RFID-Chips und Datenschutz

RdW 2005/ S. 2

Als Nachfolger der Strichcodes zur Kennzeichnung von Waren sind RFID-Chips immer häufiger in den Medien zu finden. Im Gegensatz zu den Strichcodes können diese Chips kontaktlos, und somit ohne Wissen und Willen des Trägers, über Funk ausgelesen werden. Die verschiedenen Einsatzmöglichkeiten haben bereits zu Warnungen von Datenschützern rund um den Globus geführt.

RA Dr. Rainer Knyrim
RAA Mag. Viktoria Haidinger, LL.M.
Wien

1. Einleitung

Fast unbemerkt von der Weltöffentlichkeit sind RFID-Chips (Radio Frequency Identity Chips), auch RFID-Tags genannt, in bestimmte Wirtschaftsbereiche vorgedrungen. Allen voran erwartet sich die Logistikbranche enorme Einsparungen durch elektronische Überwindung des sog Medienbruchs[1]). Aber erst in jüngster Zeit macht diese – wenn auch nicht mehr ganz so neue[2]) – Technologie vermehrt Schlagzeilen, nämlich immer dann, wenn der Zweck des Einsatzes über die bloße Kennzeichnung von Waren und Gütern hinausgeht und in den Privatbereich der Kunden eindringt[3]). Die Anwendungsmöglichkeiten sind sehr vielfältig und reichen vom bereits erwähnten, vernünftigen Einsatz der Chips im Logistikbereich bis zu „Horrorszenarien" totaler Überwachung.

Vorab sei darauf hingewiesen, dass der Chip selbst ein bloßer Datenspeicher ist. Das Besondere ist jedoch, dass durch die Möglichkeit des kontaktlosen Auslesens der Träger jederzeit mit einem Lesegerät identifiziert werden kann (geht man davon aus, dass die Daten unverschlüsselt auf dem Chip gespeichert sind). Wenn auch in vielen Fällen nicht der Name einer Person gespeichert wird, sondern lediglich eine Nummer, so könnte man doch einer Person eine große Menge Daten zuordnen, mag diese dem „Ausleser" namentlich auch unbekannt sein[4]). Sind die Daten anonym, stellen sich zwar keine datenschutzrechtlichen Probleme, wohl aber persönlichkeitsrechtliche, wenn nicht sogar vermögensrechtliche[5]).

2. Technische Grundlagen

Radio Frequency Identification (RFID, englisch für „Identifizierung per Funk") ist eine Methode, um kontaktlos Daten lesen und speichern zu können. Das System wurde ursprünglich entwickelt, um die Identifikation von Objekten mittels der „Strichcodes" zu ersetzen. Die Daten werden auf sog RFID-Tags – technisch gesehen handelt es sich um Transponder – gespeichert. Die gespeicherten Daten werden über elektromagnetische Wellen ausgelesen. Bei niedrigen Frequenzen geschieht dies induktiv, bei höheren über Funk. Die Entfernung, über die ein Tag ausgelesen werden kann, schwankt aufgrund der Ausführung (aktiv/passiv) je nach benutzem Frequenzband, Sendestärke und Umwelteinflüssen zwischen wenigen Zentimetern und maximal 30 Metern. Aktive Tags sind batteriebetrieben und können typischerweise sowohl gelesen als auch beschrieben werden. Sie senden idR nur dann Informationen aus, wenn sie ein spezielles Aktivierungssignal empfangen. Der interne Speicher kann je nach Modell bis zu einer Million Bytes aufnehmen. Passive Tags hingegen beziehen ihre Energie zur Übertragung der Informationen aus den empfangenen Funkwellen. Gespeicherte Daten können meist nur ausgelesen werden und die Menge der speicherbaren Daten ist wesentlich geringer als bei aktiven Tags. Dieser Speicher wird üblicherweise benutzt, um eine eindeutige Identifikationsnummer zu hinterlegen. Sehr gut funktioniert das massenweise Einlesen vieler Chips (sog bulk mode) auf einmal, sodass zB in einem Kaufhaus bei „item tagging" Hunderte Artikel auf einmal an der Kasse eingelesen werden können.

Ein technisches Problem ist derzeit, dass der Großteil der Chips auf UHF funktioniert, einem Frequenzband, das bei Nässe und Metall schlecht bis überhaupt nicht funktioniert, was im Ergebnis heißt, dass eine Vielzahl an Produkten mit RFID-Etiketten derzeit noch gar nicht gekennzeichnet werden kann (zB Getränkedosen). Auch sind die Kosten der Chips derzeit noch zu hoch, um tatsächlich weit verbreitetes item tagging zu betreiben. Es gibt daher Projekte, die sich auf Branchen übergreifendes „unit tagging" mit wiederverwertbaren Chips konzentrieren, zB die Kennzeichnung von Paletten[6]).

3. Anwendungsmöglichkeiten

Die RFID-Technologie ist keine Utopie mehr. Die Stadt Wien schreibt seit Anfang 2004 die Implantierung von RFID-Chips zur Identifizierung von Hunden unter deren Haut vor[7]) und nützt die Technik in der neuen Hauptbibliothek zur Bücherausleihe[8]). Art 4 Abs 1 lit b der VeterinärVO[9]) schreibt Haltern von Hunden, Katzen und Frettchen ab 2011[10]) österreichweit die Kennzeichnung ihrer Tiere durch einen elektronischen Transponder zwingend vor,

1) Beim normalen Einscannen des Barcodes wird der Medienbruch Papier – Datenträger durch menschliche Intervention überwunden.

2) Vorläufer der RFID-Technologie werden bereits seit den 60er Jahren zur Diebstahlsicherung eingesetzt, seit den 80er Jahren werden sie in manchen Staaten für Mautsysteme verwendet. Vgl hierzu: Wikipedia, RFID, de.wikipedia.org/wiki/rfid. Die RFID-Technologie ist schon länger bekannt, bislang fehlten aber die notwendigen Hardware- und Software-Ressourcen, um sie gewinnbringend einzusetzen.

3) Je nach Anwendung können sich hier aber auch im Logistikbereich datenschutzrechtliche Probleme, insb mit arbeitsrechtlichem Hintergrund Natur stellen, so wenn Daten der Mitarbeiter in einer Weise gespeichert werden, die eine (lückenlose) Überwachung erlauben (§ 96 Abs 1 Z 3 und 4, § 96a Abs 1 ArbVG).

4) Die Nummer ist somit eine Art Pseudonym. Tritt man im Internet, vor allem in Foren und Chat-Rooms, mit Nick-Names auf, hat man die gleiche Situation. Es handelt sich hierbei im Ergebnis um indirekt personenbezogene Daten, da zwar der Verwender die Daten nicht zuordnen kann, aber eine andere Person, zB der Host-Provider.

5) Nachstehendes Fallbeispiel 3 soll dies zeigen.

6) Logistiker nennen dies „collaborative supply chain management".

7) § 13d Wiener Tierschutz- und Tierhaltegesetz idF Wr LGBl 2004/5.

8) Golem.de v 8. 4. 2004, Bibliothek zum Selbstausleihen: 300.000 Funkchips in Büchern, www.golem.de/0304/24912.html.

9) Verordnung (EG) Nr 998/2003 des Europäischen Parlaments und des Rates vom 26. 5. 2003 für die Verbringung von Heimtieren zu andere als Handelszwecken und zur Änderung der RL 92/65/EWG (ABl L 146, 13. 6. 2003, 1).

10) Es gilt eine Übergangsfrist von acht Jahren ab In-Kraft-Treten, sohin 20 Tage nach ihrer Veröffentlichung im ABl.

wenn diese auf Reisen gehen. Der „Baja Beach Club“[11]) in Barcelona bietet seinen „VIPs“ gänzlich unbelastetes Tanzvergnügen: Jeder kann sich einen RFID-Chip mit Identifikationsnummer und Kreditkartenfunktion unter die Oberarmhaut implantieren lassen und braucht so nur mehr mit diesem am Lesegerät vorbeizugehen, um Zutritt zu dem Club zu erhalten oder ein Getränk zu bezahlen[12]). Vergangenes Jahr wurde RFID-Technologie für die Kennzeichnung von SARS-Patienten in Spitälern in Singapur verwendet[13]). Metro Deutschland versuchte mit seinem Future Store[14]) der Öffentlichkeit das rasche und bequeme „Einlesen“ eines ganzen Einkaufswagens durch bloßes Vorbeifahren an einer RFID-Kasse schmackhaft zu machen, kam jedoch in die Schlagzeilen, weil Kundenkarten mit RFID-Chips ausgegeben wurden, ohne dies den Kunden mitzuteilen[15]). Wal-Mart, die größte US-Supermarktkette, hat ihr RFID-Projekt mit acht Lieferanten gestartet, deren Güter nunmehr vom Lager bis zum Supermarkt elektronisch verfolgbar sind. Eine Ausweitung auf 100 Lieferanten soll zu Jahresanfang 2005 erreicht werden. Ausgestattet werden bei Wal-Mart anfangs nur die Paletten, später soll jede Verpackung gekennzeichnet werden, sodass eine Verfolgung bis in das Regal des einzelnen Marktes möglich ist[16]).

Holland testet bereits Pässe, die mit einem RFID-Chip versehen sind, auf denen biometrische Daten gespeichert werden sollen[17]). Künftig könnten die Chips zB auch in anderen amtlichen Dokumenten[18]), Kfz-Kennzeichen[19]), ja sogar Banknoten zum Einsatz kommen.

Bei der Fußball-WM 2006 in Deutschland will man mit den Chips nicht nur Kartenverkauf und Zugangskontrolle in den Stadien vereinfachen, sondern damit auch gleichzeitig bekannte Gewalttäter bereits vom Erwerb ausschließen (Anonymität wird durch das Bezahlen mittels Kreditkarte ausgeschlossen)[20]). Bei den großen österreichischen Laufveranstaltungen werden die Läufer seit 1997 mittels RFID-Chips, die an den Schuhbändern befestigt werden, gemessen[21]). Im Bereich des Lebensmittelrechts der EU werden die Chips ebenfalls bald zum Einsatz kommen[22]).

Was sind nun die konkreten „Gefahren“, die von diesen Chips ausgehen? In erster Linie – wie bereits erwähnt – die grundsätzliche Möglichkeit, die Daten der Chips ohne Wissen und Willen des Trägers auszulesen. Häufig wird es für den Kunden auch schwierig sein herauszufinden, ob ein Produkt mit einem Chip versehen ist oder nicht. Durch die Zuweisung einer eindeutigen Identifikationsnummer und der Ausstattung bestimmter Areale mit Lesegeräten kann man sehr einfach Bewegungsprofile erstellen. Technisch ist es derzeit noch nicht möglich, mit sog RFID-Blocker-Tags die Kommunikation zwischen Chip und Lesegerät verlässlich zu unterbinden, und es wird überdies kritisiert, dass damit dem jeweiligen Betroffenen der Schutz seiner Privatsphäre überwälzt wird, obwohl er die RFID-Chips vielleicht gar nicht auf seinem Produkt wollte[23]). Der Verein für Internet-Benutzer Österreichs (VIBE)[24]) zeigt auf, dass das Entfernen der Etiketten beispielsweise am Ausgang eines Warenhauses eine bewusste Anstrengung auf Seiten der Konsumenten erfordert und daher viele davon keinen Gebrauch machen würden, sei es aus Furcht, Unwissenheit oder Zeitmangel. Dies würde zu zwei Klassen von Konsumenten führen: jene, die sich um den Schutz ihrer Privatsphäre ausreichend kümmern und die RFID-Etiketten in ihren Waren zerstören, und jene, die dies nicht tun[25]). Verlässlich zerstört werden können die Chips durch Mikrowellen. Allerdings ist diese Methode nachteilig, wenn der Chip nicht zuvor vom betreffenden Artikel entfernt wurde, weil der Chip mit einer Stichflamme in der Mikrowelle verglüht, was den meisten Produkten wohl abträglich sein würde[26]).

4. Zulässigkeit der Datenverwendung[27])

4.1 Datenschutz als Grundrecht

§ 1 Abs 1[28]) gewährt jedem das verfassungsgesetzlich gewährleistete Recht auf Geheimhaltung der ihn betreffenden personenbezogenen Daten[29]) gegenüber jedermann (Drittwirkung), soweit ein schutzwürdiges Interesse daran besteht.

11) Eine „in“-Diskothek, www.bajabeach.es.

12) S auch bei *Alex Jones*, Prisonplanet, Baja Beach Club in Barcelona, Spain Launches Microchip Implantation for VIP Members, www.prisonplanet.com/articles/april2004/040704bajabeachclub.htm; orf futurezone v 13. 5. 2004, Party mit implantierten Funkchips, http://futurezone.orf.at/futurezone.orf?read=detail&id=230631&tmp=54154.

13) RFID-Journal v 4. 5. 2003, Singapore Fights SARS with RFID, http://www.rfidjournal.com/article/articleview/446/1/1/. Auf der Homepage des RFID Journals finden sich auch jede Menge weiterer realisierter RFID-Projekte.

14) www.future-store.org.

15) Vgl die umfangreiche Berichterstattung bei FoeBuD: FoeBuD deckt auf: Versteckte RFID in Metro-Payback-Kundenkarte, www.foebud.org/texte/aktion/rfid/.

16) orf futurezone v 1. 5. 2004, Wal-Mart startet mit Funkchips, futurezone.orf.at/futurezone.orf?read=detail&id=229911&tmp=87561.

17) heise online v 2. 7. 2004, Holland testet Biometrie im Pass, http://www.heise.de/newsticker/meldung/48809; *Schulzki-Haddouti*, Elektronischer Pass – Biometrische Reisepässe mit RFID-Chips in der Einführungsphase, c't 9/2004, 52, auszugsweise im Internet veröffentlicht unter: www.heise.de/ct/04/09/052/.

18) Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein, Biometrie in offiziellen Ausweisen: Rechtliche Rahmenbedingungen, www.datenschutzzentrum.de/material/themen/divers/biometrie_ausweis.htm.

19) orf futurezone v 12. 6. 2004, Mit GPS und Funkchips gegen Autodiebe,futurezone.orf.at/futurezone.orf?read=detail&id=233450&tmp=3707.

20) heise online v 15. 1. 2004, Fußball-WM 2006: Nur mit RFID ins Stadion, www.heise.de/newsticker/meldung/43645; heise online v 24. 4. 2004, RFID-Umfrage: Fußball-WM 2006 soll den Durchbruch bringen, www.heise.de/newsticker/meldung/46724.

21) S www.pentek-timing.at, wo zu den verschiedenen Veranstaltungen die Ergebnisse mit Namen der Läufer (inklusive Namenssuchfunktion) veröffentlicht werden, wobei deren Zustimmung dafür bedenklicherweise nicht eingeholt wird.

22) Vgl den laut Art 65 mit 1. 1. 2005 in Kraft tretenden Art 18 (Rückverfolgbarkeit von Lebensmitteln und Futtermitteln) der Verordnung (EG) Nr 178/2002 des Europäischen Parlaments und des Rates vom 28. 1. 2002 zur Festlegung der allgemeinen Grundsätze und Anforderungen des Lebensmittelrechts, zur Errichtung der Europäischen Behörde für Lebensmittelsicherheit und zur Festlegung von Verfahren zur Lebensmittelsicherheit (ABl L 31, 1. 2. 2002, 1). Siemens ist schon darauf vorbereitet: Wettbewerbsvorteile durch EU-Verordnung 178/2002, www.ad.siemens.de/beverage/html_00/news/letter_031_03.htm.

23) FoeBuD e.V., Was sind RFID Blocker Tags? Sollte ich mir so was besorgen?, www.foebud.org/texte/Aktion/rfid/blocker_tags/index.html.

24) www.vibe.at.

25) vibe!at, Positionspapier über den Gebrauch von RFID auf und in Konsumgütern, www.vibe.at/begriffe/rfid.html.

26) FoeBuD deckt auf: Versteckte RFID in Metro-Payback-Kundenkarte, www.foebud.org/texte/aktion/rfid/.

27) Ein detailliertes Prüfungsschema findet sich bei *Knyrim*, Datenschutzrecht (2003) 81. Ein etwas kürzeres, vor allem im Hinblick auf die Übermittlung von Daten, bei *Knyrim*, Zulässigkeit eines internationalen Datenverkehrs nach DSG 200, ecolex 2002, 470.

28) Paragrafenangaben ohne Gesetzesbezeichnung beziehen sich auf das DSG 2000.

29) Unter personenbezogenen Daten sind laut § 4 Z 1 Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist, ist zu verstehen.

Ausgeschlossen ist ein solcher Geheimhaltungsanspruch, wenn die Daten veröffentlicht wurden oder anonym sind. § 1 Abs 2 normiert einen materiellen Gesetzesvorbehalt, nach dem Eingriffe in das Grundrecht nur in folgenden Fällen erlaubt sind: Die Datenverwendung liegt im lebenswichtigen Interesse des Betroffenen, sie erfolgt mit seiner Zustimmung oder ist zur Wahrung überwiegender berechtigter Interessen eines anderen notwendig. Staatliche Eingriffe dürfen nur aufgrund einer gesetzlichen Grundlage erfolgen und müssen zur Verwirklichung eines in Art 8 Abs 2 der EMRK aufgezählten öffentlichen Interesses notwendig sein. Die Verwendung personenbezogener Daten, sei es durch Behörden oder Private, ist daher grundsätzlich unzulässig, sofern sie sich nicht auf einen Ermächtigungstatbestand stützen kann.

Gleichfalls im Verfassungsrang stehen die Betroffenenrechte nach § 1 Abs 3, nämlich das Auskunftsrecht über verarbeitete Daten sowie das Recht auf Richtigstellung und Löschung unrichtiger bzw unzulässigerweise verarbeiteter Daten.

4.2 Gesetzlicher Rahmen für RFID-Anwendungen

Die nähere Ausgestaltung der §§ 1 Abs 1 und 2 finden sich in den §§ 6 bis 9. § 6 normiert die bei jeder Datenverwendung[30]) zu prüfenden Grundsätze. Diesem zufolge dürfen RFID-Daten nur nach Treu und Glauben und auf rechtmäßige Weise verwendet werden, die Datenverwendung muss sich an den Zweckbindungsgrundsatz sowie an den Wesentlichkeitsgrundsatz halten. Die Zulässigkeit der Verwendung regelt § 7. Hier finden sich in Abs 1 zunächst die Voraussetzungen für die Zulässigkeit der Verarbeitung von RFID-Daten, in Abs 2 jene der Übermittlung. In beiden Fällen dürfen Zweck und Inhalt der Datenverwendung die schutzwürdigen Geheimhaltungsinteressen des Betroffenen nicht verletzen. Ebenso wie bei allen anderen Grundrechten müssen auch beim Grundrecht auf Datenschutz Eingriffe dem Verhältnismäßigkeitsgrundsatz entsprechen.

Die §§ 8 und 9 nennen jene Fälle, in denen die Verwendung nicht sensibler bzw sensibler Daten schutzwürdige Geheimhaltungsinteressen des Betroffenen grundsätzlich nicht verletzen. Mit Zustimmung des Betroffenen[31]), im lebenswichtigen Interesse des Betroffenen, bei einer gesetzlichen Ermächtigung oder Verpflichtung[32]) sowie bei Verarbeitung von indirekt personenbezogenen[33]) Daten ist die Datenverwendung bei RFID-Anwendungen ohne Zustimmung zulässig[34]). Für eine Verarbeitung sensibler Daten im Interesse eines Dritten lässt die taxative Aufzählung des § 9 wenig Möglichkeiten. Hingegen sind für nicht-sensible Daten die konkreten Fälle, wann ein überwiegendes berechtigtes Interesse des Auftraggebers oder eines Dritten vorliegt, in § 8 demonstrativ aufgezählt. Während daher im privaten Bereich die Verwendung sensibler Daten in RFID-Anwendungen fast ausschließlich nur mit Zustimmung des Betroffenen erfolgen wird dürfen, sind die schutzwürdigen Geheimhaltungsinteressen bei nicht-sensiblen Daten auch dann nicht verletzt, wenn die Datenverwendung zur Erfüllung einer vertraglichen Pflicht zwischen Auftraggeber und Betroffenen notwendig ist. Die anderen Ausnahmefälle gelangen im privaten Bereich eher selten zur Anwendung.

Auch außerhalb des DSG finden sich Beschränkungen für die Verwendung personenbezogener Daten. Im Zusammenhang mit der RFID-Technologie wurden in das neue Heimaufenthaltsgesetz[35]) Bestimmungen aufgenommen, die eine elektronische Überwachung zum Zwecke der Freiheitsbeschränkung an bestimmte Voraussetzungen bindet[36]). Sogar im datenschutzrechtlichen „Entwicklungsland" USA überlegt man die Erlassung beschränkender Regelungen[37]).

In diesem Zusammenhang sei noch auf Folgendes hingewiesen: Häufig werden neue Überwachungstechnologien im Zusammenhang mit geistig Verwirrten, Behinderten, alten Menschen und Kindern angepriesen[38]). Manche übersehen dabei, dass auch diese Personen Grundrechtsträger sind und sich mit dem elterlichen Erziehungsrecht und der Aufsichtspflicht nicht jegliche Überwachungsmaßnahme rechtfertigen lässt[39]).

4.3 Zweckbindungsgrundsatz

Der bereits erwähnte Zweckbindungsgrundsatz nach § 6 Abs 1 Z 3 DSG schränkt die Möglichkeit der Weiterverwendung von zulässigerweise ermittelten Daten erheblich

30) Das „Verwenden von Daten" umfasst laut § 4 Z 8 jede Art der Handhabung von Daten einer Datenanwendung, also sowohl das Verarbeiten (Z 9) als auch das Übermitteln (Z 12) von Daten.

31) Bei sensiblen Daten hat die Zustimmung „ausdrücklich" zu erfolgen (§ 9 Z 6).

32) Aufgrund der taxativen Aufzählung muss bei sensiblen Daten die Ermächtigung/Verpflichtung zur Datenverwendung nur hervorgehen (§ 9 Z 3), bei nicht-sensiblen Daten muss dies ausdrücklich im Gesetz geregelt sein (§ 8 Abs 1 Z 1). Vgl *Drobesch/Grosinger*, Datenschutzgesetz (2000) § 9 Anm zu Z 1, 144.

33) Nur indirekt personenbezogen sind Daten für einen Auftraggeber, Dienstleister oder Empfänger einer Übermittlung dann, wenn der Personenbezug der Daten derart ist, dass dieser Auftraggeber, Dienstleister oder Übermittlungsempfänger die Identität des Betroffenen mit rechtlich zulässigen Mitteln nicht bestimmen kann (§ 4 Z 1 zweiter Satz).

34) Zur Unterscheidung indirekt personenbezogen und anonym: Während bei anonymen Daten niemand mehr einen Personenbezug herstellen kann, kann bei indirekt personenbezogenen Daten lediglich der Übermittlungsempfänger den Personenbezug nicht herstellen.

35) BGBl I 2004/11.

36) § 3 Abs 1. Laut EB dürfen zB weder „Optionsschleifen" oder sog „Skorpione", soweit diese eine Freiheitsbeschränkung darstellen, eingesetzt werden. Freiheitsbeschränkend sind sie dann, wenn bei Auslösen des Alarms unmittelbar der Freiheit entziehende Folgen zu erwarten sind, also etwa der Betreute „zurückgeholt" wird.

37) Vgl orf futurezone v 13. 5. 2004, Party mit implantierten Funkchips (http://futurezone.orf.at/futurezone.orf?read=detail&id=230631&tmp=54154), wo berichtet wird, dass der „VeriChip" vor zwei Jahren von der Food and Drug Administration mit der Auflage freigegeben wurde, dass darauf keine medizinischen Daten gespeichert werden. Im Februar 2004 wurde unter der Nummer 1834 eine Senate Bill im kalifornischen Senat eingebracht. Dort werden Unternehmen, die RFID zur Datensammlung verwenden, Informationspflichten auferlegt; ein Zuwiderhandeln gegen diese Bestimmungen ist ein Wettbewerbsverstoß (s http://www.leginfo.ca.gov/pub/bill/sen/sb_1801-1850/sb_1834_bill_20040220_introduced.pdf; und heise online v 2 5. 2. 2004, US-Politikerin fordert Regeln für RFID-Technik, http://www.heise.de/newsticker/meldung/44983.

38) S zB die Website der berolina elektronik GmbH, die den sog „phonetracker" vertreibt. Ein Gerät, das auf ein handelsübliches Mobiltelefon montiert wird und das die Funkzellen-ID weiterleitet, womit eine Ortung des Standorts des Telefons möglich ist. Dort heißt es ua: „Eltern können wieder aufatmen! Dank dem Phonetracker – einem kleinen Handyzubehör – können besorgte Eltern ihren Schützlingen beistehen, auch wenn sie nicht in ihrer Nähe sind." (www.phonetracker.de/Anwendungen/anw_personen.html). S auch die treffende Kritik bei Stop1984, Kinder, Zensur, Überwachung. .., http://www.stop1984.com/print.php?lang=es&text=zensur_texte_sebastianders_kinder.txt.

39) Zum Spannungsverhältnis Erziehungsrecht und Überwachungsmaßnahmen s *Geiger*, Indiskretionsdelikte und Neue Medien – Zur strafrechtlichen Relevanz der Überwachung privater Kommunikation mittels „Internet Monitoring Software" (Master Thesis Wien 2003), www.rechtsprobleme.at/doks/indiskretionsdelikte_und_neue_medien-geiger.pdf, 50.

ein. Ausnahmen gibt es nach § 46 für die Weiterverwendung zu wissenschaftlichen oder statistischen Zwecken. Ein Auftraggeber darf demzufolge Daten aus einer RFID-Anwendung nur soweit, als sie für den Zweck der Datenanwendung wesentlich sind, verwenden und über diesen Zweck nicht hinausgehen werden. Dieser Grundsatz beschränkt die Verwendungsmöglichkeiten der einmal ermittelten Daten und Auftraggeber haben vom rein „vorsorglichen" Datensammeln nichts. Von Bedeutung für ein Unternehmen ist vielmehr, wie es die gesammelten Daten weiter verwenden darf, wofür allenfalls eine entsprechende Zustimmung eingeholt werden müsste.

5. Datenschutzrechtliche Problemfelder bei RFID-Anwendungen

5.1 Informationspflichten

Um dem Betroffenen die Möglichkeit zu geben, seine Rechte zu wahren, muss er aktiv darüber informiert werden, dass seine Daten überhaupt ermittelt und weiterverarbeitet werden. Daher schreibt § 24 dem Auftraggeber eine Informationspflicht gegenüber dem Betroffenen vor. Der Auftraggeber hat nach dieser Bestimmung aus Anlass der Ermittlung von Daten den Betroffenen in geeigneter Weise über den Zweck der Datenanwendung, für die die Daten ermittelt werden, und über Namen und Adresse des Auftraggebers zu informieren, sofern diese Informationen dem Betroffenen nach den Umständen des Falles nicht bereits vorliegen. Darüber hinausgehende Informationen sind in geeigneter Weise zu geben, wenn dies für eine Verarbeitung nach Treu und Glauben erforderlich ist. Dies gilt insbesondere dann, wenn die Daten in einem Informationsverbundsystem[40]) verarbeitet werden sollen, ohne dass dies gesetzlich vorgesehen ist. Die Informationen müssten in geeigneter Form erfolgen, in einem Kaufhaus zB durch Hinweisschilde, dass RFID-Chips im Einsatz sind. Bei nicht meldepflichtigen Datenanwendungen bestehen allerdings keine Informationspflichten (§ 24 Abs 2).

5.2 Zustimmungserklärung

Werden die schutzwürdigen Geheimhaltungsinteressen des Betroffenen deshalb nicht berührt, weil die Datenverwendung zu Zwecken der Vertragserfüllung notwendig ist, bedarf es in aller Regel keiner Zustimmungserklärung. Liegt keine Vertragserfüllung vor, ist eine Zustimmung einzuholen. Die Judikatur des OGH zu Formulierung und Inhalt von Zustimmungserklärungen ist denkbar streng[41]). Aufgrund dieser und einem Rundschreiben des Verfassungsdienstes aus dem Jahre 1985[42]) sollte daher die Zustimmungserklärung folgenden Inhalt haben: Bezeichnung der Datenarten (taxative Aufzählung), Benennung der Übermittlungsempfänger (Angabe des Namens, der Firma, der Behördenbezeichnung), eine ausreichende Information des Betroffenen über die Übermittlungszwecke und einen ausdrücklichen Hinweis auf den jederzeit möglichen schriftlichen Widerruf. In formeller Hinsicht ist die Zustimmungsklausel im Text jedenfalls hervorzuheben. Wird sie in die AGB aufgenommen, so ist die Zustimmung nicht gültig erteilt worden[43]). Auftraggeber von RFID-Anwendungen müssen daher sehr darauf achten, Zustimmungserklärungen entsprechend dieser Regeln richtig zu formulieren.

6. Fallbeispiele

6.1 Logistikkette

Eine Warenhandelskette verpflichtet ihre Lieferanten, die Paletten, mit denen die von ihnen gelieferten Produkte transportiert werden, mit RFID-Tags auszustatten („unit tagging"). Die Paletten durchlaufen mehrere Stationen von der Herstellung über den Transport durch die einzelnen Zwischenhändler, bis die Produkte letztlich im Kaufhaus landen. Bei jedem Stopp werden die Daten vom Chip ausgelesen und im System der Warenhandelskette gespeichert. Die Identifikationsnummer der Palette wird mit Art und Anzahl der Artikel verknüpft.

Bei den hier anfallenden Daten handelt es sich überwiegend um Wirtschaftsdaten, an deren Geheimhaltung auch ein schutzwürdiges Interesse bestehen kann, ist es doch beispielsweise für einen Konkurrenten durchaus von Interesse, wie die Logistikkette seines Mitbewerbers organisiert ist und wie viele Artikel in einem bestimmten Zeitraum geliefert werden, sofern dies erfasst wird. Betroffene sind hier aber nicht nur die Warenhandelskette, sondern auch die Lieferanten, weil diese gleichfalls ein schutzwürdiges Geheimhaltungsinteresse daran haben, dass der konkrete Ablauf der Warenverschiebungen nicht öffentlich wird[44]). Die Einholung einer expliziten Zustimmung wird aber in aller Regel nicht erforderlich sein, da die Zustimmung durch die Befolgung der Verpflichtung zur Ausstattung mit RFID-Tags durch den Lieferanten, dessen konkludente Zustimmung enthält. Zu prüfen wäre allerdings, inwieweit auch allfällige Zwischenhändler eine konkludente Zustimmung dabei abgeben.

6.2 Warenhaus

In einem Kaufhaus sind die Produkte mit RFID-Tags ausgestattet („item tagging"), der Kunde kann so bei der Kassa mit seinem Einkaufswagen einfach vorbeigehen, die Nummern der Artikel und jene der Kundenkarte werden kontaktlos ausgelesen, und dann über die Kundenkarte mittels Bankeinzug verrechnet. Die RFID-Tags werden beim Verlassen des Kaufhauses weder entfernt noch gelöscht.

In diesem Fall könnte zunächst gespeichert werden, welche Kunden wann welche Artikel gekauft haben, was für Marketingzwecke sehr interessante Daten sind. Während in Österreich die Rechtslage unklar ist, wird in Deutschland vertreten, dass Daten für Marketingzwecke sogar benutzt werden dürfen[45]). Im konkreten Fall wäre eine Zustimmung

40) Vgl § 4 Z 13: Ein Informationsverbundsystem ist die gemeinsame Verarbeitung von Daten in einer Datenanwendung durch mehrere Auftraggeber unter gemeinsamer 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.

41) OGH 27. 1. 1999, 7 Ob 170/98w – Merkur = ecolex 1999, 182; OGH 22. 3. 2001, 4 Ob 28/01y – Bankenentscheidung I = ecolex 2001, 147 (*Rabl*); OGH 13. 9. 2001, 6 Ob 16/01y – Mobilpoints = ecolex 2002, 86 (*Leitner*); OGH 19. 11. 2002, 4 Ob 179/02f – Bankenentscheidung II = ÖBA 2003, 41.

42) Rundschreiben des BKA VD, 810.008/1 V/1a/85 vom 10. 8. 1985, abgedruckt bei *Dohr/Pollirer/Weiß*, DSG (2002) Anhang III, 2.

43) Details und eine Besprechung der zitierten Entscheidungen finden sich bei *Knyrim*, Datenschutzrecht (2003) 165 ff.

44) VfSlg 12.228/1989, 12.880/1991. Vgl auch *Singer* in *Wittmann* ua, Datenschutzrecht im Unternehmen (1991) 4 f.

45) Publizierte österreichische Meinung gibt es dazu bisher nicht. Zur deutschen Lehre s *Gola/Klug*, Grundzüge des Datenschutzrechts (2003) 126; *Simitis* (Hrsg), Kommentar zum Bundesdatenschutzgesetz[5] (2003) Rz 137 zu § 28; *Roßnagel* (Hrsg), Handbuch Datenschutzrecht (2003) 1198 f.

für die Ermittlung der Daten nicht notwendig, weil sie der Vertragserfüllung dient. Von Interesse könnte natürlich die Weitergabe der Daten an die Produzenten der Waren sein. Sollen diese in personenbezogener Form übermittelt werden, bedürfte es allerdings einer Zustimmung des Kunden. Werden die Daten anonym weitergleitet, so könnte die Übermittlung auf § 46 gestützt werden und wäre unbeschränkt zulässig. Ein weiteres Problem ist die Nichtentfernung bzw Löschung der RFID-Chips, weil die Chips dann in der unmittelbaren Privatsphäre des Kunden bleiben. Dies mag bei Lebensmitteln, die in aller Regel eine kurze Lebensdauer haben und im Kühlschrank bleiben, unproblematisch sein, anderes gilt jedoch bei Textilien und anderen nicht verderblichen Produkten, bei denen grundsätzlich die Gefahr besteht, dass sie ohne Wissen und Willen des Trägers oder Inhabers bei einem späteren Einkauf im selben Geschäft an Dritte sogar von diesen wieder ausgelesen werden können. Dazu hätte das Warenhaus vom Kunden jedenfalls die Zustimmung einzuholen.

6.3 Shopping-Center

In einem großen Einkaufszentrum wird eine Möglichkeit geschaffen, dass jeder Kunde, der etwas kauft, mit einem solchen RFID-Chip ausgestattet wird (zB die Tags befinden sich an Einkaufssackerln oder Werbeträgern). Betritt man oder verlässt man ein Geschäft bzw das Einkaufszentrum, werden die Daten entsprechend ausgelesen und an einen Zentralrechner weitergeleitet. Hierdurch sind umfangreiche statistische Berechnungen (einschließlich Bewegungsprofile, wenn auch anonym) möglich[46]). Die Betreiber des Shopping-Centers überlegen, die Kunden nach Inbesitznahme des Einkaufssackerls auf freiwilliger Basis nach Namen, Anschrift etc zu fragen. Die Daten würden in weiterer Folge verknüpft werden.

Hier stellen sich zwar mangels Vorliegens personenbezogener Daten keine datenschutzrechtlichen Probleme. Jedoch greift es in die Persönlichkeitsrechte ein, wenn man ohne sein Wissen und Einwilligung zu statistischen Berechnungen „missbraucht" wird. In Betracht käme eine Beschränkung der durch § 16 ABGB geschützten Freiheit der Willensbildung und -betätigung. Weil hier die Daten des Betroffenen zum Nutzen des Shopping-Centers verwendet werden, könnte man auch an eine Anwendbarkeit des § 1041 ABGB denken[47]). Nochmals verwiesen sei in diesem Zusammenhang auf Folgendes: Wie bereits oben angemerkt, ist es für einen Auftraggeber oftmals weniger von Bedeutung, die wahre Identität eines Betroffenen zu kennen, als vielmehr ihn identifizieren zu können, mag dies über ein Pseudonym oder auch über eine bloße Nummer geschehen. Der Auftraggeber, hier die Betreiber des Shopping-Centers, wäre in der Lage, den Betroffenen mit maßgeschneiderten Werbeangeboten, zB wenn der Betroffene an einer Video-Wand oder einem Lautsprecher vorbeigeht, zu „beglücken".

Bei Realisierung eines solchen Projekts könnten umfangreiche personenbezogene Bewegungsprofile erstellt werden und man wäre wieder im Anwendungsbereich des DSG 2000. Bei der Ermittlung der Daten der Betroffenen würden die Betreiber umfangreiche Informationspflichten treffen. Bei einer späteren Erhebung von Name und Anschrift wäre die Einbindung einer transparenten Zustimmungserklärung notwendig. Die geplante Datenanwendung wäre meldepflichtig, weil Bewegungsprofile kaum unter „Kaufverhalten" iSd SA022 (Kundenbetreuung und Marketing für eigene Zwecke) zu subsumieren sind.

7. Anwendbarkeit des TKG?

Abschließend soll noch darauf hingewiesen werden, dass RFID-Applikationen unter Umständen auch als ein öffentlich angebotener Kommunikationsdienst iSd § 3 Z 9 TKG 2003 eingestuft werden könnten und daher nach § 15 TKG 2003 anzeigepflichtig sein könnten. Dies, da das TKG 2003 einen Kommunikationsdienst als gewerbliche Dienstleistung versteht, die ganz oder überwiegend in der Übertragung von Signalen über Kommunikationsnetze besteht, ausgenommen Dienste, die Inhalte über Kommunikationsnetze und -dienste öffentlich anbieten oder eine redaktionelle Kontrolle über sie ausüben. RFID-Anwendungen, die zB nur am eigenen Betriebsgelände einer Firma zur Steuerung eines Warenlagers genutzt werden, sind kein öffentlicher Kommunikationsdienst. Bietet ein Unternehmen aber zB eine RFID-Anwendung an, mit der eine Reihe anderer Unternehmen die Möglichkeit erhalten, Standortdaten in einem öffentlichen Bereich zu vernetzen (zB an strategischen Orten in einer Stadt werden RFID-Lesegeräte montiert, die es zB Botendiensten oder Taxiunternehmen ermöglichen, Standortdaten und Bewegungsprofile ihrer Botenfahrer oder Taxis zu erhalten, oder in einer Einkaufsstraße werden bei Geschäftseingängen Lesegeräte montiert, die es ermöglichen, die Frequenz von Kunden oder Serviceleistern wie zB Wachdiensten zu messen), so könnte ein solches System dann unter das TKG 2003 fallen, wenn das Service des Systembetreibers überwiegend in der Übertragung von Signalen besteht. RFID-Anwendungen, die nicht bloß in einem abgegrenzten Betriebsgelände genutzt werden, sollten daher nicht nur einer datenschutzrechtlichen Prüfung sondern auch einer Prüfung auf allfällige Anzeigepflichten nach § 15 TKG 2003 unterzogen werden.

46) Dieses Beispiel ist nicht so fiktiv, wie es im ersten Moment anmuten mag, s orf futurezone v 27. 4. 2004, Freizeitparks setzen auf Kinder-Ortung,http://futurezone.orf.at/futurezone.orf?read=detail&id=229632&tmp=95534.

47) Vgl auch OGH 23. 10. 1990, 4 Ob 147/90 – Jose Carreras = SZ 67/79 = MR 1991,68: Der Bekanntheitsgrad einer Person ist ein vermögenswertes Gut iSd § 1041 ABGB; ebenso könnte die Zurverfügungstellung der Bewegung ein solches Gut sein.

Der Autor:
Dr. Rainer Knyrim ist Rechtsanwalt und Partner bei Preslmayr Rechtsanwälte, Wien. In seinem Tätigkeitsschwerpunkt Datenschutz- und IT-Recht berät er in- und ausländische Unternehmen, hält regelmäßig Vorträge und ist unter anderem Autor des „Praxishandbuch Datenschutzrecht". Kontakt: knyrim@preslmayr.at

Die Autorin:
Mag. Viktoria Haidinger, LL.M., ist Rechtsanwaltsanwärterin bei Preslmayr Rechtsanwälte, Wien. Sie ist Absolventin des Universitätslehrganges für Informationsrecht und Rechtsinformation. Ihre Tätigkeitsschwerpunkte liegen in den Gebieten Datenschutz- und IT-Recht.