Datenschutzrechtliche Melde-prozesse und die Einführung von DVR-Online

Mit der Einführung von „DVR-Online" soll im Jahr 2012[1] ein System zur Verfügung stehen, das es jedermann ermöglicht, kostenlos über die Webseite der Datenschutzkommission das Datenverarbeitungsregister abzufragen und die nach Datenschutzgesetz vorgeschriebenen Meldungen an die Datenschutzkommission zu erstatten.[2] Dieser Artikel nimmt die geplante Einführung von „DVR-Online" zum Anlass, die Meldepflichten von Unternehmen nach dem Datenschutzgesetz zu beleuchten und „DVR-Online" kurz vorzustellen.

Von Rainer Knyrim | Gerold Pawelka

Datenschutz in Österreich

Das Datenschutzgesetz versteht unter „personenbezogenen Daten" Daten von natürlichen oder juristischen Personen, deren Identität bestimmt oder bestimmbar ist. Wie oftmals fälschlicherweise angenommen wird, umfassen personenbezogene Daten daher nicht nur persönliche Daten des allgemeinen Sprachgebrauchs wie etwa Name, Geburtsdatum und Schuhgröße, sondern alle Daten, die mit einer bestimmten Person in Verbindung gebracht werden können. Daten dürfen nur dann verwendet werden, wenn eine der diesbezüglichen gesetzlichen Ausnahmeregelungen anwendbar ist. So ist beispielsweise die Verwendung personenbezogener Daten mit Zustimmung oder bei Lebensgefahr des Betroffenen zulässig. Weiters zulässig ist aber auch – und das ist wohl für Unternehmen die wichtigste Ausnahme – die Verwendung personenbezogener Daten bei überwiegenden berechtigten Interessen Anderer. Gesetzliche Ausnahmen finden sich aber nicht nur im Datenschutzgesetz. Beispielsweise enthalten auch das Unternehmensgesetzbuch (UGB) und die Bundesabgabenordnung (BAO) Bestimmungen, die bestimmte Aufbewahrungspflichten – auch für personenbezogene Daten – normieren. Gerne übersehen wird, dass personenbezogene Daten, deren Verarbeitung an sich zulässig war, nicht beliebig lange verwendet werden dürfen. Ist der legitime Zweck der Datenverwendung erfüllt worden oder ist die gesetzliche Verpflichtung zur Datenspeicherung weggefallen, sind die personenbezogenen Daten umgehend zu löschen oder zu anonymisieren. Die vorgenannten Regelungen beziehen sich auf das materielle Datenschutzrecht. Parallel zu diesem sind die formellen Pflichten des Datenschutzrechts zu beachten, insbesondere die Meldepflicht beim Datenverarbeitungsregister.

Meldepflichten

Die Kontrolle der Einhaltung der datenschutzrechtlichen Bestimmungen obliegt der Datenschutzkommission.[3] Um die Zulässigkeit von Datenverwendungen sicherzustellen, hat sich derjenige Auftraggeber, der sich entschieden hat, personenbezogene Daten zu verwenden, *vor Inbetriebnahme* der Datenanwendung bei der Datenschutzkommission zu melden (AG-Meldung). Gleichzeitig hat er bei der Datenschutzkommission eine Meldung der von ihm betriebenen Datenanwendungen in Form einer Datenanwendungsmeldung beim Datenverarbeitungsregister (DVR-Meldung) zu erstatten.

Zu beachten ist, dass der Begriff der Datenanwendung im datenschutzrechtlichen Sinne nicht mit dem Begriff der Softwareapplikation gleichzusetzen ist. Eine Datenanwendung ist nach Art 2 § 4 Z 7 DSG 2000 die Summe der in ihrem Ablauf logisch verbundenen Verwendungsschritte, die zur Erreichung eines inhaltlich bestimmten Ergebnisses (des Zweckes der Datenanwendung) geordnet sind und zur Gänze oder auch nur teilweise automationsunterstützt, also maschinell und programmgesteuert, erfolgen. Datenanwendungen sind somit konkrete Arbeitsabläufe, die für die Erreichung bestimmter Ziele notwendig sind. Eine Datenanwendung kann daher neben (einer oder mehreren) Softwareapplikationen (oder Teilen von solchen) beispielsweise auch handschriftliche Notizen, Tabellen einer Tabellenkalkulation oder Ausdrucke umfassen. Datenanwendungen ohne automationsunterstütze Komponenten werden als manuelle Datenanwendungen ebenfalls vom DSG 2000 geschützt.[4] Sie unterliegen auf Grund ihrer untergeordneten Bedeutung lediglich einer eingeschränkten Meldepflicht[5] und werden daher im Folgenden nicht weiter behandelt.

Die DVR-Meldung hat die vom Auftraggeber verwendeten personenbezogenen Daten, deren jeweils zugeordneten betroffenen Personenkreis sowie all jene vom Auftraggeber verschiedene Personen, welche diese Daten ebenfalls mit Eigeninteresse nutzen (Übermittlungsempfänger) zu enthalten. Zusätzlich hat der Auftraggeber Angaben zu den von ihm ergriffenen Maßnahmen zu machen, welche die Sicherheit der Daten gewährleisten sollen (Datensicherheitsmaßnahmen). Insbesondere bei größeren, automationsunterstützten Datenanwendungen kann die Ermittlung der verarbeiteten personenbezogenen Daten sehr aufwändig sein. Werden die Daten mittels Datenbank oder strukturiert in Computerdateien gespeichert, können für die DVR-Meldung – sofern verfügbar – die Datenbankdefinitionen der Softwareent-

wickler herangezogen werden. Auch die einzelnen Eingabemasken der Datenanwendungen sind eine gute Grundlage für die Ermittlung der einzelnen Datenfelder. Die Meldung selbst erfolgt derzeit noch mittels Formularen,[6] die per Post, Telefax oder E-Mail an die Datenschutzkommission übermittelt werden können. Der Gesetzgeber hatte geplant, dass spätestens ab 1. Jänner 2012 die Meldungen mittels „DVR-Online" eingebracht werden müssen, dieser Stichtag soll nun kurzfristig auf 1. September verschoben werden.[7]

Daten über die rassische und ethnische Herkunft, politische Meinung, Gewerkschaftszugehörigkeit, religiöse oder philosophische Überzeugung, Gesundheit, das Sexualleben von Betroffenen, strafrechtliche Daten oder Daten über die Kreditwürdigkeit greifen besonders tief in den Persönlichkeitsbereich des Betroffenen ein, weshalb deren Verwendung besonders geschützt ist. Datenanwendungen, die diese Daten verwenden, müssen *vor ihrer Inbetriebnahme* von der Datenschutzkommission genehmigt werden, dh diese Datenanwendungen sind „vorabkontrollpflichtig".[8]

Nationale und internationale Datenübermittlungen

Auch die Übermittlung von Daten an Dritte, dh an Personen, die von Auftraggeber und Betroffenem verschieden sind, sieht der Gesetzgeber als datenschutzrechtlich bedenklich an. In der DVR-Meldung sind daher die einzelnen Datenübermittlungen anzuführen, deren Zulässigkeit die Datenschutzkommission gesondert prüft.[9] Als besonders kritisch werden grundsätzlich Datenübermittlungen in das Ausland gesehen, da das Datenschutzniveau im Empfängerland geringer als in Österreich sein könnte. Datenübermittlungen in das Ausland sind daher grundsätzlich durch die Datenschutzkommission *vorab zu genehmigen.*[10] Von der Vorabgenehmigungspflicht sind Datenübermittlungen an Empfänger in Vertragsstaaten des Europäischen Wirtschaftsraumes und in Länder, in denen ein angemessener Datenschutz besteht, allerdings ausgenommen. In welchen Ländern angemessener Datenschutz besteht, wird durch Verordnung des Bundeskanzlers oder der EU-Kommission festgelegt, derzeit sind dies ua die Schweiz, Kanada, Argentinien, Jersey und Guernsey. Hinsichtlich US-Unternehmen gibt es eine Sonderregelung, diese können sich selbst zur Einhaltung sogenannter „Safe Harbor"-Bestimmungen verpflichten[11] und gelten dann bezüglich des Datenschutzniveaus mit der EU gleichgestellt.[12]

Zu beachten ist, dass im österreichischen Datenschutzrecht Datenübermittlungen zwischen einzelnen Konzernunternehmen denselben materiellen Voraussetzungen und formellen Meldepflichten unterliegen wie Datenübermittlungen an konzernexterne Dritte. Ein „Konzernprivileg" in dem Sinne, dass gesellschaftsrechtlich verflochtene Gesellschaften datenschutzrechtlich „eins" sind, gibt es *nicht.* In der Praxis stellen Datenübermittlungen bei multinationalen Konzernen daher ein großes datenschutzrechtliches Problem dar. Teambildungen erfolgen in diesen Unternehmen oftmals projektbezogen über nationale Unternehmensgrenzen hinweg, Vorgesetzte von Mitarbeitern nationaler Konzernunternehmen finden sich vermehrt in ausländischen Konzernunternehmen. Dadurch entsteht eine Vielzahl internationaler Datenströme, die von der Datenschutzkommission vorab zu genehmigen sind. Insbesondere bei internationalen Datenübermittlungen innerhalb einer Matrixorganisation,[13] ist mit einer besonders genauen Prüfung durch die Datenschutzkommission zu rechnen.

Standard- und Musteranwendungen

In der Praxis hat sich gezeigt, dass bestimmte Arten von Datenanwendungen in Unternehmen besonders häufig verwendet werden. So werden beispielsweise in den meisten Unternehmen Kunden- und Lieferantendaten verwaltet. Um die Meldungsflut von – wohl unbedenklichen – Datenanwendungen zu reduzieren, wurde im Datenschutzgesetz die Möglichkeit geschaffen, bestimmte Datenanwendungen im Verordnungsweg als Standardanwendungen bzw Musteranwendungen zu definieren.[14] Datenanwendungen, die nicht über den Inhalt einer Standardanwendung hinausgehen, müssen bei der Datenschutzkommission nicht gemeldet werden. Bereits ein einziges Datum, das nicht in der jeweiligen Standardanwendung enthalten ist, bedingt die Meldepflicht der gesamten Datenanwendung. Musteranwendungen unterliegen einem vereinfachten Meldungsvorgang, es muss nur das Vorliegen der Musteranwendung, nicht jedoch deren genauer Inhalt gemeldet werden.[15] Zu beachten ist, dass in den Standard- und Musteranwendungen auch die zulässigen Übermittlungsempfänger festgelegt werden. Werden in der Datenanwendung Daten an andere Empfänger übermittelt, ist die gesamte Datenanwendung zu melden.

Informationsverbundsysteme

Ein Informationsverbundsystem liegt vor, wenn mehrere Auftraggeber Daten in ein gemeinsames System einspeisen und jeder der Auftraggeber auf die Daten der jeweils anderen Auftraggeber Zugriff hat. Klassische Informationsverbundsysteme sind zB die „Warnliste" der Banken. Informationsverbundsysteme werden als datenschutzrechtlich bedenklich angesehen und unterliegen daher ebenfalls einer Vorabkontrollpflicht durch die Datenschutzkommission.[16]

Videoüberwachungssysteme

Die Verwendung von Videoüberwachungssystemen, dh von Systemen, die der systematischen Überwachung von Objekten oder Personen durch technische Bildaufnahme- oder Bildübertragungsgeräte dienen, ist ebenfalls der Datenschutzkommission zu melden,[17] sie ist grundsätzlich vorabkontrollpflichtig. Eine Videoüberwachungsanlage darf daher erst nach erfolgter Genehmigung durch die Datenschutzkommission in Betrieb genommen werden. Von der Meldepflicht ausgenommen sind Echtzeitüberwachungssysteme die keine Aufzeichnungen durchführen sowie analoge Videoüberwachungssysteme.

DVR-Online

Auftraggeber, Datenanwendungen, Informationssysteme und Videoüberwachungssysteme sollen in Zukunft über die Webseite der Datenschutzkommis-

sion registriert werden können. Ebenso soll der Registerstand geändert und abgefragt werden können. Die hierfür notwendigen Voraussetzungen sollten bis längstens 1. Jänner 2012 geschaffen sein, dieser Termin wird vom Gesetzgeber voraussichtlich kurzfristig auf 1. September 2012 verschoben werden.[18] Mit der Einführung des Systems „DVR-Online" stehen diese Möglichkeiten in Kürze jedermann weltweit kostenlos über Internet zur Verfügung.

Die Benutzeroberfläche von „DVR-Online" soll den bisherigen Meldeformularen angelehnt werden. Personen, die bereits mit den Meldeformularen zu tun hatten, sollten sich daher im neuen System schnell zurechtfinden. Das DSG sieht vor, dass nicht vorabkontrollpflichtige DVR-Meldungen automatisch mittels Stichwortlisten auf ihre Plausibilität und datenschutzrechtliche Unbedenklichkeit überprüft werden sollen. DVR-Meldungen, die diese Prüfung bestehen, sollen automatisch registriert werden. Durch dieses System ist mit einer Entlastung des Arbeitsaufkommens der Datenschutzkommission und einer schnelleren Abwicklung der Registrierungsprozesse zu rechnen.

Die Praxis hat gezeigt, dass viele Unternehmen ihrer Pflicht zur Erstmeldung der von ihnen betriebenen Datenanwendungen nicht nachkommen. Von vielen Unternehmen, die gemeldet haben, wird weiters übersehen, dass Auftraggeber aber auch verpflichtet sind, ihre Datenanwendungsmeldungen aktuell zu halten.[19] Verwaltungsrechtlich war die Verletzung der Aktualisierungspflicht schon bisher nach Art 2 § 52 Abs 2 Z 1 DSG 2000 strafbar, durch mangelnde Online-Recherchemöglichkeiten und eine Überlastung des Datenverarbeitungsregisters mussten Unternehmen die Entdeckung und Bestrafung ihrer Pflichtverletzung aber bisher kaum befürchten.

Die Einführung der Online-Abfrage des Registerstandes erhöht das Risiko einer Entdeckung veralteter Registerstände stark, da diese mittels „DVR-Online" für jedermann – also auch für Konkurrenten, Mitarbeiter, ehemalige Mitarbeiter, Betriebsräte etc – ohne nennenswerten Aufwand in Echtzeit sichtbar gemacht werden können. Die Praxis der anwaltlichen Beratung zeigt, dass Datenanwendungsmeldungen zahlreicher – auch großer und bekannter – Unternehmen zum Teil Jahrzehnte (!) alt sind.

Verstöße gegen die Meldepflichten können für Auftraggeber empfindliche Folgen haben. Sie werden nach Art 2 § 52 Abs 2 Z 1 DSG 2000 mit einer Geldstrafe in der Höhe von bis zu 10.000 Euro geahndet, zusätzlich kann der „Verfall" von Datenträgern und Programmen ausgesprochen werden, dh diese könnten von der Behörde eingezogen werden. Denkbar sind auch Unterlassungs- und Schadenersatzklagen durch konkurrierende Unternehmen nach § 1 Abs 1 UWG. Nicht zu unterschätzen ist auch die negative Öffentlichkeitswirksamkeit von Verstößen gegen das Datenschutzrecht.

Nationale und internationale Datenskandale der letzten Monate (mehrfacher Diebstahl von Kundendaten bei Sony,[20] im Internet veröffentlichte Patientendaten der Tiroler Gebietskrankenkasse,[21] „GIS-Hack" etc) haben die Öffentlichkeit für das Thema Datenschutz besonders sensibilisiert. Die betrieblichen Compliance-Verantwortlichen sollten daher noch tunlichst vor Einführung von „DVR-Online" die Einhaltung der formellen Meldepflichten beim DVR auf ihre Agenda setzen und die betrieblichen Datenanwendungen auf deren notwendige Registrierung und bereits gemeldete Datenanwendungen auf die Aktualität der Meldung hin prüfen.

1) Ursprünglich für Jänner 2012 geplant, sieht das Budgetbegleitgesetz 2012 (RV 1494 BlgNr, 24. GP 19) eine Verschiebung der Einführung von DVR-Online bis längstens September 2012 vor. Da das Budgetbegleitgesetz 2012 zum Zeitpunkt der Drucklegung noch nicht beschlossen worden war, kann sich dieser Einführungszeitpunkt noch ändern.
2) *Knyrim*, Datenschutzrecht (2003) 26.
3) Art 2 § 30 DSG 2000.
4) Art 2 § 58 DSG 2000.
5) Art 2 § 17 Abs 1 letzter Satz DSG 2000 sowie Art 2 § 58 DSG 2000.
6) Zu finden unter https://www.dsk.gv.at/site/6296/default.aspx, abgerufen am 14.10.2011.
7) Eine detaillierte Ausfüllhilfe zu den Meldeformularen enthält *Knyrim* Datenschutzrecht (2003) 50 ff.
8) Art 2 Abs 4 Z 2 DSG 2000 und Art 2 § 18 Abs 2 DSG 2000.
9) Art 2 § 7 Abs 2 DSG 2000.
10) Art 2 § 13 Abs 1 DSG 2000.
11) Eine Liste jener Unternehmen, die sich den „Safe-Harbor"-Bestimmungen unterworfen haben findet sich unter http://www.export.gov/safeharbor.
12) ABL L 215 v 25.8.2000; *Oberhofer* in *Bauer/Reimer* (Hsg) Handbuch Datenschutzrecht (2009) 499.
13) Http://de.wikipedia.org/wiki/Matrixorganisation, abgerufen am 14.10.2011.
14) Eine Auflistung der aktuellen Standard- und Musteranwendungen findet sich in der Standard- und Musterverordnung 2004 Anlagen 1 und 2.
15) Für weiterführende Informationen siehe *Knyrim* Datenschutzrecht (2003) 45 ff.
16) Art 2 § 18 Abs 2 Z 4 DSG 2000.
17) Art 2 § 50a ff DSG 2000.
18) Art 2 § 17 Abs 1a DSG 2000 iVm Art 2 § 61 Abs 8 DSG 2000 idF RV 1494 BlgNr, 24. GP 19.
19) Art 2 § 17 Abs 1 2. Satz DSG 2000.
20) Http://diepresse.com/home/techscience/internet/sicherheit/700341/Sony_Hacker-knacken-wieder-93000-NutzerKonten, abgerufen am 14.10.2011.
21) Http://diepresse.com/home/techscience/internet/sicherheit/696658/Anonymous_Haben-600475-Tiroler-Krankenkassendaten, abgerufen am 14.10.2011.

Foto Preslmayr

Foto privat

Die Autoren

RA Dr. Rainer Knyrim (links) ist Partner bei Preslmayr Rechtsanwälte, wo er ständig in- und ausländische Mandanten im Datenschutzrecht berät. Er ist Autor des „Praxishandbuch Datenschutzrecht" und Mitherausgeber des größten österreichischen Datenschutz-Kommentars. Dr. Knyrim ist Mitglied der „Task Force on Privacy and the Protection of Personal Data" der Internationalen Handelskammer (ICC) Paris sowie wissenschaftlicher Beirat der Zeitschrift jusIT und Mitglied des Programmkomitees des Österreichischen IT-Rechtstages.

Mag. Gerold Pawelka, CMC (rechts) ist Rechtsanwaltsanwärter bei Preslmayr Rechtsanwälte OG. Er war zuvor über zehn Jahre als IT-Berater tätig.