

6. April 2011

RFID-Technik als Herausforderung für den Datenschutz

Positionspapier des Verbraucherzentrale Bundesverbandes

zum europäischen Selbstverpflichtungsrahmen für Datenschutzfolgenabschätzungen („PIA Framework“) für die Nutzung von RFID

Verbraucherzentrale Bundesverband e.V. – vzbv
KOM-Registernummer: 2893800753-48
Fachbereich Wirtschaft und Internationales
Markgrafenstr. 66
10969 Berlin
wirtschaft@vzbv.de
www.vzbv.de

Am 06. April 2011 wurde ein europäischer Selbstverpflichtungsrahmen für Datenschutzfolgenabschätzungen („PIA Framework“) für die Nutzung von RFID durch Vertreter der Industrie, der Zivilgesellschaft und Datenschützern unterzeichnet. Der Verbraucherzentrale Bundesverband begrüßt diesen Schritt, mahnt aber eine konsequente Umsetzung der Selbstverpflichtung an.

Der Einsatz der RFID-Technik im Einzelhandel wirft neben Vorteilen für Verbraucher auch datenschutzrechtliche Probleme auf. Die sehr kleinen RFID-Chips („Tags“) enthalten eine eindeutige Nummer, die kontaktlos und unbemerkt ausgelesen werden kann. Dadurch ermöglicht es diese Technik Objekte eindeutig zu identifizieren – und damit auch Personen, die diese mit sich führen. Werden diese Daten in der Hintergrunddatenbank des Systems mit weiteren Informationen zusammengeführt, besteht beispielsweise die Gefahr, dass das Verhalten der Verbraucher ausspioniert wird und Konsumentenprofile erstellt werden.

Mit der Einführung von RFID-Systemen wachsen daher die Herausforderungen für den Datenschutz und die Datensicherheit. Die praktische Gewährleistung der datenschutzrechtlichen Vorgaben wird jedoch durch die besondere Funktionsweise von RFID erschwert. Denn aufgrund der automatischen und sichtkontaktlosen Art der Datenübertragung vom Chip zum Lesegerät ist nicht erkennbar, wann, wo und in welchem Umfang ein Personenbezug entsteht und welche Verknüpfungen gemacht werden können.

Die Anzahl der RFID-Anwendungen in der Sphäre des Verbrauchers hat sich in den letzten Monaten deutlich erhöht. So nehmen derzeit fest integrierte Anwendungen rasant zu, zum Beispiel im Textil- und Modebereich¹ oder auch im e-Ticketing². Informationsmaßnahmen der Betreiber werden teilweise zwar durchgeführt, sind aber in der Regel uneinheitlich und punktuell. Auch eine breiter angelegte und systematische Sensibilisierungskampagne von Seiten der Politik zur Anregung einer umfassenden gesellschaftlichen Diskussion bleibt weitgehend aus.

Um den Gefahren der RFID-Technik zu begegnen, ist es aus Sicht des vzbv weiterhin geboten, dass der Gesetzgeber klare Vorgaben zum Einsatz der RFID-Technik macht. Auch aus gesamtwirtschaftlicher Sicht sind klare Vorgaben unerlässlich, denn nur wenn die Verbraucher Vertrauen in Datenschutz haben und sich ausreichend informiert fühlen, werden sie die RFID-Technologie annehmen.

Empfehlung der EU / Datenschutzfolgeabschätzung

Im Mai 2009 veröffentlichte die EU-Kommission eine „*Empfehlung (2009/387/EG) zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen*“³. Kern der Empfehlung ist die Aufforderung an die Mitgliedstaaten dafür zu Sorge tragen, dass die RFID-Branche in Zusammenarbeit mit den jeweiligen Beteiligten aus der Zivilgesellschaft einen europäischen Rahmen für Datenschutzfolgenabschätzungen („PIA Framework“) für die Nutzung von RFID-Systemen aufstellt. Dieser soll eine Orientierungshilfe für die Betreiber von RFID-Anwendungen bieten, um ihre Systeme datenschutzgerecht zu gestalten.

Auf europäischer Ebene hat inzwischen eine „*Informal Working Group*“ unter Beteiligung von Industrie, Betreibern und Normungsorganisationen den in der Empfehlung benannten Rahmen für die Datenschutzfolgeabschätzung erarbeitet⁴.

¹ <http://www.gerryweber.com/ag-website/de/startseite/unternehmen/unternehmensprofil/innovationen/rfid>

² http://www.vrr.de/de/global/hilfe_faq/fragen_und_antworten/01029/index.html

³ <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:DE:PDF>

⁴ http://www.gs1.org/docs/epcglobal/Privacy_Impact_Assessment_Framework.pdf

Nachdem der erste Entwurf im Frühjahr 2010 durch die Artikel-29-Datenschutzgruppe der EU als unzureichend zurückgewiesen wurde⁵, stimmte sie dem aktuellen Papier im Februar 2011 zu⁶. Am 06. April 2011 wurde das PIA Framework schließlich durch Vertreter der Industrie, der Zivilgesellschaft und Datenschützern unter der Teilnahme der EU-Kommissarin Neelie Kroes unterzeichnet.

Was nun ansteht, ist die schnelle, konsequente Umsetzung der Empfehlungen sowie der Datenschutzfolgeabschätzung auf nationaler Ebene. Nur unter den im PIA Framework definierten Voraussetzungen wird es gelingen, den dem Datenschutz angemessen Rechnung zu tragen und den nach wie vor weit verbreiteten Sorgen von Verbrauchern in Bezug auf den Einsatz von RFID-Anwendungen adäquat zu begegnen.

Anforderungen des vzbv

Für die weitere Vorgehensweise formuliert der vzbv aus Verbrauchersicht folgende Anforderungen:

Wirksame Selbstverpflichtung der Betreiber

Nach der Annahme des PIA Frameworks muss nun eine wirksame, flächendeckende und verpflichtende Selbstregulierung der Wirtschaft auf nationaler Ebene dringend angestrebt werden. Scharfe und wirksame Sanktionsmöglichkeiten müssen definiert und in der Praxis strikt umgesetzt werden.

Weiterhin gelten hierfür die Grundsätze von Transparenz und Kennzeichnung (keine heimliche Anwendung), verbindliche Durchführung von Datenschutzfolgeabschätzungen, Zugang zu ausführlicher Information, Deaktivierung als Standard, Datenvermeidung und Datensparsamkeit, Gewährleistung von Wahlfreiheit. Gelingt es hier nicht, zu überzeugenden Lösungen zu kommen, muss die Frage der Spezialgesetzgebung zur Reglementierung zentraler Aspekte erneut in Erwägung gezogen werden.

Datenschutzfolgeabschätzungen konsequent durchführen und nachhalten

Datenschutzfolgeabschätzungen gemäß dem PIA Framework müssen kompromisslos durchgeführt werden. Bei Anwendungen, die im Einzelhandel bis in die Verbrauchersphäre reichen (z.B. beim Einsatz in Textilien zur Diebstahlsicherung oder Verkaufsförderung), müssen diese Abschätzungen auch rückwirkend durchgeführt werden. Gemäß der Vorgaben der Europäischen Union sollten diese Verfahren in spätestens drei Jahren evaluiert und falls nötig überarbeitet werden.

Kennzeichnung

Bei der Umsetzung der Empfehlungen dürfen die Betreiber von RFID-Anwendungen nicht alleine auf die Kennzeichnung von Lesegeräten verpflichtet werden. Gleichzeitig sind unmissverständliche Kennzeichnungen am Produkt unerlässlich, um die notwendige Transparenz für den Verbraucher herzustellen. Diese Kennzeichen müssen außerdem den Namen des Betreibers und Kontaktinformationen enthalten. Außerdem darf diese Regelung nicht auf den Einzelhandel beschränkt sein. Es muss stets Klarheit herrschen, wo RFID-Chips eingesetzt werden.

⁵ http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2010/wp175_de.pdf

⁶ http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-a29wp-opinion-11-02-2011_en.pdf

Transparenz und freien Zugang zu Information ermöglichen

Zur Absicherung und Erhöhung der Transparenz von Informationen müssen insbesondere die Risiken einer Anwendung klar kommuniziert werden. Weiterführende Informationen am „*Point of sale*“ sowie Zugang zu vollständigen Ergebnissen der Datenschutzfolgeabschätzung (z.B. durch Bereitstellung im Internet durch die zuständigen Stellen, denen die Berichte vorgelegt werden) sind daher dringend notwendig. Durch die Informationen muss auch deutlich werden, ob beispielsweise der Standort der Chips überwacht wird. Zusätzlich müssen alle Kommunikationsvorgänge durch optische bzw. akustische Signale begleitet werden.

Ein derartig transparent gestalteter Zugang zu Information trägt dazu bei, dass die gesellschaftliche Diskussion auf der Grundlage von Fakten beeinflusst wird und unbegründete Sorgen von Verbrauchern glaubwürdig ausgeräumt werden können.

Selbstbestimmung ermöglichen

Wann immer wenn ein Chip eindeutig identifizierbar ist, besteht die Möglichkeit einen Personenbezug herzustellen. Die überprüfbare Deaktivierung muss daher, wie in der Empfehlung der Kommission bestätigt, als Standard praktiziert werden („*opt-in*“) - auch in den Fällen, in denen die Datenschutzfolgeabschätzung zu einem unbedenklichen Ergebnis gekommen ist. Da es für den Verbraucher nicht ersichtlich ist, um was für einen Chip es sich handelt und ob dieser zerstört, deaktiviert oder aktiviert wird, fordert der vzbv die physische Entfernung der Tags am Verkaufsort oder vor Versand im Fernabsatz.

Für die Verbraucher dürfen dabei kein unzumutbarer Aufwand oder wirtschaftliche Nachteile entstehen. After-Sales-Prozesse (wie Garantieleistungen) dürfen beispielsweise nicht von aktivierten Tags abhängig sein.

Sollte sich ein Verbraucher informiert und bewusst dafür entscheiden, einen Chip aktiviert zu lassen, müssen die Einwilligungserklärungen klar, verständlich und an die Alltagsrealität des Einkaufs angepasst sein. Auf keinen Fall dürfen durch Kennzeichnung und Information die Anforderungen an die Wirksamkeit von datenschutzrechtlichen Einwilligungen abgesenkt werden.

Angemessene Ausstattung für Datenschutzbeauftragte

Das PIA Framework besagt, dass den zuständigen Datenschutzaufsichtsbehörden durch die Betreiber der RFID-Anwendungen die Datenschutzfolgeabschätzung spätestens sechs Wochen vor Inbetriebnahme der Systeme vorgelegt werden muss. Damit die Datenschutzbeauftragten diese Aufgabe überhaupt angemessen und zeitnah wahrnehmen können, müssen sie entsprechend mit finanziellen und personellen Ressourcen ausgestattet werden. Ihre bisherige Arbeit darf nicht unter dieser neuen Aufgabe leiden.

Aufklärungspolitik verbessern

Alle relevanten Akteure (Wirtschaft, Bund und Länder, Verbraucherorganisationen) müssen eine aktive Rolle bei der Sensibilisierung der Öffentlichkeit übernehmen. Mittlerweile haben sich die verbraucherrelevanten Anwendungen von RFID stark verbreitet. Eine breitere öffentliche Diskussion und Aufklärung der Verbraucher ist daher dringend nötig. In dieser Diskussion muss insbesondere auf die Gefahren durch Verknüpfung verschiedener Anwendungen und die datenschutzrechtlichen Aspekte potentiell personenbeziehbarer Daten abgehoben werden.