Die (un)überwindbaren Schranken des Datenschutzrechts für Unternehmen mit Fokus auf Informationsverbundsysteme

Paul Oberndorfer, Peter Trybus

Beurle Oberndorfer Mitterlehner Rechtsanwälte
Landstrasse 9, 4020 Linz
paul.oberndorfer@bom.at

Binder Grösswang Rechtsanwälte
Sterngasse 13, 1010 Wien
trybus@bgnet.at

Schlagworte: Datenschutz, Informationsverbundsystem, Datenschutzkommission, Verarbeitung von Daten

Abstract: Globalisierung und Vernetzung von Unternehmensgruppen führen zu einer Internationalisierung der Datenverwaltung und zur wesentlichen Erleichterung des unternehmens- und konzerninternen Datenaustausches. Dies stellt auch entsprechende Anforderungen an den Datenschutz. Das österreichische Datenschutzgesetz sieht hier im europäischen Vergleich eine Besonderheit vor: das Informationsverbundsystem. Der folgende Beitrag soll überblicksartig auf die datenschutzrechtlichen Besonderheiten von Informationsverbundsystemen eingehen.

1. Ausgangsfall

Konzerne und Unternehmensgruppen haben gegenüber kleineren Unternehmen einen erhöhten Bedarf an Informationsvernetzung, da diese Unternehmen oft Interesse daran haben, wechselseitig auf ermittelte und gespeicherte Daten zuzugreifen, diese zu übermitteln und weiter zu verarbeiten. In der Praxis kommen Unternehmensgruppen ihrem konzerninternen Informations- und Datenverwaltungsbedarf meist durch die Implementierung eines EDV-Systems zur entsprechenden Datenerfassung und -verwaltung nach.

Regelmäßig enthält ein derartiges EDV-System etwa folgende typische Dateninhalte:

– Informationen über die Gesellschaften des Konzerns (Daten zur Geschäftsentwicklung, Daten für das Risikomanagement, Statistiken, Bilanzen etc)
– Adress- und Kontaktdaten der Lieferanten und Kunden
– Vertragsbedingungen, spezifische Lieferanten- und Kundendaten (zB aus integrierten CRM-Systemen, einschließlich Informationen über die wirtschaftliche Situation der Kunden).[1]

Mit diesem EDV-System soll meist für alle Konzerngesellschaften ein möglichst weitgehender Zugriff auf die im EDV-System verwalteten Daten gewährleistet werden. Es besteht dann für jede Gesellschaft die Möglichkeit, Daten selbst zu ermitteln und diese Daten im EDV-System zu erfassen, zu speichern und zu bearbeiten.[2]

Erfasste, gespeicherte und bearbeitete Daten werden in der Praxis regelmäßig an verschiedene (Konzern-)Gesellschaften übermittelt.[3] Die Konzernmutter oder andere mit besonderen Aufgaben betraute Unternehmen sollen dazu in der Lage sein, auf bestimmte, von den einzelnen Konzerngesellschaften erfasste Daten zuzugreifen. Ein derartiges System könnte als Informationsverbund zu qualifizieren sein (siehe dazu im Folgenden).

2. Betroffene sowie Zulässigkeit der Verarbeitung und Übermittlung von Daten

Das DSG 2000 schützt die so genannten Betroffenen,[4] wobei dies alle natürlichen und juristischen Personen sowie Personengemeinschaften umfasst, deren personenbezogene Daten im Rahmen des Anwendungsbereichs des DSG 2000 verarbeitet bzw übermittelt werden. Im vorliegenden Fall kommen die Lieferanten und Kunden der einzelnen am Informationsverbund teilnehmenden Gesellschaften mit Sitz in Österreich sowie die Gesellschaften des Konzerns selbst als Betroffene in Betracht.

---

1 Dies trifft insbesondere auf Kredit- und Finanzinstitute zu, die Daten über die Kreditwürdigkeit der Kunden einschließlich Daten aus den Datenbanken des Kreditschutzverbandes und anderer Datenbankanbieter verarbeiten.

2 Hier wird davon ausgegangen, dass das EDV-System von den Unternehmen selbst betrieben wird und die Daten nicht einem externen Dienstleister überlassen werden.

3 Für die Zwecke dieses Beitrags wird ausschließlich von einer Übermittlung innerhalb der Europäischen Union ausgegangen.

4 Das sind „*vom Auftraggeber verschiedene natürliche oder juristische Personen oder Personengemeinschaften, deren Daten verwendet werden*“ (§ 4 Z 3 DSG 2000).

Die Qualifikation als Auftraggeber[5] ist von wesentlicher Bedeutung, da dieser Adressat einer Vielzahl von vom DSG 2000 auferlegten Pflichten ist.[6] Als Auftraggeber iSd DSG 2000 gelten im vorliegenden Fall die am Informationsverbundsystem teilnehmenden Gesellschaften mit Sitz in Österreich, soweit sie Daten für die genannten Zwecke in einem gemeinsamen EDV-System auf die im Folgenden näher beschriebene Art und Weise verarbeiten. Es ist von der Verarbeitung[7] und Übermittlung[8] von Daten iSd DSG 2000 durch diese Gesellschaften auszugehen.[9]

Soweit, wie oben dargelegt, im Rahmen des EDV-Systems Lieferanten- und Kundendaten verarbeitet werden, enthalten diese Angaben über Personen, einschließlich Informationen über deren Identität, sowie weitere Informationen wirtschaftlicher oder finanzieller Natur.

Die Verarbeitung und Übermittlung dieser personenbezogenen Daten iSd § 4 Z 1 DSG 2000 unterliegt umfassenden datenschutzrechtlichen Vorgaben. Es ist zu beachten, dass neben der Zulässigkeit der Datenverarbeitung stets auch der Umfang und die Zulässigkeit der Datenübermittlung zu prüfen sind.[10]

---

5 Auftraggeber sind gemäß § 4 Z 4 DSG 2000 „*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*."

6 Auftraggeber einer Datenanwendung sind insbesondere für die Einhaltung der datenschutzrechtlichen Grundsätze (§ 6 DSG 2000), die Zulässigkeit der Verarbeitung und Übermittlung von Daten (§ 7 DSG 2000), die Wahrung der schutzwürdigen Geheimhaltungsinteressen der Betroffenen (§§ 8 und 9 DSG 2000), die Datensicherheitsmaßnahmen (§ 14 DSG 2000), die Meldepflicht bezüglich der Datenanwendung (§ 17 DSG 2000), die Informations- und Offenlegungspflichten (§§ 24, 25 DSG 2000) und die Auskunfts-, Richtigstellungs- und Löschungspflichten (§ 26 ff DSG 2000) verantwortlich.

7 Dies umfasst das „*Ermitteln, Erfassen, Speichern, Aufbewahren, Ordnen, Vergleichen, Verändern, Verknüpfen, Vervielfältigen, Abfragen, Ausgeben, Benützen, Überlassen, Sperren, Löschen, Vernichten sowie jede andere Art der Handhabung von Daten einer Datenanwendung durch den Auftraggeber oder Dienstleister mit Ausnahme des Übermittelns*" (§ 4 Z 9 DSG 2000).

8 Dies bezeichnet „*die Weitergabe von Daten einer Datenanwendung an andere Empfänger als den Betroffenen, den Auftraggeber oder einen Dienstleister, insbesondere auch das Veröffentlichen solcher Daten*" (§ 4 Z 12 DSG 2000).

9 Es wird auch von einer Übermittlung iSd DSG 2000 gesprochen, wenn Daten auf elektronischem Weg weitergegeben werden. Vgl *Dohr/Pollirer/Weiss*, Datenschutzrecht[2] § 4 Rz 13.

10 Die Zulässigkeit der Verarbeitung personenbezogener Daten ist eine notwendige Voraussetzung für die Zulässigkeit der Übermittlung von Daten, welche nach § 7 Abs 2 DSG 2000 jedoch gesondert zu prüfen ist.

2.1 Verarbeitung von Kunden- und Lieferantendaten

Zulässigkeitsvoraussetzung für die Verarbeitung von Daten[11] ist das Vorliegen einer entsprechenden rechtlichen Befugnis, die den Zweck und den Inhalt des EDV-Systems deckt.[12]

Die Auftraggeber des Informationsverbundsystems können die rechtliche Befugnis zur Verarbeitung von Daten ihrer Kunden regelmäßig aus der Gewerbeberechtigung, der Satzung bzw allfälligen Konzessionen (zB jener eines Kreditinstituts) sowie dem Zweck der Unternehmen und der damit verbundenen Geschäftstätigkeit ableiten. Von einer Befugnis der entsprechenden Gesellschaften zur Verarbeitung der diesbezüglich relevanten personenbezogenen Lieferanten- und Kundendaten ist grundsätzlich auszugehen.

Neben dem Vorliegen einer rechtlichen Befugnis zur Datenverwendung, dürfen durch die Datenverarbeitung keine schutzwürdigen Geheimhaltungsinteressen der Betroffenen verletzt werden. § 8 DSG 2000 enthält eine demonstrative Aufzählung von Tatbeständen, bei denen schutzwürdige Geheimhaltungsinteressen des Betroffenen jedenfalls nicht verletzt werden. Im vorliegenden Fall kommen insbesondere die folgenden zwei Rechtfertigungsgründe in Betracht, auf Grund derer die schutzwürdigen Geheimhaltungsinteressen der Betroffenen durch das beschriebene EDV-System nicht verletzt werden:

– Die Zustimmung der Betroffenen
– Berechtigte Interessen der Auftraggeber oder Dritter.

2.1.1 Zustimmung der Betroffenen

Um diesen Rechtfertigungsgrund für die Datenverarbeitung zur Anwendung zu bringen, ist eine ausdrückliche Zustimmung der Betroffenen zur Verarbeitung ihrer Daten einzuholen.

---

11 Neben der erörterten Verarbeitung der Kunden- und Lieferantendaten ist in der Praxis meist noch die (hier nicht näher behandelte) Zulässigkeit der Übermittlung der Kunden- und Lieferantendaten innerhalb der Konzerngruppe zu prüfen. Dafür ist im Wesentlichen die Glaubhaftmachung einer ausreichenden rechtlichen Befugnis bei gleichzeitiger Wahrung der schutzwürdigen Geheimhaltungsinteressen der Betroffenen (zB Zustimmung der Betroffenen oder Vorliegen überwiegender berechtigter Interessen der Auftraggeber oder Dritter) im Hinblick auf den Übermittlungszweck erforderlich.

12 Der Zweckbindungs- und Wesentlichkeitsgrundsatz (§ 6 Abs 1 Z 2 und 3 DSG 2000) verlangt, dass Daten nur für festgelegte, eindeutige und rechtmäßige Zwecke ermittelt und nicht in einer mit diesen Zwecken unvereinbaren Weise verarbeitet werden sowie für den Zweck der Datenanwendung wesentlich sind bzw über diesen Zweck nicht hinausgehen.

Die Rechtsprechung legt für die Wirksamkeit einer solchen Zustimmung einen sehr strengen Maßstab an. Eine Zustimmungserklärung ist nur dann gültig, wenn

- der Betroffene weiß, welche seiner personenbezogenen Daten zu welchem Zweck verarbeitet werden,
- allfällige Übermittlungsempfänger genau bezeichnet werden[13] und
- der Betroffene auf die Widerrufsmöglichkeit (§ 28 DSG 2000) bezüglich der Zustimmungserklärung ausdrücklich hingewiesen wird.[14]

Wesentlich für die Wirksamkeit einer Zustimmungserklärung ist, dass sich der Betroffene bewusst ist, welche seiner Daten zu welchem Zweck verarbeitet werden. Dabei müssen sowohl die Einrichtungen, die die Daten verwenden sollen, als auch deren Aufgaben bekannt sein.[15]

Bloß allgemein gehaltene AGB-Klauseln reichen für die Wirksamkeit der Zustimmungserklärung jedenfalls nicht aus. Nur eine ausreichend präzise Formulierung der Zustimmung zur Verwendung der betroffenen Daten vermag diesen Anforderungen gerecht zu werden. Zustimmungserklärungen in AGB werden nach der hier strengen Judikatur nur dann rechtsgültig abgegeben, wenn sie deutlich lesbar (idealerweise mittels deutlicher Hervorhebung, wie zB Fettdruck) aus den AGB hervorgehen oder durch zusätzlichen Hinweis im entsprechenden Vertragsdokument explizit auf die AGB aufmerksam gemacht wird.

2.1.2 Berechtigte Interessen der Auftraggeber oder Dritter

Alternativ zu einer Zustimmungserklärung kommen überwiegende berechtigte Interessen der Auftraggeber für die Rechtmäßigkeit der Datenanwendung in Betracht. Schutzwürdige Geheimhaltungsinteressen der Betroffenen werden bei der Verwendung personenbezogener Daten dann nicht verletzt, wenn überwiegende berechtigte Interessen des Auftraggebers oder eines Dritten vorliegen.

Im spezifischen Fall kann die Verarbeitung der für die Geschäftstätigkeit der Auftraggeber erforderlichen Lieferanten- und Kundendaten eine Voraussetzung für die Abwicklung der entsprechenden Verträge darstellen. So ist beispielsweise bei Bankgeschäften unter dem Blickwinkel des berechtigten Interesses des Gläubigerschutzes die Erfassung von Daten

13 OGH 22. 3. 2001, 4 Ob 28/01y.

14 OGH 19. 11. 2002, 4 Ob 179/02 f.

15 OGH 15. 12. 2005, 6 Ob 275/05t; vgl *Thiele*, Bonitätslisten der Banken datenschutzwidrig!, lex:itec 03/06, 29 f.

über die wirtschaftliche Situation der Kunden zur Vertragserfüllung notwendig, da Kreditinstitute die Bonität ihrer Kunden prüfen müssen.[16] Es ist stets im Einzelfall zu prüfen ob ein solches berechtigtes Interesse des Auftraggebers (oder eines Dritten) vorliegt.

3. Informationsverbundsystem

Wie bereits dargelegt bezeichnet man das hier behandelte EDV-System, das die Datenerfassung und -speicherung durch die Gesellschaften der Unternehmensgruppe (jeweils in ihrer Funktion als Auftraggeber) sowie den Zugriff auf und die Bearbeitung der selbst und von den anderen Auftraggebern verarbeiteten Daten ermöglichen soll, als Informationsverbundsystem iSd § 4 Z 13 DSG 2000.

Auf die datenschutzrechtlichen Besonderheiten eines Informationsverbundsystems sei hier kurz eingegangen. Dieses ist dadurch charakterisiert, dass

- Daten in einer Datenanwendung durch mehrere Auftraggeber verarbeitet werden und
- jeder Auftraggeber auf die Daten des jeweils anderen Auftraggebers im EDV-System Zugriff hat.[17]

Ein Informationsverbundsystem darf grundsätzlich erst nach einer Prüfung durch die DSK gemäß § 18 Abs 2 DSG 2000 (Vorabkontrolle) betrieben werden. Bei der Meldung an das DVR ist insbesondere genau auszuführen und zu begründen, warum im konkreten Fall ein Informationsverbundsystem in dieser Form erforderlich ist. Es ist jedenfalls eine differenzierende Beschränkung der Zugriffmöglichkeit geboten und bei der Handhabe des EDV-Systems zu berücksichtigen, da widrigenfalls das Informationsverbundsystem im Widerspruch zu den datenschutzrechtlichen Grundsätzen des § 6 Abs 1 DSG 2000 stünde.

Die DSK hat nach Einreichen der diesbezüglichen Meldung zwei Monate Zeit die Rechtmäßigkeit des Informationsverbundsystems zu prüfen. Sofern die Behörde innerhalb dieser Frist keinen Auftrag zur Verbesserung erteilt,

16 Der OGH hat dies im Zusammenhang mit dem berechtigten Interesse des Gläubigerschutzes bejaht; OGH 15. 12. 2005, 6 Ob 275/05t.

17 Daten in einem Unternehmensnetzwerk, auf die jeder unbeschränkt Zugriff hat, dürften ebenfalls ein Informationsverbundsystem darstellen; vgl *Knyrim*, Datenschutzrecht, 21.

gilt die Meldepflicht als erfüllt und die Datenverarbeitung darf gemäß § 20 Abs 5 DSG 2000 aufgenommen werden.

Die DSK hat hinsichtlich eines Informationsverbundsystems von Banken, das die Warnliste der österreichischen Kreditinstitute zum Zweck des Gläubigerschutzes und der Risikominimierung durch Hinweis auf vertragswidriges Kundenverhalten („Warnliste") betraf, festgehalten, dass hier jedenfalls besondere Vorkehrungen erforderlich sind, um geeignete Garantien für die Richtigkeit der gespeicherten Daten zu gewährleisten.[18] Im konkreten Fall verlangte die DSK, dass der im engen zeitlichen Zusammenhang erfolgte Abschluss einer Tilgungsvereinbarung in der Warnliste anzumerken sei, der Betroffene vom Auftraggeber darüber zu informieren sei, er sich an den Auftraggeber oder den Kreditschutzverband wenden kann, wenn er sein Auskunfts-, Richtigstellungs-, Löschungs- oder Widerspruchsrecht gemäß §§ 26, 27 und 28 DSG 2000 hinsichtlich der „Warnliste" geltend machen will und die Daten jährlich auf deren Richtigkeit zu überprüfen seien. Es ist somit davon auszugehen, dass die Genehmigung des Informationsverbundsystems durch die DSK gegebenenfalls unter Vorschreibung von Auflagen erfolgt, die die Einhaltung der Grundsätze gemäß § 6 DSG 2000 gewährleisten sollen.

Zudem sind bei der Meldung eines Informationsverbundsystems weitere besondere Verpflichtungen zu beachten, die je nach Beurteilung durch die DSK im Einzelfall unterschiedlich ausgestaltet sein können. Solche zusätzlichen Verpflichtungen bei der Ausgestaltung eines Informationsverbundsystems sind beispielsweise:

- Gemäß § 50 Abs 1 DSG 2000 ist ein verantwortlicher Betreiber des Informationsverbundsystems zu bestimmen (das wird idR einer der Auftraggeber sein).[19]
- Gemäß § 14 DSG 2000 ist der Betreiber für die Einhaltung der Datensicherheitsmaßnahmen verantwortlich.
- Gemäß § 24 Abs 2 Z 3 DSG 2000 besteht eine zusätzliche Informationspflicht der Auftraggeber gegenüber den Betroffenen.[20]

18 Bescheide K095.014/016-DSK/2001 und K095.014/021-DSK/2001.

19 *Knyrim*, Datenschutzrecht, 23.

20 Jeder Betroffene ist bei der Ermittlung seiner Daten davon in Kenntnis zu setzen, dass seine Daten in einem Informationsverbundsystem verarbeitet werden. Dies ist idealer Weise bei der Gestaltung der entsprechenden Zustimmungserklärung zu berücksichtigen.

4. Schluss

Abschließend ist festzuhalten, dass das österreichische Datenschutzrecht dem immer größer werdenden Informationsbedarf von Konzernen mit Regelungen begegnet, die eine Einhaltung des Grundsatzes der Verwendung von Daten nach Treu und Glauben gewährleisten sollen. Die Spruchpraxis der zuständigen Behörden und des OGH zeigt deutlich, dass die Einrichtung von Informationsverbundsystemen nur bei Einhaltung entsprechender datenschutzrechtlicher Vorkehrungen zulässig ist. In der Zukunft ist hier jedenfalls mit steigernder Bedeutung des Rechtsinstituts Informationsverbundsystem zu rechnen.