



Gemeinsame Stellungnahme zu der Entschließung der 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder „Verbindliche Regelungen für den Einsatz von RFID-Technologien“

Dezember 2006

Die 72. Konferenz der Datenschutzbeauftragten des Bundes und der Länder hat im Oktober 2006 eine Entschließung verabschiedet, die sich mit dem Einsatz der Radiofrequenz-Identifikation (RFID) im Alltag beschäftigt und hierfür verbindliche Regeln fordert. Die Datenschutzbeauftragten sehen insgesamt im Einsatz von RFID Risiken für die informationelle Selbstbestimmung. Insbesondere seien beim Einsatz von RFID generell Forderungen nach Transparenz, Kennzeichnung von Transpondern und Deaktivierung zu berücksichtigen; heimliche Profilbildung und eine unbefugte Kenntnisnahme gespeicherter Daten seien auszuschließen.

Vorbemerkung

Das Informationsforum RFID e.V., der Bundesverband Informationswirtschaft Telekommunikation und neue Medien e.V. (BITKOM), der Bundesverband der Deutschen Industrie e.V. (BDI), GS1 Germany sowie der Hauptverband des Deutschen Einzelhandels e.V. (HDE) stimmen mit den Datenschutzbeauftragten überein, dass im Rahmen des breiten Einsatzes der RFID-Technologie im Endverbraucherbereich der Schutz personenbezogener Daten ein wichtiger Faktor ist. Leider ist jedoch festzustellen, dass sich sowohl die öffentliche als auch die fachliche Diskussion zum Thema RFID und Datenschutz oft auf unzutreffende Annahmen und unrealistische Missbrauchsszenarien stützt. Auch die Entschließung der Datenschutzbeauftragten geht – basierend auf verschiedenen Anwendungsbeispielen – von einem hohen Risikopotenzial der Technologie aus und fordert dementsprechend regulatorische Einschränkungen bis hin zu gesetzlichen Regelungen.

Bedauerlich ist dabei, dass bei den Einzelforderungen der Datenschutzbeauftragten vom Abgleich mit dem gesetzlichen Status Quo abgesehen wurde. In vielen der angesprochenen Zusammenhänge finden z.B. das Bundesdatenschutzgesetz, das Telekommunikationsgesetz oder das Strafgesetzbuch Anwendung und bieten ein differenziertes und effektives Regelungsgefüge. Die Aufstellung von Forderungen ohne die Einordnung in dieses bestehende Regelungsgefüge erweckt den unzutreffenden Eindruck, dass sich RFID-Anwendungen in einem rechtsfreien Raum bewegen. Das erschwert die Diskussion über einen etwaigen Ergänzungsbedarf bestehender Regelungen. Auch führt es zu Rechtsunsicherheit bei Unternehmen, die wissen müssen, wann sie sich im Geltungsbereich zwingender gesetzlicher Vorschriften bewegen.

Differenzierung bei der Darstellung der Anwendungen

Die RFID-Technologie wurde bereits Mitte des letzten Jahrhunderts zur Flugzeugidentifikation eingesetzt und seitdem ständig weiterentwickelt. Heute findet sie hauptsächlich Anwendung in Transport und Logistik, Identifizierung und Sicherheit, Zugangsmanagement und Produktionssteuerung. Für die Zukunft werden Anwendungen vor allem im Gesundheitssektor und im Einzelhandel erwartet. Weitere oft zitierte Beispiele gehören dagegen eher in den Bereich der Visionen; ob z.B. in absehbarer Zukunft eine Ausstattung von Geldscheinen mit RFID-Transpondern zu erwarten ist, ist äußerst fraglich.

Was den Einzelhandel betrifft, so gibt es heute – entgegen der Aussage in der Entschließung – keine RFID-Kennzeichnung von Lebensmitteln außerhalb eng begrenzter Pilotprojekte. Es wird erwartet, dass eine Kennzeichnung von Produkten auf Artelebene im Einzelhandel nicht vor Ablauf mehrerer Jahre technisch möglich und wirtschaftlich sinnvoll sein wird.

Schließlich vermischt die Entschließung Anwendungen im hoheitlichen und nicht-hoheitlichen Bereich. Hier ist eine klare Differenzierung erforderlich, da nur im letzteren Fall die Wirtschaft Einfluss auf die Gestaltung der Rahmenbedingungen hat.

Keine pauschale Bewertung der RFID-Technologie

Was die datenschutzrechtliche Bewertung der RFID-Technologie betrifft, ist zu berücksichtigen, dass RFID eine Basistechnologie für eine Vielzahl von Anwendungen darstellt. Eine pauschale Bewertung der Technologie, wie sie die Entschließung vornimmt, verbietet sich schon auf Grund der Vielfalt der darauf basierenden Anwendungen. Relevant für die datenschutzrechtliche Betrachtung sind vielmehr immer die einzelne Anwendung und die Art der Daten, die durch sie verarbeitet werden.

Klare Unterscheidung zwischen personenbezogenen und produktbezogenen Daten

Für den Schutz personenbezogener Daten existiert in Deutschland ein klares und bewährtes Regelwerk. Sofern also in der Entschließung die Einhaltung von Prinzipien wie Datensparsamkeit, Zweckbindung etc. gefordert wird, ergibt sich dies für die Verarbeitung personenbezogener Daten bereits unmittelbar aus dem geltenden Datenschutzrecht. Gleiches gilt für die in der Entschließung erwähnten detaillierten Datenprofile von Betroffenen, die nach dem Bundesdatenschutzgesetz immer eine Einwilligung des Betroffenen voraussetzen.

Die Datenschutzbeauftragten sehen jedoch offenbar auch bei den Anwendungen, bei denen auf RFID-Transpondern lediglich produktbezogene Daten gespeichert sind, generell Risiken für das Recht auf informationelle Selbstbestimmung. Das Bundesdatenschutzgesetz verneint dort einen Schutzbedarf, da dieser erst beginnt, wo das konkrete Risiko der Identifizierung einer natürlichen Person besteht. Um den Bedenken gleichwohl Rechnung zu tragen, existieren bereits mehrere Selbstverpflichtungserklärungen und Richtlinien von Wirtschaftsorganisationen, die Grundregeln für den Einsatz der RFID-Technologie auch im Bereich nicht-personenbezogener Daten regeln¹. Diese Regeln werden sukzessive der Entwicklung der Technologie angepasst.

Kein Bedarf für ein Eingreifen des Gesetzgebers

Nach alledem besteht für ein Eingreifen des Gesetzgebers kein Bedarf. Was den breiten Einsatz im Endkundenbereich betrifft, befindet sich die Technologie noch in der Erprobungsphase; konkrete Gefährdungen für das Recht auf informationelle Selbstbestimmung gehen hiervon nicht aus. Und die bereits existierenden Anwendungen im Bereich RFID sind, sofern

¹ Siehe z.B. „Positionspapier der deutschen Konsumgüterwirtschaft von GS1 Germany, abrufbar unter www.gs1-germany.de/content/e39/e466/e468/datei/epc_rfid/daten_verbraucherschutz.pdf.

sie personenbezogene Daten verarbeiten oder produktbezogene Daten mit denen einer natürlichen Person verknüpfen, durch das geltende Datenschutzrecht hinreichend abgedeckt.

Was zukünftige Anwendungen insbes. im Einzelhandel betrifft, so lässt sich heute noch nicht absehen, wie eine Umsetzung im Detail erfolgen wird und wie die Prozesse beispielsweise für die Abrechnung an einer Transponderkasse oder die Deaktivierung von Transpondern ausgestaltet werden. Eine diesbezügliche Regulierung liefe daher Gefahr, entweder bei der breiten Einführung von RFID im Endkundenbereich nicht mehr dem Stand der Technik zu entsprechen oder – und dies ist ein durchaus realistisches Risiko – letztlich die erfolgreiche Einführung der Technologie in Deutschland sachwidrig zu verhindern.

Stellungnahme zu den Forderungen für eine verbindliche Regelung

Forderung 1 der Datenschutzkonferenz: **Transparenz**

Alle Betroffenen müssen umfassend über den Einsatz, Verwendungszweck und Inhalt von RFID-Tags informiert werden.

Die Wirtschaft teilt das grundsätzliche Anliegen, Transparenz zu schaffen. Transparenz ist eine grundlegende Voraussetzung für das Vertrauen in RFID-Anwendungen. Es gibt daher schon seit geraumer Zeit Aktivitäten der Wirtschaft, Betroffene über existente und potentielle RFID-Anwendungen, ihre Zusammenhänge und Implikationen zu informieren. Auch gibt es bereits zahlreiche Richtlinien für die Anwendung von RFID im Endverbraucherbereich, so beispielsweise von der International Chamber of Commerce oder dem US-amerikanischen Center for Democracy and Technology. Besondere Bedeutung haben die Verbraucherschutzrichtlinien von EPCglobal, zu deren Einhaltung sich alle Unternehmen weltweit verpflichten, die den Electronic Product Code (EPC) nutzen. Danach werden umfassende Informationen für Verbraucher über RFID bereitgestellt; insbesondere beim Einsatz von RFID auf Endverbrauchereinheiten werden Verbraucher durch weiterführende Informationen über den EPC und die Technologie aufgeklärt.

RFID-Hersteller- und Anwenderunternehmen stellen sich auch auf nationaler Ebene der Forderung nach Transparenz im Rahmen einer Selbstverpflichtung. Erste Diskussionen hierüber fanden im Rahmen eines vom Bundeswirtschaftsministerium initiierten Runden Tisches statt. Was den Wortlaut der Forderung der Datenschutzkonferenz betrifft, so bestünde aus Sicht der Wirtschaft allerdings Konkretisierungsbedarf hinsichtlich der verwendeten unbestimmten Begriffe und des Umfangs der Verpflichtung. Unerlässlich sind hierbei eine differenzierte Betrachtung der unterschiedlichen RFID-Anwendungen und eine sorgfältige Abwägung zwischen den Schutzinteressen des Betroffenen und den Interessen des Verwenders.

Zusätzlich zu den freiwilligen Schritten im Rahmen von Richtlinien und Selbstverpflichtungen sind bestimmte Informationspflichten bereits heute gesetzlich vorgeschrieben. Im Bereich der personenbezogenen Daten gelten alle Informationspflichten, die sich aus zentralen Vorschriften des BDSG ergeben.

Forderung 2 der Datenschutzkonferenz: **Kennzeichnungspflicht**

Nicht nur die eingesetzten RFID-Tags selbst, sondern auch die Kommunikationsvorgänge, die durch die Chips ausgelöst werden, müssen für die Betroffenen leicht zu erkennen sein. Eine heimliche Anwendung darf es nicht geben.

Kennzeichnung der RFID-Tags

In der überwiegenden Anzahl der Anwendungen werden auf dem RFID-Tag keine personenbezogenen Daten gespeichert oder durch den Chip erhoben, sondern der Chip enthält lediglich sach- bzw. objektbezogene Informationen. Auch bei der Kennzeichnung von Konsumgütern auf Artikelebene, die in einigen Jahren beginnen könnte, werden lediglich Produktdaten gespeichert. Diese sach- bzw. objektbezogenen Informationen sind datenschutzrechtlich

neutral. Trotzdem bezieht sich ein großer Teil der in der öffentlichen Diskussion geäußerten Bedenken auf die Ausstattung von Alltags- und Verbrauchsgegenständen mit RFID-Etiketten.

Um diesen Bedenken Rechnung zu tragen, sehen beispielsweise die EPCglobal-Verbraucherschutzrichtlinien vor, dass Endverbraucherprodukte, die mit einem EPC versehen sind, mit einem Logo besonders kenntlich gemacht werden. Verbraucher werden über das Logo und seine Bedeutung informiert.

Kennzeichnung der Kommunikationsvorgänge

Mit der Entschließung wird nicht nur die Kennzeichnung bzgl. der RFID-Tags gefordert, sondern darüber hinaus auch die Kenntlichmachung der „Kommunikationsvorgänge, die durch den Chip ausgelöst werden“. Der Inhalt dieser Forderung bleibt jedoch pauschal und unklar. Gemeint ist möglicherweise, dass Verfahren zur Sichtbarmachung des Aktivierungszustands bzw. der Aktivierbarkeit implementiert werden müssen, um die betroffene Person über die Übertragung von Daten mittels RFID zu informieren.

Eine entsprechende Kennzeichnungspflicht ergibt sich bereits aus dem BDSG für Konstellationen, in denen bei mobilen Speicher- bzw. Verarbeitungsmedien eine über die Speicherung hinausgehende Verarbeitung personenbezogener Daten möglich ist. Beispiele hierfür sind Versicherungskarten oder bestimmte Formen elektronischer Tickets.

Wo dies aber nicht der Fall ist, weil der RFID-Tag lediglich ein automatisiertes Auslesen von sach- oder objektbezogenen Informationen ermöglicht, stellt sich die Frage nach dem Sinn einer solchen Kenntlichmachung. Die Übertragung von Produktdaten stellt für den Verbraucher kein Datenschutzrisiko dar, mangels einer Übertragung personenbezogener Daten hat er auch keine Auskunft- oder Lösungsansprüche, deren Geltendmachung ihm durch die Kenntlichmachung erleichtert würde. Dem gegenüber stünde der hohe Aufwand der Wirtschaft für die Umsetzung einer solchen Regel. Schließlich zeigt auch die Erfahrung, dass optische oder akustische Warnsignale, wie sie heute z.B. bei Warensicherungssystemen zum Einsatz kommen, bereits nach kurzer Zeit nicht mehr wahrgenommen werden.

Heimliche Anwendung

Nach Satz 2 der zweiten Forderung darf es keine heimlichen Anwendungen geben. Diese Forderung dürfte inhaltlich redundant zur Forderung 1 (Transparenz) sein, da die gemäß der ersten Forderung sicherzustellende „umfassende Information über den Einsatz“ eine heimliche Anwendung ausschließt.

Forderung 3 der Datenschutzkonferenz: Keine heimliche Profilbildung

Daten von RFID-Tags aus verschiedenen Produkten dürfen nur so verarbeitet werden, dass personenbezogene Verhaltens-, Nutzungs- und Bewegungsprofile ausschließlich mit Wissen und Zustimmung der Betroffenen erstellt werden können. Soweit eine eindeutige Identifizierung einzelner Gegenstände für einen bestimmten Anwendungszweck nicht erforderlich ist, muss auf eine Speicherung eindeutig identifizierender Merkmale auf den RFID-Tags verzichtet werden.

Zustimmung des Betroffenen

Eine heimliche Profilbildung ist nach geltendem Recht unzulässig. Die Erstellung von personenbezogenen Verhaltens-, Nutzungs- und Bewegungsprofilen setzt notwendig eine Datenverarbeitung voraus. Eine solche Datenverarbeitung ist nach geltendem Recht nur nach vorheriger Einwilligung des Betroffenen zulässig. An die Wirksamkeit der Einwilligung des Betroffenen werden strenge Anforderungen gestellt (umfassende Information, Freiwilligkeit, Schriftform etc.), die Einwilligung ist zudem frei widerruflich. Diese Anforderungen sind technikneutral, sie gelten in gleicher Weise bei allen denkbaren Formen der Datenerfassung, also auch für die Verarbeitung von Kundendaten mit Hilfe von RFID-Systemen.

Wissen des Betroffenen

Soweit gefordert wird, dass die Verarbeitung nur mit Wissen des Betroffenen geschieht, ist zu beachten, dass das Wissen des Betroffenen über den Zweck der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten eine zwingende Voraussetzung der wirksamen Einwilligung und damit auch von den geltenden Datenschutzregeln bereits sichergestellt ist.

Verzicht auf Speicherung eindeutig identifizierender Merkmale

Der große Vorteil der RFID-Technologie im Vergleich zu existierenden Auto-ID-Technologien liegt gerade in der Möglichkeit, Produkte eindeutig zu identifizieren. So wurde die Serialisierung der Nummern im Transponder gerade zum Schutz und Vorteil von Verbrauchern und Unternehmen entwickelt, um u. a. Rückverfolgbarkeit und Produktsicherheit, Umtausch- und Garantieabwicklung sowie Plagiatschutz und Fälschungssicherheit realisieren zu können. Das gilt sowohl für Logistik und Lagerhaltung wie auch für weiterführende Anwendungsgebiete wie Wartung, Garantie oder Recycling. Die eindeutige Identifizierbarkeit ist für eine Vielzahl von RFID-Anwendungen daher ein unverzichtbares Merkmal. Ein Verzicht auf die Speicherung eindeutig identifizierender Merkmale würde diese Vorteile und Sicherheit ausschließen. Darüber hinaus wäre es auch aus wirtschaftlicher, technischer und organisatorischer Sicht nur mit erheblichem Aufwand handhabbar.

In den meisten Anwendungsfällen befinden sich keine personenbezogenen Daten auf den Transpondern. Wo dies der Fall sein sollte, greifen selbstverständlich die datenschutzrechtlichen Anforderungen an eine Einwilligung wie auch die Grundsätze der Datensparsamkeit bzw. Datenvermeidung. Der Schutz der Betroffenen ist dadurch gewährleistet. Ein darüber hinausgehendes Schutzbedürfnis beim Einsatz nicht-personenbezogener Daten ist angesichts des hohen Differenzierungsaufwandes für die Verwender der Technologie nicht ersichtlich.

Forderung 4 der Datenschutzkonferenz: Vermeidung der unbefugten Kenntnisnahme

Das unbefugte Auslesen der gespeicherten Daten muss beispielsweise durch Verschlüsselung bei ihrer Speicherung und Übertragung unterbunden werden.

Der Schutz von Datenbanken gegen unbefugtes Auslesen hat in IT-Systemen hohe Priorität. Schon aus eigenem Interesse sind Wirtschaftsunternehmen bestrebt, größtmögliche Datensicherheit in ihren Systemen zu gewährleisten. Dies gilt selbstverständlich auch für RFID-Systeme, die ja in der Regel in IT-Systeme der Unternehmen wie z.B. Warenwirtschaftssysteme eingebettet sind.

Bei der Frage nach der Angemessenheit von Sicherungsmaßnahmen müssen jedoch immer die Umstände des Einzelfalles ausschlaggebend sein. Je nach Charakter der verarbeiteten Daten sind mehr oder weniger aufwendige Maßnahmen geboten. Pauschale Forderungen z.B. nach einer zwingenden Verschlüsselung bei der Speicherung und Übertragung sind in diesem Zusammenhang nicht zielführend.

Im Übrigen schützen bereits heute verschiedene Gesetze Daten in umfassender Form gegen unbefugtes Auslesen. Zusätzlich zu den Regeln des Bundesdatenschutzgesetzes bietet gesetzlichen Schutz zum einen das Telekommunikationsgesetz, das in § 89 ein Abhörverbot für Nachrichten enthält, die durch eine Funkanlage gesendet werden. Im Missbrauchsfall droht Freiheitsstrafe bis zu zwei Jahren oder Geldstrafe. Zum anderen hinaus findet auch § 202 a StGB Anwendung, der die Vertraulichkeit von Daten schützt. Was den präventiven, technischen Schutz von Daten betrifft, so enthält die Anlage zu § 9 BDSG (technisch-organisatorische Maßnahmen) umfassende Anforderungen an Organisationen, die personenbezogene Daten verarbeiten.

Forderung 5 der Datenschutzkonferenz: Deaktivierung

Es muss vor allem im Handels- und Dienstleistungssektor die Möglichkeit bestehen, RFID-Tags dauerhaft zu deaktivieren bzw. die darauf enthaltenen Daten zu löschen, insbesondere dann, wenn Daten für die Zwecke nicht mehr erforderlich sind, für die sie auf dem RFID-Tag gespeichert wurden.

Die Möglichkeit einer Deaktivierung von RFID-Tags ist ein wichtiges Mittel, um die Akzeptanz für die RFID-Technologie bei Verbrauchern zu erhöhen. Die Verbraucherschutzrichtlinien von EPCglobal sehen daher vor, dass Kunden RFID-Chips vor dem Verlassen des Ladengeschäfts deaktivieren können und hierzu entsprechende Informationen erhalten. Die neueste Generation von EPC-Transpondern enthält einen sogenannten Kill-Befehl, der eine einfache Deaktivierung durch Zerstörung des Datensatzes ermöglicht. Ein Auslesen der Daten auf dem Transponder ist danach nicht mehr möglich.

Ferner werden auch technische Lösungen entwickelt, die es ermöglichen, das unbefugte Auslesen eines Transponders zu verhindern, ohne dabei den Datensatz zu zerstören. So hat beispielsweise das Unternehmen IBM einen sogenannten Clipped Tag entwickelt, bei dem die Verbindung zwischen Chip und Antenne durch einfaches Abreißen getrennt werden kann. Die Informationen auf dem Chip bleiben erhalten und können durch Auslesen aus sehr geringer Entfernung auch noch genutzt werden, z.B. zur Geltendmachung von Gewährleistungsansprüchen.

Schluss

RFID-Hersteller und -Anwenderunternehmen nehmen ihre Verantwortung für eine verbraucherfreundliche Technologieeinführung sehr ernst. Hierzu gehört zunächst, dass die Anwendungen, soweit sie personenbezogene Daten berühren, konform mit dem geltenden Datenschutzrecht ausgestaltet werden. Darüber hinaus wird den Bedenken von Verbrauchern, die die Verarbeitung nicht-personenbezogener Daten betreffen, über Selbstverpflichtungserklärungen oder Richtlinien von Wirtschaftsorganisationen Rechnung getragen. Dabei besteht Einigkeit, dass die Vermittlung von Informationen, die Herstellung von Transparenz und die Ermöglichung einer Deaktivierung wesentliche Elemente sind, um Vertrauen bei Verbrauchern zu erzeugen. Die genaue Ausgestaltung solcher Richtlinien muss – alleine schon wegen des schnellen technologischen Wandels – einer dauernden Evaluation und Weiterentwicklung unterworfen sein.

Die Mitgliedsunternehmen des Informationsforum RFID und des BITKOM sowie der BDI, GS1 Germany und HDE sind offen für die Fortsetzung des Dialogs mit Daten- und Verbraucherschutzorganisationen. Dabei ist aber zum einen zu berücksichtigen, dass Verbraucher insbes. im Einzelhandel derzeit noch kaum mit der RFID-Technologie in Berührung kommen. Eine detaillierte Regulierung der Technologie, wie sie teilweise in der politischen Diskussion und der Entschließung der Datenschutzbeauftragten vorgeschlagen wird, steht daher in keinem Verhältnis zum tatsächlichen Schutzbedürfnis des Verbrauchers zum jetzigen Zeitpunkt. Zum anderen muss im Dialog Beachtung finden, welchen Schutz das Bundesdatenschutzgesetz schon jetzt bietet. Ziel muss sein, ein ausgewogenes Verhältnis herbeizuführen zwischen dem Schutz der Verbraucher und der Flexibilität, die für die Wirtschaft bei Einführung innovativer Technologien unerlässlich ist, um Deutschland im globalen Wettbewerb erfolgreich positionieren zu können.