft macht und schutzwürdige Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

Die Zulässigkeit der ursprünglichen Datenanwendung darf - wie erörtert - angenommen werden. Möchte der Detektiv personenbezogene Daten speichern, um bei Anhaltung einer Person überprüfen zu können, ob diese bereits in der Vergangenheit einschlägig verdächtigt wurde, übermittelt er die Daten aus der ur-

[82] Was konkret darunter zu verstehen ist, sagt das Gesetz nicht. Gemeint könnte beispielsweise die gesetzliche Verpflichtung nach § 212 HGB sein, wonach ein Kaufmann Handelsbücher, Inventare, Eröffnungsbilanzen, Jahresabschlüsse samt den Lageberichten, Konzernabschlüsse samt den Konzernlageberichten, empfangene Handelsbriefe, Abschriften der abgesendeten Handelsbriefe und Belege für Buchungen in den von ihm gemäß § 189 Abs. 1 HGB zu führenden Büchern (Buchungsbelege) sieben Jahre lang geordnet aufzubewahren hat; darüber hinaus noch solange, als sie für ein anhängiges gerichtliches oder behördliches Verfahren, in dem der Kaufmann Parteistellung hat, von Bedeutung sind.

sprünglichen Anwendung gewissermaßen "an sich selbst". Es ist somit zu fragen, ob er eine rechtliche Befugnis besitzt, derartige Daten zu empfangen. Diese rechtliche Befugnis könnte vordergründig wiederum in § 249 GewO erblickt werden.

Gemäß § 1 GewO gilt die Gewerbeordnung - abgesehen von den in §§ 2 bis 4 normierten Ausnahmen - für alle (in Österreich) gewerbsmäßig ausgeübten und nicht gesetzlich verbotenen Tätigkeiten. Eine Tätigkeit wird gewerbsmäßig ausgeübt, wenn sie selbständig, regelmäßig und in der Absicht betrieben wird, einen Ertrag oder sonstigen wirtschaftlichen Vorteil zu erzielen. Selbständigkeit liegt vor, wenn die Tätigkeit auf eigene Rechnung und Gefahr ausgeübt wird, wobei bereits eine einmalige Handlung als regelmäßige Tätigkeit gilt, wenn nach den Umständen des Falles auf die Absicht der Wiederholung geschlossen werden kann oder wenn sie längere Zeit erfordert. Bereits das Anbieten einer den Gegenstand eines Gewerbes bildenden Tätigkeit an einen größeren Kreis von Personen oder bei Ausschreibungen wird der Ausübung des Gewerbes gleichgehalten. Die Absicht, einen Ertrag oder sonstigen wirtschaftlichen Vorteil zu erzielen, liegt auch dann vor, wenn der Ertrag oder sonstige wirtschaftliche Vorteil den Mitgliedern einer Personenvereinigung zufließen soll.

Eine das Grundrecht auf Datenschutz berücksichtigende wertende Auslegung[83] der genannten Bestimmung legt den Schluss nahe, dass die einem Berufsdetektiv nach § 249 GewO eingeräumten Rechte zur Verwendung von personenbezogenen Daten von einem konkreten Auftrag abhängig sind.[84] Die Datenermittlung bzw. -verwendung "aus Interesse" oder "auf Vorrat" ist m.E. nicht zulässig. Der Betrieb einer Datenanwendung ehemals verdächtigter Personen ist einem Detektiv somit nicht gestattet.

Folgt man hingegen der Auffassung, die von der Gewerbeordnung eingeräumten Befugnisse eines Berufsdetektivs stünden diesem unabhängig von einem

---

Bezüglich des besonderen Schutzes dieser Daten gibt § 14 DSG unter Berücksichtigung vom Stand der technischen Möglichkeiten und wirtschaftlichen der Vertretbarkeit die zu ergreifenden Maßnahmen vor.

[83] Zur Gesetzesauslegung siehe z.B. *Antoniolli-Koja*, Allgemeines Verwaltungsrecht (1986), 91 ff.

[84] So auch das überwiegende Verständnis der Berufsdetektivbranche ("Standesregeln").

konkreten Auftrag zu, bleibt zu prüfen, ob der Betrieb einer Datei ehemals Verdächtiger deren schutzwürdige Geheimhaltungsinteressen verletzt. § 8 Abs. 4 DSG legt fest, wann schutzwürdige Geheimhaltungsinteressen eines Betroffenen bei der 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 nicht verletzt werden. Gemäß § 8 Abs. 4 Z 3. DSG kann sich die Zulässigkeit der Verwendung dieser Daten aus gesetzlichen Sorgfaltspflichten oder sonstigen, die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegenden berechtigten Interessen des Auftraggebers ergeben, wenn die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen nach dem Datenschutzgesetz gewährleistet.

Will ein Detektiv Daten in einer Datei verarbeiten, wird er somit nachzuweisen haben, dass diese Datenanwendung den genannten Anforderungen entspricht.[85] Da es sich um strafrechtlich relevante Daten handelt, darf die Verarbeitung weiters erst nach erfolgter Registrierung, bzw. wenn innerhalb von zwei

[85] Eine Meldung im Sinne des § 17 DSG hat zu enthalten:
1. den Namen (die sonstige Bezeichnung) und die Anschrift des Auftraggebers sowie eines allfälligen Vertreters gemäß § 6 Abs. 3 oder eines Betreibers gemäß § 50 Abs. 1, weiters die Registernummer des Auftraggebers, sofern ihm eine solche bereits zugeteilt wurde, und
2. den Nachweis der gesetzlichen Zuständigkeit oder der rechtlichen Befugnis für die erlaubte Ausübung der Tätigkeit des Auftraggebers, soweit dies erforderlich ist, und
3. den Zweck der zu registrierenden Datenanwendung und ihre Rechtsgrundlagen, soweit sich diese nicht bereits aus den Angaben nach Z. 2 ergeben, und
4. die Kreise der von der Datenanwendung Betroffenen und die über sie verarbeiteten Datenarten und
5. die Kreise der von beabsichtigten Übermittlungen Betroffenen, die zu übermittelnden Datenarten und die zugehörigen Empfängerkreise - einschließlich allfälliger ausländischer Empfängerstaaten - sowie die Rechtsgrundlagen der Übermittlung und
6. - soweit eine Genehmigung der Datenschutzkommission notwendig
ist - die Geschäftszahl der Genehmigung durch die Datenschutzkommission sowie
7. allgemeine Angaben über die getroffenen Datensicherheitsmaßnahmen im Sinne des § 14, die eine vorläufige Beurteilung der Angemessenheit der Sicherheitsvorkehrungen erlauben.

Monaten nach erfolgter Meldung[86] kein Verbesserungsauftrag erfolgt ist, aufgenommen werden (vgl. § 9 Abs. 6 DVRV).[87]

Abgesehen von jenen Fällen, in welchen der Betroffene in die Verwendung seiner Daten einwilligt, wird sein schutzwürdiges Geheimhaltungsinteresse höherwertig als das detektivische Informationsinteresse sein, weshalb davon ausgegangen werden darf, dass eine "Verdächtigendatei" von der Datenschutzkommission nicht genehmigt werden würde.

Aufnahme in die Datei:

Eine Aufnahme in die firmeninterne Datei verdächtigter Personen setzt wiederum voraus, dass es sich dabei um eine zulässige Datenanwendung handelt. Wird ein neuer Satz personenbezogener Daten angelegt, so kann dies, abhängig von den Intentionen des Detektivs, ein "Ermitteln von Daten" iS. § 4 Z 10 DSG oder ein "Verwenden von Daten" iS. § 4 Z 9 DSG darstellen.

Jede Art der Handhabung von Daten einer derartigen Datenanwendung setzt die Zustimmung des Betroffenen voraus, wobei eine Zustimmungserklärung nur dann gültig ist, wenn sie vom Betroffenen in Kenntnis der Sachlage für den konkreten Fall und ohne Zwang abgegeben wird.[88] Bezüglich nicht-sensibler Daten muss die Zustimmung weder ausdrücklich noch schriftlich erfolgen.[89] Da strafrechtsrelevante Daten jedoch in die Nähe sensibler Daten gerückt werden, ist in Fällen, in welchen eine verdächtigte Person einem Detektiv die Verwen-

---

[86] Datenschutzkommission, 1011 Wien, Bäckerstraße 20. Download der Meldeformulare auf Grund der Anordnung § 5 Abs. 1 Datenverarbeitungsregister-Verordnung 2000 - DVRV, BGBl. II Nr. 520/1999 unter: www.bka.gv.at/datenschutz/ . Die Meldung hat an das Datenverarbeitungsregister bei der Datenschutzkommission zu erfolgen. Sie kann per E-Mail eingebracht werden (dvrpost@bka.gv.at). Das Datenverarbeitungsregister befindet sich in 1010 Wien, Hohenstaufengasse 3.

[87] Eine Meldung kann nur unterbleiben, wenn die Datenanwendung rein private Datenanwendungen enthält, ausschließlich veröffentlichte Daten oder nur indirekt personenbezogene Daten verwendet, weiters für publizistische Tätigkeiten genutzt wird, für Datenanwendungen der Staatssicherheit, Landesverteidigung und Strafverfolgung unter gewissen Voraussetzungen, für Standardanwendungen.

[88] Siehe § 4 Z 14 DSG.

[89] Bezüglich der Verwendung sensibler Daten vgl. *Duschanek/Rosenmayr-Klemenz*, Datenschutzgesetz 2000, 52, Kommentar zu § 9, Rz 4. wonach für die Zulässigkeit der Verwendung sensibler Daten die Zustimmung "ausdrücklich" erteilt werden muss, was in der Regel Schriftlichkeit bedeute. Mit Hinweis auf *Ehrmann/Helfrich*, 136, erachten die Kommentatoren digitale

dung ihrer personenbezogenen Daten gestattet, die Gültigkeit der Zustimmungserklärung besonders kritisch zu prüfen. Vielfach wird sich eine nach § 86 Abs. 2 StPO angehaltene Person in einem Zustand "verdünnter Willensfreiheit" befinden und deshalb eine gültige Zustimmungserklärung gar nicht abgeben können. Eine Aufnahme in die Datenanwendung ist in derartigen Fällen unzulässig.

Informationsverbundsystem:

Nach der Legaldefinition in § 4 Z. 13 DSG handelt es sich bei einem Informationsverbundsystem um die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber[90] 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. Gemäß § 50 DSG haben die Auftraggeber eines Informationsverbundsystems einen geeigneten Betreiber[91] für das System zu bestellen, welcher der Datenschutzkommission zur Eintragung in das Datenverarbeitungsregister bekannt zu geben ist.[92]

Ein Informationsverbundsystems darf erst nach erfolgter Prüfung (Vorabkontrolle) durch die Datenschutzkommission die Verarbeitung aufnehmen (§ 18 Abs. 2 DSG). Wird innerhalb von zwei Monaten nach Erstattung der Meldung[93] kein Verbesserungsauftrag erteilt und die Verarbeitung nicht bescheidmäßig untersagt, darf der Vollbetrieb aufgenommen werden (§ 20 Abs. 5 DSG).[94]

Ein vollständiges Register der strafrechtlichen Verurteilungen darf nach Art. 8 Abs. 5 DSRL jedoch nur "unter behördlicher Aufsicht" geführt werden.

Zustimmungen, die ein aktives Tätigwerden des Betroffenen voraussetzen, ebenfalls als zulässig.

[90] Auftraggeber eines Datenverbundsystems ist der jeweils Daten einmeldende oder abfragende Detektiv.

[91] Der Betreiber ist "Ansprechpartner" des Betroffenen und ist vor allem für die Datensicherheit des Systems verantwortlich.

[92] Wird die Meldung unterlassen, treffen jeden einzelnen Auftraggeber die Pflichten des Informationsverbundbetreibers.

[93] Meldeformulare der Datenschutzkommission unter: www.bka.gv.at/datenschutz .

Auch wenn das DSG keine ausdrückliche Regelung über "vollständige Register strafrechtlicher Verurteilungen" enthält, wird man im Sinne einer richtlinienkonformen Interpretation davon ausgehen müssen, dass ein derartiges Register nur von staatlichen Behörden geführt werden darf.[95] Melden hingegen ausschließlich Detekteien Daten Verdächtiger in ein Informationsverbundsystem ein, wird dieses niemals alle Verdachtsfälle und noch weniger die Fälle, welche tatsächlich zu einer strafrechtlichen Verurteilungen führten, enthalten können.[96] Selbst wenn man davon ausgeht, dass die Sicherheitsbehörden speziell im Bereich des Ladendiebstahls überwiegend über Aufforderung eines Detektivs einschreiten und ein Informationsverbundsystem mit Daten verdächtigter Personen im Laufe der Zeit einen solchen Umfang annehmen kann, dass durch die Abfrage mit großer Wahrscheinlichkeit bestimmt werden kann, ob eine Person bereits einschlägig aufgefallen ist, sind derartige Register privater Auftraggeber - trotz der evidenten datenschutzrechtlichen Gefährdungspotentiale - nicht von vornherein unzulässig.

Die Verwendung von Daten des Ladendiebstahls verdächtiger Personen ist dann zulässig, wenn berechtigte Interessen des Auftraggebers vorliegen, welche die schutzwürdigen Geheimhaltungsinteressen des Betroffenen überwiegen und die Art und Weise, in der die Datenanwendung vorgenommen wird, die Wahrung der Interessen der Betroffenen gewährleistet.[97] Liegt eine gültige Zustimmung des Betroffenen vor, ist die Verletzung schutzwürdiger Geheimhaltungsinteressen denkunmöglich. Bei der Beurteilung der Interessenlage in den restlichen Fällen kommt es auf die Art der Daten und ihre Nähe zum Privat- und Familienleben des Betroffenen an. Diesbezüglich wurde in der Literatur eine Skala aufgestellt, wobei die Schutzwürdigkeit und damit die Vermutung der Unzulässigkeit einer Datenübermittlung von oben nach unten zunimmt, welche auch in gegebenen Zusammenhang herangezogen werden kann.[98] Berücksich-

---

[94] Gegen Bescheide der Datenschutzkommission sind keine ordentlichen Rechtsmittel zulässig, es kann jedoch Beschwerde an VfGH oder VwGH erhoben werden.
[95] Vgl. *Duschanek/Rosenmayr-Klemenz*, 49.
[96] *Duschanek/Rosenmayr-Klemenz*, 48, weisen besonders auf die Einbeziehung von Verdachtsfällen hin. Nach *Drobesch/Grosinger*, 140, erfasst Abs. 4 lex.cit. nicht nur Daten über Verurteilte sondern auch jene über Tatverdächtige, Beschuldigte und Angeklagte. Außerdem sind strafbare Handlungen, die nach dem Verwaltungsstrafrecht zu ahnden sind, mitumfasst.
[97] Vgl. § 8 Abs. 4 Z. 3 DSG.
[98] Vgl. *Stadler*, Wirtschaftsinformationen und Datenschutz, ÖZW 1979, 9 (13).

tigt man die durch das DSG 2000 eingeführten sensiblen Daten, lässt sich die Schutzwürdigkeit wie folgt darstellen:

- Zulässigerweise veröffentlichte Daten oder nur indirekt personenbezogene Daten (keine schutzwürdigen Geheimhaltungsinteressen)
- Nicht-sensible Daten
- Daten in allgemeinen Informationsverbundsystemen
- Informationsverbundsysteme mit strafrechtlich relevanten Daten
- Sensible Daten.

Die Verwendung strafrechtsbezogener Daten in einem Informationsverbundsystem weisen somit eine besondere Nähe zum Privat- und Familienleben des Betroffenen auf. Ein berechtigtes Interesse des Berufsdetektivs an der Verwendung der gegenständlichen Daten kann weder aus der Gewerbeordnung noch aus sonstigen Bestimmungen abgeleitet werden, weshalb ein derartiges Informationsverbundsystem m.E. von der Datenschutzkommission nicht genehmigen werden darf.

Datenübermittlung an den geschädigten Kaufhausbetreiber:

Werden Daten an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister weitergegeben, stellt dies ein "Übermitteln von Daten" iS. § 4 Z. 12 DSG dar. Die Fälle, in den der Kaufhausbetreiber als datenschutzrechtlicher Auftraggeber zu qualifizieren ist, stellen somit kein Problem hinsichtlich der Datenweitergabe an ihn dar. Ist der Berufsdetektiv hingegen datenschutzrechtlicher Auftraggeber, ist die Zulässigkeit der Datenübermittlung im Einzelfall zu prüfen.[99]

Gemäß § 7 Abs. 2 DSG dürfen Daten nur übermittelt werden, wenn sie aus einer zulässigen Datenanwendung stammen, der Empfänger dem Übermittelnden seine ausreichende Zuständigkeit oder rechtliche Befugnis im Hinblick auf den Übermittlungszweck glaubhaft gemacht hat und durch den Zweck und Inhalt der

[99] Zur Frage, wann der Berufsdetektiv datenschutzrechtlicher Auftraggeber ist, vgl. Seite 11 ff.

Übermittlung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzt werden.

Nach der Rechtssprechung ist eine Datenübermittlung zulässig, wenn sie mit der Entfaltung einer zumindest typischerweise dem rechtlich anerkannten Zweck des Übermittlers dienenden Tätigkeit zwangsläufig verbunden ist.[100] Jedenfalls gilt dies, soweit eine derartige Unternehmensfunktion in der Rechtsordnung allgemein anerkannt ist.[101] Die Tätigkeit eines Berufsdetektivs ist eine solche, mit der - von der Rechtsordnung anerkannt - die Übermittlung von Recherchеergebnissen an den Auftraggeber zwangsläufig verbunden ist. Die rechtliche Befugnis des Kaufhausbetreibers liegt in der Geltendmachung seiner Forderungen gegen den mutmaßlichen Dieb, ein schutzwürdiges Geheimhaltungsinteresse des Betroffenen liegt in dieser Konstellation nicht vor, weshalb eine Übermittlung der vom Detektiv erhobenen Daten an den Kaufhausbetreiber zulässig ist.[102]

In welcher Form die Daten dem Geschädigten dabei mitgeteilt werden, ist rechtlich unerheblich. Bisher war es üblich, dass ein Detektiv seinem Auftraggeber in einem schriftlichen Bericht die Ermittlungsergebnisse mitteilt. Denkbar ist aber auch, dass der Kunde künftig via Internet den Stand der Ermittlungen verfolgen kann und auch den Endbericht auf diese Weise abruft.[103]

Datenübermittlung ins Ausland:

Da der Berufsdetektiv Kunden im Geschäftslokal seines Auftraggebers beobachtet, verfügt dieser zwangsläufig über eine Niederlassung in Österreich. Zu einer Übermittlung ins Ausland kann es jedoch kommen, wenn Ermittlungser-

[100] Vgl. OGH 5.4.1991, EDVuR 1991, 172.
[101] Vgl. *Duschanek*, Datenweitergabe bei Inanspruchnahme von Werkleistungen, ecolex 1990, 581.
[102] OGH 26.8.1999, 2 Ob 244/99t: Jeder Weitergabe von Daten muss eine Interessenabwägung vorangehen, wobei im Zweifel die Vermutung für die Schutzwürdigkeit spricht. Als berechtigte Interessen eines Dritten sind dabei auch auf gesetzlicher oder vertraglicher Grundlage beruhende Ansprüche anerkannt.
[103] Global agierende Paketzustellunternehmen bieten ihren Kunden die Möglichkeit, den Weg ihrer Sendung via Internet zu verfolgen. Auch einige österreichische Rechtsanwälte geben ihren Mandanten die Möglichkeit, nach Eingabe eines Passwortes den jeweils aktuellen Aktenstand online abzurufen. Vielleicht werden auch Detekteien in Zukunft ein entsprechendes Service anbieten.

gebnisse direkt an die im Ausland situierte Hauptniederlassung des Kaufhauseigentümers geleitet werden. Innerhalb der Europäischen Union unterliegt die Übermittlung von zulässigerweise ermittelten Daten durch einen Detektiv an seinen Auftraggeber nach § 12 DSG grundsätzlich keinen Beschränkungen. Eine derartige Übermittlung ist wie ein Datentransfer im Inland zu behandeln.

Weiters bedarf auch die Datenübermittlung an Empfänger in Drittstaaten - abgesehen von den für einen Detektiv wenig praktikablen Ausnahmen nach § 12 Abs. 3 DSG[104] - keiner Genehmigung, wenn im jeweiligen Land ein angemessener Datenschutz gewährleistet ist. Bezüglich der Schweiz und Ungarn besteht eine Verordnung des Bundeskanzlers,[105] welche diesen Länder ein angemessenes Datenschutzniveau attestiert und den Mitgliedsstaaten der Europäischen Union gleichstellt. In alle anderen Länder ist eine Übermittlung und Überlassung von Daten nur nach erfolgter Genehmigung durch die Datenschutzkommission zulässig.[106]

[104] § 12 Abs. 3 DSG lautet: "Darüber hinaus ist der Datenverkehr ins Ausland dann genehmigungsfrei, wenn
1. die Daten im Inland zulässigerweise veröffentlicht wurden oder
2. Daten, die für den Empfänger nur indirekt personenbezogen sind, übermittelt oder überlassen werden oder
3. die Übermittlung oder Überlassung von Daten ins Ausland in Rechtsvorschriften vorgesehen ist, die im innerstaatlichen Recht den Rang eines Gesetzes haben und unmittelbar anwendbar sind, oder
4. Daten aus Datenanwendungen für private Zwecke (§ 45) oder für publizistische Tätigkeit (§ 48) übermittelt werden oder
5. der Betroffene ohne jeden Zweifel seine Zustimmung zur Übermittlung oder Überlassung seiner Daten ins Ausland gegeben hat oder
6. ein vom Auftraggeber mit dem Betroffenen oder mit einem Dritten eindeutig im Interesse des Betroffenen abgeschlossener Vertrag nicht anders als durch Übermittlung der Daten ins Ausland erfüllt werden kann oder
7. die Übermittlung zur Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen vor ausländischen Behörden erforderlich ist und die Daten rechtmäßig ermittelt wurden, oder
8. die Übermittlung oder Überlassung in einer Standardverordnung (§ 17 Abs. 2 Z 6) oder Musterverordnung (§ 19 Abs. 2) ausdrücklich angeführt ist oder
9. es sich um Datenverkehr mit österreichischen Dienststellen im Ausland handelt oder
10. Übermittlungen oder Überlassungen aus Datenanwendungen erfolgen, die gemäß § 17 Abs. 3 von der Meldepflicht ausgenommen sind."

[105] Verordnung des Bundeskanzlers über den angemessenen Datenschutz in Drittstaaten (Datenschutzangemessenheits-Verordnung - DSAV), BGBl. II Nr. 521/1999.

[106] Für den europäischen Raum ist somit zu beachten, dass auch Datenübermittlungen nach Norwegen und in das Fürstentum Liechtenstein genehmigungspflichtig sind.

Rechtsdurchsetzung:

Kontrollbefugnisse der Datenschutzkommission:

Gemäß § 30 DSG kann die Datenschutzkommission bei Vorliegen eines begründeten Verdachts auf Verletzung von Rechten eines Betroffenen oder Pflichten eines Auftraggebers oder Dienstleisters die betreffende Datenanwendung überprüfen, wobei sie vom Auftraggeber oder Dienstleister der überprüften Datenanwendung insbesondere alle notwendigen Aufklärungen verlangen und Einschau in die Datenanwendung und die diesbezüglichen Unterlagen begehren kann.

Datenanwendungen, die der Vorabkontrolle unterliegen können von der Datenschutzkommission auch ohne Vorliegen eines Verdachts auf rechtswidrige Datenverwendung überprüft werden. Dazu zählen meldepflichtige Datenanwendungen, die weder einer Musteranwendung nach § 19 Abs. 2 DSG entsprechen, noch innere Angelegenheiten der anerkannten Kirchen und Religionsgesellschaften betreffen, sofern sie den Kriterien des § 18 Abs. 2 Z. 1 - 4 DSG entsprechen. Für den Tätigkeitsbereich von Berufsdetektiven kommen dabei Informationsverbundsysteme und Datenanwendungen in Frage, welche strafrechtlich relevante Daten iS. § 8 Abs. 4 DSG enthalten.

Nach Verständigung des Inhabers der Räumlichkeiten und des Auftraggebers (Dienstleisters) ist die Datenschutzkommission berechtigt, Räume, in welchen Datenanwendungen vorgenommen werden, zwecks Einschau zu betreten und Datenverarbeitungsanlagen in Betrieb zu setzten, die zu überprüfenden Verarbeitungen durchzuführen sowie Kopien von Datenträgern herzustellen. Bei der unter möglichster Schonung seiner Rechte und der Rechte Dritter durchzuführenden Kontrolltätigkeit hat der Auftraggeber bzw. Dienstleister die für die Einschau notwendige Unterstützung zu leisten.

Informationen, die der Datenschutzkommission bei ihrer Kontrolltätigkeit zukommen, dürfen ausschließlich für die Kontrolle im Rahmen der Vollziehung datenschutzrechtlicher Vorschriften verwendet werden. Wenn die Einschau jedoch den Verdacht einer strafbaren Handlung nach §§ 51 oder 52 DSG oder

eines Verbrechens nach § 278a StGB (kriminelle Organisation),[107] oder eines Verbrechens mit einer Freiheitsstrafe, deren Höchstmaß 5 Jahre übersteigt, ergibt, ist die Datenschutzkommission verpflichtet, Anzeige zu erstatten. Weiters sind den Strafgerichten Informationen betreffend solcher Verbrechen oder Vergehen zu geben, um welche diese nach § 26 StPO ersucht haben.[108]

Die Datenschutzkommission kann zur Herstellung des rechtmäßigen Zustandes Empfehlungen aussprechen und für deren Befolgung erforderlichenfalls eine angemessene Frist setzen. Wird einer solchen Empfehlung nicht entsprochen, kann die Datenschutzkommission ein Verfahren zur Überprüfung der Registrierung gemäß § 22 Abs. 4 einleiten, oder Strafanzeige nach §§ 51 oder 52 erstatten, oder bei schwerwiegenden Verstößen durch Auftraggeber des privaten Bereichs Klage vor dem zuständigen Gericht gemäß § 32 Abs. 5 erheben, oder bei

---

[107] § 278a. StGB lautet:
"(1) Wer eine auf längere Zeit angelegte unternehmensähnliche Verbindung einer größeren Zahl von Personen gründet oder sich an einer solchen Verbindung als Mitglied beteiligt,
1. die, wenn auch nicht ausschließlich, auf die wiederkehrende und geplante Begehung schwerwiegender strafbarer Handlungen, die das Leben, die körperliche Unversehrtheit, die Freiheit oder das Vermögen bedrohen, oder schwerwiegender strafbarer Handlungen im Bereich der sexuellen Ausbeutung von Menschen, der Schlepperei oder des unerlaubten Verkehrs mit Kampfmitteln, Kernmaterial und radioaktiven Stoffen, gefährlichen Abfällen, Falschgeld oder Suchtmitteln ausgerichtet ist,
2. die dadurch eine Bereicherung in großem Umfang oder erheblichen Einfluß auf Politik oder Wirtschaft anstrebt und
3. die andere zu korrumpieren oder einzuschüchtern oder sich auf besondere Weise gegen Strafverfolgungsmaßnahmen abzuschirmen sucht, ist mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen. § 278 Abs. 2 gilt entsprechend.
(2) Wer wissentlich Bestandteile des Vermögens einer kriminellen Organisation (Abs. 1) in deren Auftrag oder Interesse an sich bringt, verwahrt, anlegt, verwaltet, umwandelt, verwertet oder einem Dritten überträgt, ist mit Freiheitsstrafe bis zu drei Jahren, wer die Tat in bezug auf einen 500 000 S übersteigenden Wert begeht, mit Freiheitsstrafe von sechs Monaten bis zu fünf Jahren zu bestrafen. § 165a gilt entsprechend."

[108] § 26 StPO lautet:
"(1) Die Strafgerichte sind berechtigt, zur Durchführung der Strafrechtspflege mit allen Dienststellen der Gebietskörperschaften, mit anderen Körperschaften des öffentlichen Rechtes sowie mit den von ihnen betriebenen Anstalten unmittelbares Einvernehmen durch Ersuchen zu pflegen. Solchen Ersuchen ist mit möglichster Beschleunigung zu entsprechen, oder es sind die entgegenstehenden Hindernisse unverzüglich bekanntzugeben; erforderlichenfalls ist Akteneinsicht zu gewähren.
(2) Ersuchen gemäß Abs. 1, die sich auf Straftaten einer bestimmten Person beziehen, dürfen mit dem Hinweis auf bestehende gesetzliche Verpflichtungen zur Verschwiegenheit oder darauf, dass es sich um automationsunterstützt verarbeitete personenbezogene Daten handelt, nur dann abgelehnt werden, wenn entweder diese Verpflichtungen ausdrücklich auch gegenüber Strafgerichten auferlegt sind oder wenn der Beantwortung überwiegende öffentliche Interessen entgegenstehen, die im einzelnen anzuführen und zu begründen sind.
(3) Die Strafgerichte können sich nach Maßgabe des Auslieferungs- und Rechtshilfegesetzes mit Ersuchen im Sinn der vorstehenden Bestimmungen auch an ausländische Behörden wenden, und zwar auf dem durch zwischenstaatliche Vereinbarungen oder allgemein anerkannte Regeln des Völkerrechtes vorgesehenen Weg."

Verstößen von Auftraggebern, die Organe einer Gebietskörperschaft sind, das zuständige oberste Organ befassen.

Ist die Datenschutzkommission über Anregung eines Betroffenen tätig geworden, ist dieser darüber zu informieren, wie mit seiner Eingabe verfahren wurde. Eine Eingabe kann nicht nur auf die Verletzung des DSG 2000 gegründet werden, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedsstaates der Europäischen Union, soweit solche Vorschriften gemäß § 3 DSG[109] im Inland anzuwenden sind.

Beschwerde an die Datenschutzkommission:

Bezüglich Auftraggebern des privaten Bereichs erkennt die Datenschutzkommission auf Antrag des Betroffenen ausschließlich über behauptete Verletzungen des Rechts auf Auskunft durch den Auftraggeber der Datenanwendung (§ 31 DSG).[110] Alle anderen Rechte hat der Betroffen vor den ordentlichen Gerichten durchzusetzen.

Wie Eingaben, können auch Beschwerden nach § 31 DSG nicht nur auf die Verletzung des DSG 2000 gegründet werden, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedsstaates der

[109] § 3 DSG lautet:
"(1) Die Bestimmungen dieses Bundesgesetzes sind auf die Verwendung von personenbezogenen Daten im Inland anzuwenden. Darüber hinaus ist dieses Bundesgesetz auf die Verwendung von Daten im Ausland anzuwenden, soweit diese Verwendung in anderen Mitgliedstaaten der Europäischen Union für Zwecke einer in Österreich gelegenen Haupt- oder Zweigniederlassung (§ 4 Z 15) eines Auftraggebers (§ 4 Z 4) geschieht.
(2) Abweichend von Abs. 1 ist das Recht des Sitzstaates des Auftraggebers auf eine Datenverarbeitung im Inland anzuwenden, wenn ein Auftraggeber des privaten Bereichs (§ 5 Abs. 3) mit Sitz in einem anderen Mitgliedstaat der Europäischen Union personenbezogene Daten in Österreich zu einem Zweck verwendet, der keiner in Österreich gelegenen Niederlassung dieses Auftraggebers zuzurechnen ist.
(3) Weiters ist dieses Bundesgesetz nicht anzuwenden, soweit personenbezogene Daten durch das Inland nur durchgeführt werden.
(4) Von den Abs. 1 bis 3 abweichende gesetzliche Regelungen sind nur in Angelegenheiten zulässig, die nicht dem Recht der Europäischen Gemeinschaften unterliegen."

[110] Gemäß § 31 Abs. 2 DSG die Datenschutzkommission zur Entscheidung über behauptete Verletzungen der Rechte eines Betroffenen auf Geheimhaltung, auf Richtigstellung oder auf Löschung dann zuständig, wenn der Betroffene seine Beschwerde gegen einen Auftraggeber des öffentlichen Bereichs richtet, der nicht als Organ der Gesetzgebung oder der Gerichtsbarkeit tätig ist.

Europäischen Union, soweit solche Vorschriften gemäß § 3 DSG im Inland anzuwenden sind.[111]

Klage vor den ordentlichen Gerichten:

Ansprüche gegen Auftraggeber des privaten Bereichs wegen Verletzung der Rechte des Betroffenen auf Geheimhaltung, auf Richtigstellung oder Löschung sind vom Betroffenen auf dem Zivilrechtsweg geltend zu machen (§ 32 Abs. 1 DSG). Das Recht auf Auskunft ist von Betroffenen auch gegenüber Auftraggebern des privaten Bereichs vor der Datenschutzkommission, geltend zu machen.

Für Klagen und Anträge auf Erlassung einer einstweiligen Verfügung ist in erster Instanz das mit der Ausübung der Gerichtsbarkeit in bürgerlichen Rechtssachen betraute Landesgericht zuständig, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat. Der Betroffene kann seine Klage jedoch wahlweise auch beim Landesgericht des Sprengels erheben, in welchem der Auftraggeber oder Dienstleister seinen gewöhnlichen Aufenthalt oder Sitz hat.[112]

Der Betroffene kann auf Unterlassung und Beseitigung des gesetzwidrigen Zustandes klagen, wobei zur Sicherung des Unterlassungsanspruchs selbst dann eine einstweilige Verfügungen erlassen werden kann, wenn die Voraussetzungen nach § 381 EO nicht zutreffen.[113]

---

[111] Auf Datenverarbeitungen in Österreich ist dann das Datenschutzrecht eines anderen EU-Staates anzuwenden, wenn Daten in Österreich für einen Auftraggeber des privaten Bereichs aus einem anderen EU-Staat verarbeitet werden, ohne dass dieser eine feste Betriebsstätte in Österreich hat. Für die Fälle, in welchen ein Kaufhaus in Österreich einen Berufsdetektiv beauftragt, ist diese Regelung - da ja eine Betriebsstätte im Inland vorliegt - somit ohne praktischer Bedeutung.

[112] Dem Betroffenen kommt somit ein Wahlrecht als Kläger zu, der Auftraggeber hingegen kann Klagen, etwa auf Kostenersatz gemäß § 26 Abs. 6 DSG nur bei dem Landesgericht einbringen, in dessen Sprengel der Betroffene seinen gewöhnlichen Aufenthalt oder Sitz hat. (siehe auch *Drobesch/Grosinger*, 236).

[113] § 381 EO lautet:
"Zur Sicherung anderer Ansprüche können einstweilige Verfügungen getroffen werden:
1. wenn zu besorgen ist, dass sonst die gerichtliche Verfolgung oder Verwirklichung des fraglichen Anspruches, insbesondere durch eine Veränderung des bestehenden Zustandes, vereitelt oder erheblich erschwert werden würde; als solche Erschwerung ist es anzusehen, wenn das Urteil in Staaten vollstreckt werden müßte, die weder das Übereinkommen vom 27. September 1968 über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in

In Fällen, in welchen ein begründeter Verdacht vorliegt, ein Auftraggeber des privaten Bereichs mache sich einer schwerwiegenden Datenschutzverletzung schuldig, hat die Datenschutzkommission eine Feststellungsklage nach § 228 ZPO beim zuständigen Gericht zu erheben.

Wird dies vom Betroffenen verlangt und ist es zur Wahrung der Interessen einer größeren Zahl von Betroffenen geboten, hat die Datenschutzkommission einem Rechtsstreit auf Seiten des Betroffenen als Nebenintervenient (§§ 17 ff ZPO) beizutreten.

Klagen können auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedsstaates der Europäischen Union, soweit solche Vorschriften gemäß § 3 DSG im Inland anzuwenden sind, gestützt werden.

Schadenersatz:

Erleidet ein Betroffener dadurch einen Schaden, dass der Auftraggeber oder Dienstleister schuldhaft Daten entgegen den Bestimmungen des Datenschutzgesetzes verwendet, so ist ihm dieser nach den allgemeinen Bestimmungen des bürgerlichen Rechts zu ersetzen (§ 33 DSG).
Handelt es sich um einen besonders schwerwiegenden Fall der Datenschutzverletzung, welcher einer Bloßstellung des Betroffenen gemäß § 7 Abs. 1 MedienG[114] gleichkommt, besteht sogar ein Anspruch auf angemessene Entschädigung für die erlittene Kränkung. Ein besonders schwerwiegender Fall einer Datenschutzverletzung liegt vor, wenn die Verletzung mit meldepflichtigen Daten erfolgt, welche der Vorabkontrolle durch die Datenschutzkommission unterliegen. Gemäß § 18 Abs. 2 DSG handelt es sich dabei um Datenanwendungen,

---

Zivil- und Handelssachen noch das Übereinkommen vom 16. September 1988 über die gerichtliche Zuständigkeit und die Vollstreckung gerichtlicher Entscheidungen in Zivil- und Handelssachen ratifiziert haben;
2. wenn derartige Verfügungen zur Verhütung drohender Gewalt oder zur Abwendung eines drohenden unwiederbringlichen Schadens nöthig erscheinen."

[114] § 7 Abs. 1 MedienG lautet:
"Wird in einem Medium der höchstpersönliche Lebensbereich eines Menschen in einer Weise erörtert oder dargestellt, die geeignet ist, ihn in der Öffentlichkeit bloßzustellen, so hat der Betroffene gegen den Medieninhaber (Verleger) Anspruch auf eine Entschädigung für die erlittene Kränkung. Der Entschädigungsbetrag darf 200 000 S nicht übersteigen; im übrigen ist § 6 Abs. 1 zweiter Satz anzuwenden."

die sensible oder strafrechtlich relevante Daten im Sinne § 8 Abs. 4 DSG enthalten oder die Auskunfterteilung über die Kreditwürdigkeit der Betroffenen zum Zweck haben oder in Form eines Informationsverbundsystems durchgeführt werden. Die Tätigkeit eines Berufsdetektivs kann - abgesehen von der Erteilung von Auskünften über Kreditverhältnisse, welche er gemäß § 249 Abs. 4 GewO nicht zu erteilen berechtigt ist, alle genannten vorabkontrollpflichtigen Datenanwendungen mit sich bringen.

Drobesch/Grosinger führen unter Hinweis auf die EB aus, dass das DSG insgesamt als Schutzgesetz im Sinne des § 1311 ABGB zu verstehen sei, da es abstrakte Gefährdungsverbote normiert, die auf den Schutz der Mitglieder eines bestimmten Personenkreises (von einer Datenverarbeitung Betroffene) vor Verletzung eines Rechtsgutes (das Datengeheimnis) abzielen. Demzufolge hafte etwa der Auftraggeber oder Dienstleister, auch wenn im Einzelfall der aus der Verbotsübertretung entstandene Schaden nicht vorhersehbar war. Ebenso bedürfe es keines strikten Nachweises des Kausalzusammenhangs, weil die Kausalität der in der Missachtung der Norm liegenden Pflichtwidrigkeit für die Schadensfolgen, deren Eintritt das DSG gerade zu verhindern bestimmt ist, vermutet wird.[115]

Besteht der begründete Verdacht, dass eine schwerwiegende Datenschutzverletzung durch einen Auftraggeber des privaten Bereichs vorliegt, ist die Datenschutzkommission ermächtigt, eine Feststellungsklage zu erheben, um damit den Betroffenen die Durchsetzung immaterieller Schadenersatzforderungen zu erleichtern.[116]

Schadenersatzansprüche nach § 33 DSG können nicht nur auf die Verletzung der Vorschriften des DSG 2000 gestützt werden, sondern auch auf die Verletzung von datenschutzrechtlichen Vorschriften eines anderen Mitgliedsstaates der EU, soweit solche Vorschriften gemäß § 3 DSG im Inland anzuwenden sind.

[115] *Drobesch/Grosinger*, 245.
[116] Siehe § 32 Abs. 5 DSG.

Verjährungsfristen:

Gemäß § 34 DSG erlischt der Anspruch auf Behandlung einer Eingabe nach § 30, einer Beschwerde nach § 31 oder einer Klage nach § 32, wenn der Einschreiter sie nicht binnen eines Jahres, nachdem er Kenntnis von dem beschwerenden Ereignis erlangt hat, längstens aber binnen drei Jahren, nachdem das Ereignis behauptetermaßen stattgefunden hat, einbringt.

Strafbestimmungen:

Gerichtlich strafbare Handlungen:

Das Datenschutzgesetz 2000 enthält eine einzige gerichtliche Strafbestimmung, die Datenverwendung in Gewinn- oder Schädigungsabsicht (§ 51 DSG).[117] Danach ist, wenn die Tat nicht nach einer anderen Bestimmung mit strengerer Strafe bedroht ist, vom Gericht mit Freiheitsstrafe bis zu einem Jahr zu bestrafen, wer in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, personenbezogene Daten, die ihm ausschließlich auf Grund seiner berufsmäßigen Beschäftigung anvertraut oder zugänglich geworden sind oder die er sich widerrechtlich verschafft hat, selbst benützt, einem anderen zugänglich macht oder veröffentlicht, obwohl der Betroffene an diesen Daten ein schutzwürdiges Geheimhaltungsinteresse hat. Der Täter ist nur mit Ermächtigung des Verletzten zu verfolgen.

Die Datenverwendung in Gewinn- oder Schädigungsabsicht kann mit der Datenbeschädigung nach § 126a StGB und dem Betrügerischen Datenverarbeitungsmissbrauch nach § 148a StGB konkurrieren.

Gemäß § 126a Abs. 3 StGB ist, wer einen anderen dadurch schädigt, dass er automationsunterstützt verarbeitete, übermittelte oder überlassene Daten, über die er nicht oder nicht allein verfügen darf, verändert, löscht oder sonst unbrauchbar macht oder unterdrückt, wenn die Tat einen S 25.000,- übersteigenden Schaden herbeiführt, mit einer Freiheitsstrafe bis zu zwei Jahren (oder mit

[117] Das DSG 1978, BGBl. Nr. 565/1978, pönalisierte den Geheimnisbruch in § 48 und den unbefugten Eingriff in den Datenverkehr in § 49.

Geldstrafe bis zu 360 Tagessätzen) zu bestrafen. Übersteigt der Schaden S 500.000,-, beträgt die Freiheitsstrafe zischen sechs Monaten und fünf Jahren.

Nach § 148a StGB ist, wer mit dem Vorsatz, sich oder einen Dritten unrechtmäßig zu bereichern, einem anderen dadurch am Vermögen schädigt, dass er das Ergebnis einer automationsunterstützten Datenverarbeitung durch Gestaltung des Programms, durch Eingabe, Veränderung oder Löschung von Daten oder sonst durch Einwirkung auf den Ablauf des Verarbeitungsvorgangs beeinflusst, wenn er die Tat gewerbsmäßig begeht oder durch die Tat einen S 25.000,- übersteigenden Schaden herbeiführt, mit Freiheitsstrafe bis zu drei Jahren zu bestrafen. Übersteigt der Schaden S 500.000,-, beträgt die Freiheitsstrafe zwischen einem und zehn Jahren.

Verwaltungsstrafbestimmungen:

§ 52 DSG:

(1) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet oder nach anderen Verwaltungsstrafbestimmungen mit strengerer Strafe bedroht ist, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 260 000 S zu ahnden ist, wer

1. sich vorsätzlich widerrechtlichen Zugang zu einer Datenanwendung verschafft oder einen erkennbar widerrechtlichen Zugang vorsätzlich aufrechterhält oder
2. Daten vorsätzlich in Verletzung des Datengeheimnisses (§ 15) übermittelt, insbesondere Daten, die ihm gemäß §§ 46 oder 47 anvertraut wurden, vorsätzlich für andere Zwecke verwendet oder
3. Daten entgegen einem rechtskräftigen Urteil oder Bescheid verwendet, nicht beauskunftet, nicht richtigstellt oder nicht löscht oder
4. Daten vorsätzlich entgegen § 26 Abs. 7 löscht.

(2) Sofern die Tat nicht den Tatbestand einer in die Zuständigkeit der Gerichte fallenden strafbaren Handlung bildet, begeht eine Verwaltungsübertretung, die mit Geldstrafe bis zu 130 000 S zu ahnden ist, wer

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

2. Daten ins Ausland übermittelt oder überlässt, ohne die erforderliche Genehmigung der Datenschutzkommission gemäß § 13 eingeholt zu haben oder
3. seine Offenlegungs- oder Informationspflichten gemäß den §§ 23, 24 oder 25 verletzt oder
4. die gemäß § 14 erforderlichen Sicherheitsmaßnahmen gröblich außer Acht läßt.
(3) Der Versuch ist strafbar.
(4) Die Strafe des Verfalls von Datenträgern und Programmen kann ausgesprochen werden (§§ 10, 17 und 18 VStG), wenn diese Gegenstände mit einer Verwaltungsübertretung nach Abs. 1 oder 2 in Zusammenhang stehen.
(5) Zuständig für Entscheidungen nach Abs. 1 bis 4 ist die Bezirksverwaltungsbehörde, in deren Sprengel der Auftraggeber (Dienstleister) seinen gewöhnlichen Aufenthalt oder Sitz hat. Falls ein solcher im Inland nicht gegeben ist, ist die am Sitz der Datenschutzkommission eingerichtete Bezirksverwaltungsbehörde zuständig.

Zweite Instanz ist der UVS.

Abschließende Bemerkungen:

§ 268 GewO räumt Adressenverlagen und Direktwerbeunternehmen ausdrücklich das Recht ein, die für ihre Tätigkeit erforderlichen Daten aus öffentlich zugänglichen Quellen, eigenen Erkundungen und aus Kunden- und Interessentendateien anderer zu beziehen und verpflichtet sie dabei zur Einhaltung des Datenschutzgesetzes.[118] Eine entsprechende Befugnis für Berufsdetektive fehlt in der Gewerbeordnung bisher, dürfte aber entbehrlich sein, da neben der zuständigen Wirtschaftskammer auch sonstige Berufsverbände und vergleichbare Einrichtungen in Verhaltensregeln festlegen können, was als Verwendung von

[118] § 268 Abs. 3 Z. 2 GewO verweist nach wie vor auf das Datenschutzgesetz 1978, BGBl. Nr. 565/1978. § 61 Abs. 7 DSG 2000 bestimmt, dass, soweit einzelne Vorschriften Verweise auf das Datenschutzgesetz 1978 enthalten, diese bis zu ihrer Anpassung an das DSG 2000 sinngemäß weitergelten. Die Formulierung, nach welcher Verweise "sinngemäß" weitergelten, wirft die Frage auf, ob das DSG 1978 weiter anzuwenden ist oder jene Bestimmungen des DSG 2000, welchem bezüglich ihres Regelungsgehaltes denjenigen des DSG 1978 entsprechen. Nach *Drobesch/Grosinger*, 304, perpetuiert § 61 Abs. 7 DSG 2000 jedoch tatsächlich die Geltung des DSG 1978 in bestimmten Bereichen. *Duschanek/Rosenmayr-Klemenz*, 164, führen hingegen aus, dass unter der "sinngemäßen Weitergeltung" von Vorschriften des DSG 1978 wohl nur verstanden werden könne, dass die jeweilige Regelung "iS" des DSG zu verstehen ist, also nach dem DSG 2000 zu beurteilen sei.

Daten nach Treu und Glauben anzusehen ist. Der Vorteil derartiger soft-law-Regeln gegenüber gesetzlichen Vorgaben liegt in ihrer größeren Flexibilität. Das Datenschutzgesetz 2000 bietet somit - abgesehen von extensiver Auslegung - eine durchaus praxistaugliche Möglichkeit zur Lösung der bisherigen Unsicherheiten seiner Anwendung durch Kaufhausdetektive. Die Festlegung von Verhaltensregeln iS. § 6 Abs. 4 DSG ist den Vertretern des Berufsstandes jedoch dringend anzuraten.