ARTIKEL-29-DATENSCHUTZGRUPPE

00327/11/DE
WP 180

Stellungnahme 9/2011 zu dem überarbeiteten Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen

Angenommen am 11. Februar 2011

Inhalt

DIE GRUPPE FÜR DEN SCHUTZ VON PERSONEN BEI DER VERARBEITUNG PERSONENBEZOGENER DATEN

eingesetzt durch die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995,

gestützt auf Artikel 29 und auf Artikel 30 Absatz 1 Buchstabe a und Absatz 3 dieser Richtlinie sowie Artikel 15 Absatz 3 der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002,

gestützt auf ihre Geschäftsordnung,

hat folgende Stellungnahme angenommen:

1 Hintergrund

1.1 Einleitung

Diese Stellungnahme knüpft an die Stellungnahme[1] 5/2010 (WP 175) zum *Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen* an. Wenngleich in der Einleitung einige Hintergrundinformationen wiederholt werden, die zum Verständnis des Zwecks und des Umfangs dieser neuen Stellungnahme erforderlich sind, wird der Leser dennoch dazu aufgefordert, die Stellungnahme 5/2010 für weitere Einzelheiten zu lesen.

Am 12. Mai 2009 nahm die Kommission eine Empfehlung[2] zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen an. In dieser Empfehlung werden die Mitgliedstaaten dazu aufgefordert, dafür zu sorgen, dass *die Branche in Zusammenarbeit mit den jeweiligen Beteiligten einen Rahmen für Datenschutzfolgenabschätzungen* aufstellt, der *der Artikel-29-Datenschutzgruppe zur Prüfung* vorgelegt werden sollte. Sobald dieser Rahmen für die Datenschutzfolgenabschätzungen vorliegt, sollen die Mitgliedstaaten dafür sorgen, dass RFID-Anwendungsbetreiber vor der Einführung von RFID-Anwendungen eine Datenschutzfolgenabschätzung durchführen und die dabei erstellten Berichte der zuständigen Behörde zur Verfügung stellen.

Am 31. März 2010 legten Branchenvertreter der Artikel-29-Datenschutzgruppe einen Vorschlag für einen Rahmen für Datenschutzfolgenabschätzungen zur Prüfung vor. Wenngleich dieser Vorschlag einen guten Ansatzpunkt darstellte, erhielt er nicht die volle Zustimmung der Datenschutzgruppe, insbesondere da in dem vorgeschlagenen Rahmen die folgenden drei wesentlichen Bestandteile fehlten:

1) ein klar definiertes Risikobewertungskonzept

2) die Berücksichtigung der RFID-Tags, die von Personen außerhalb der Reichweite der Anwendung mitgeführt werden

---

[1] Stellungnahme 5/2010 zum Vorschlag der Branche für einen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen, WP 175, 13. Juli 2010.

[2] http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

3) ein Weg, die Grundsätze zur Deaktivierung der Tags im Einzelhandel ausdrücklich zu berücksichtigen, die von der Kommission in der Empfehlung zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen festgelegt sind.

Am 13. Juli 2010 fasste die Datenschutzgruppe diese Elemente sowie weitere Bedenken in der Stellungnahme 5/2010 zusammen und forderte die Branche auf, einen überarbeiteten Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen vorzuschlagen. In Bezug auf die Risikobewertung hat die Datenschutzgruppe die Branche nachdrücklich dazu aufgefordert, auf den bestehenden Erfahrungen der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) aufzubauen.

In demselben Monat hat die ENISA eine unabhängige Stellungnahme[3] mit praktischen Empfehlungen zur Verbesserung des vorgeschlagenen Rahmens veröffentlicht. Der Vorschlag der ENISA umfasste insbesondere einige erste Richtlinien für die Einführung eines umfassenden und anerkannten methodischen Risikobewertungskonzepts sowie verschiedene strukturelle Verbesserungen.

In den folgenden Monaten hat die Branche einen überarbeiteten Rahmen für Datenschutzfolgenabschätzungen erarbeitet, wobei sie die Beiträge sowohl der Datenschutzgruppe als auch der ENISA berücksichtigte. Am 12. Januar 2011 wurde dieser überarbeitete Rahmen für Datenschutzfolgenabschätzungen *der Artikel-29-Datenschutzgruppe* zur Prüfung vorgelegt.

In dieser Stellungnahme sind die Ansichten der Datenschutzgruppe formell zusammengefasst.

Nachfolgend bezieht sich die „RFID-Empfehlung“ auf die am 12. Mai 2009 veröffentliche Empfehlung der Kommission zur Umsetzung der Grundsätze der Wahrung der Privatsphäre und des Datenschutzes in RFID-gestützten Anwendungen. Der „überarbeitete Rahmen“ oder nur „Rahmen“ bezieht sich auf den der Datenschutzgruppe am 12. Januar 2011 übermittelten und im Anhang zu dieser Stellungnahme wiedergegebenen Rahmen für Datenschutzfolgenabschätzungen für RFID-Anwendungen. (Originaltitel: *Industry Proposal - Privacy and Data Protection Impact Assessment Framework for RFID Applications*, deutsche Fassung liegt nicht vor - Anm. d. Ü.).

1.2 Zusammenfassung des überarbeiteten Rahmens

Der überarbeitete Rahmen beginnt mit einem Überblick über wichtige interne Prozeduren, die für die Durchführung der Datenschutzfolgenabschätzung relevant sind. Hierzu gehören unter anderem die Zeitplanung und Überprüfung der Datenschutzfolgenabschätzung, das Erstellen der einschlägigen Dokumentation, die Bestimmung der Personen, die innerhalb der Organisation für die Unterstützung des Prozesses der Datenschutzfolgenabschätzungen zuständig sind, die Identifizierung der Bedingungen, die in Zukunft eine Überprüfung der Datenschutzfolgenabschätzungen auslösen könnten sowie Beratungen mit den Beteiligten.

Der Prozess der Datenschutzfolgenabschätzung ist zweiphasig:

[3] http://www.enisa.europa.eu/media/news-items/enisa-opinion-on-pia, ENISA Opinion on *the Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 31. März 2010. [deutsche Fassung liegt nicht vor – Anm. d. Ü.]

I. eine Vor-Bewertungsphase, die eine RFID-Anwendung nach einer auf einem Entscheidungsbaum basierenden Vier-Stufen-Skala klassifiziert. Anhand des Ergebnisses dieser Bewertung kann festgelegt werden, ob eine Datenschutzfolgenabschätzung erforderlich ist oder nicht und ob diese in „großem" oder „kleinem Umfang" erfolgt. Anwendungen, die RFID-Tags nutzen, die vermutlich von Personen mitgeführt werden, machen zumindest eine „Datenschutzfolgenabschätzung in kleinem Umfang" (Stufe 1) erforderlich, während Anwendungen, die die personenbezogenen Daten weiter verarbeiten, eine „Datenschutzfolgenabschätzung in großem Umfang" (Stufe 2 und 3) erfordern. Umgekehrt unterliegen Anwendungen, die keine Tags nutzen, die vermutlich von Personen mitgeführt werden und die die personenbezogenen Daten nicht weiter verarbeiten, keiner Datenschutzfolgenabschätzung.

II. eine Risikobewertungsphase, die aus vier Hauptschritten besteht:
    1) Charakterisierung der Anwendung (Datentypen, Datenfluss, RFID-Technologie, Datenspeicherung, Datenübermittlung usw.)
    2) Identifizierung der Risiken für personenbezogene Daten, indem Bedrohungen, ihre Wahrscheinlichkeit und ihre Auswirkung auf den Datenschutz sowie die Einhaltung der europäischen Rechtsvorschriften bewertet werden
    3) Identifizierung und Empfehlung von Kontrollen als Reaktion auf die zuvor identifizierten Risiken
    4) Dokumentation der Ergebnisse der Datenschutzfolgenabschätzung, Abfassen einer Entschließung bezüglich der Bedingungen für die Umsetzung der geprüften RFID-Anwendung sowie Informationen zu den Restrisiken.

Jeder Schritt der Risikobewertungsphase wird zusätzlich durch Elemente unterstützt, die in den Anhängen des überarbeiteten Rahmens niedergelegt sind und die dem Prüfer durch Folgendes als Richtlinie dienen sollen:

- eine Vorlage zur Beschreibung der Hauptmerkmale der RFID-Anwendung
- eine Liste von neun Datenschutzzielen für RFID-Anwendungen, die von der Richtlinie 95/46/EG abgeleitet wurden
- eine Liste typischer Datenschutzrisiken mit Beschreibungen und Beispielen
- eine Liste mit Beispielen für Kontrollen und abschwächende Maßnahmen, die als Reaktion auf die zuvor identifizierten Risiken verwendet werden können.

Das Ergebnis der Datenschutzfolgenabschätzungen wird von dem RFID-Anwendungsbetreiber formell in einem Datenschutzfolgenabschätzungsbericht zusammengefasst, der die RFID-Anwendung beschreibt und die Einzelheiten der vorgenannten vier Risikobewertungsschritte dokumentiert.

2 Analyse

Die Datenschutzgruppe erkennt die umfangreiche Arbeit an, die von Industrieverbänden, Fachleuten, Akademikern und einzelnen Unternehmen in den vergangenen Monaten für die Erstellung eines überarbeiteten Rahmens geleistet wurde. Die Autoren des Rahmens nutzten die Gelegenheit der Überarbeitung nicht nur dazu, auf die von der Datenschutzgruppe hervorgehobenen Bedenken näher einzugehen, sondern auch dazu, den Aufbau zu

verdeutlichen und stärkere Richtlinien für die Anwendungsbetreiber vorzulegen, die diesen Rahmen umsetzen.

Die Datenschutzgruppe stellt fest, dass der überarbeitete Rahmen auf einem Risikobewertungskonzept beruht und betont erneut, dass dies ein grundlegendes Element jedes Rahmens für Datenschutzfolgenabschätzungen ist.

Die Datenschutzgruppe begrüßt auch die ausdrückliche Einbeziehung eines Konsultationsprozesses mit den Beteiligten als Teil der internen Verfahren, die zur Unterstützung der Durchführung einer Datenschutzfolgenabschätzung benötigt werden.

Die vorgeschlagene Risikobewertungsmethode wird vor der Bewertung durch einen Entscheidungsbaum eingeleitet, der die RFID-Anwendungen in vier Stufen klassifiziert. Die Datenschutzgruppe merkt an, dass der vorgeschlagene Entscheidungsbaum in Bezug auf die Frage unklar ist, was in einer RFID-Anwendung als personenbezogene Daten zu betrachten ist und was nicht. Wenn ein Tag mit einer eindeutigen Kennung dazu bestimmt ist, von einer Person mitgeführt zu werden, sollte die Tag-Kennung als personenbezogene Daten angesehen werden, wie dies bereits zuvor in der Stellungnahme 5/2010 betont wurde. Wenn der Tag von einer Person mitgeführt werden soll, würde also in den meisten Szenarien eine Anwendung der Stufe 2 und nicht der Stufe 1 vorliegen, wie es der Rahmen vorsieht. Dennoch begrüßt die Datenschutzgruppe die Tatsache, dass der überarbeitete Rahmen von RFID-Anwendungsbetreibern eindeutig die Durchführung einer Datenschutzfolgenabschätzung fordert, sobald Tags von Personen mitgeführt werden.

Wie in mehreren früheren Stellungnahmen[4] dargelegt, *„ergibt sich“* eines der größten Datenschutzbedenken im Zusammenhang mit der RFID-Technik *„aus dem Einsatz von RFID zur Verfolgung („Tracking“) einzelner Personen und zur Gewinnung personenbezogener Daten“*. Obwohl ein RFID-Anwendungsbetreiber bei der Einführung einer RFID-Anwendung ein solches Ziel nicht unbedingt im Sinn hat, muss auch das Risiko bedacht werden, dass ein Dritter Tags für solche unbeabsichtigten Zwecke nutzen könnte. Der überarbeitete Rahmen fordert jetzt von RFID-Anwendungsbetreibern eindeutig eine Bewertung der Risiken, die bei der Nutzung von Tags außerhalb des Anwendungsbereichs einer RFID-Anwendung entstehen können und/oder wenn sie von Personen mitgeführt werden.

Diesen Bedenken wurde im Bereich des Einzelhandels besondere Aufmerksamkeit zuteil. Es wird befürchtet, dass dort mit RFID-Tags versehene Gegenstände, die von Personen mitgeführt werden, von Einzelhändlern oder Dritten zum Tracking oder zur Erstellung von Profilen missbraucht werden könnten. Die Europäische Kommission geht in der Empfehlung auf diese Bedenken ein, indem sie festlegt, dass die Tags am Verkaufsort zu deaktivieren sind, sofern der Verbraucher nicht in voller Kenntnis der Sachlage der weiteren Betriebsfähigkeit des RFID-Tags zustimmt. Dieselbe Empfehlung gestattet eine Ausnahme zu diesem Deaktivierungsgrundsatz, wenn die Datenschutzfolgenabschätzung ergibt, dass die weitere Betriebsfähigkeit von Tags nach dem Verlassen des Verkaufsorts *wahrscheinlich keine Bedrohung für die Privatsphäre oder den Schutz personenbezogener Daten darstellt.* Die Datenschutzarbeitsgruppe merkt an, dass ein wie in dem Rahmen vorgeschlagener Risikomanagementansatz ein wesentliches Instrument für einen RFID-Anwendungsbetreiber bei der Bewertung der Risiken ist, die mit der Übernahme der Verantwortung verbunden sind, die Tags nach Verlassen des Kauforts betriebsbereit zu halten.

[4] Siehe beispielsweise die Stellungnahmen 5/2010 (WP 175) und WP 105, *„Arbeitspapier zu Datenschutzfragen im Zusammenhang mit der RFID-Technik“*, 19. Januar 2005.

Bei der Durchführung einer Datenschutzfolgenabschätzung wird ein entsprechender Bericht erstellt, der der zuständigen Behörde spätestens sechs Wochen vor der Einführung der RFID-Anwendung zur Verfügung gestellt werden sollte. Die Datenschutzgruppe möchte auch betonen, dass der RFID-Anwendungsbetreiber bei der Durchführung einer Datenschutzfolgenabschätzung dazu verpflichtet ist, *für jede der Anwendungen klare, genaue und einfache Informationen zu verfassen und zu veröffentlichen* (wie in Punkt 7 der Empfehlung beschrieben). Diese Informationen sollten insbesondere eine *Zusammenfassung der Datenschutzfolgenabschätzung* umfassen.

Anfänglich wird dieser Rahmen bei seiner Umsetzung in konkrete RFID-Anwendungen vermutlich angepasst werden müssen. Diese Anpassungen können nur durch die Erfahrungen und Rückmeldungen aller Beteiligten, einschließlich der Branche, der Verbraucher, der Datenschutzbehörden und der ENISA in voller Kenntnis der Sachlage erfolgen. Dies wird wahrscheinlich insbesondere in Bezug auf die Unterscheidung zwischen einer Datenschutzfolgenabschätzung „im großen Rahmen“ und „im kleinen Rahmen“ der Fall sein, wie sie in dem überarbeiteten Rahmen definiert sind. Darüber hinaus wird gemäß der Empfehlung von der Europäischen Kommission erwartet, dass sie einen *Bericht über die Umsetzung der Empfehlung, ihre Wirksamkeit und ihre Auswirkung auf die Anwendungsbetreiber und die Verbraucher* insbesondere in Bezug auf die den Einzelhandelssektor betreffenden Maßnahmen vorlegt. Dieser Bericht soll drei Jahre nach Veröffentlichung der Empfehlung vorgelegt werden, also im Mai 2012. In Anbetracht der Tatsache, dass es möglicherweise sechs Monate dauern kann, bis der Rahmen seine volle Wirkung entfaltet, wäre es jedoch für alle Beteiligten von Vorteil, wenn eine solche Bewertung später durchgeführt werden würde. Deshalb würde die Datenschutzgruppe der Europäischen Kommission empfehlen, den vorgeschlagenen Bericht entweder zu verschieben oder zu einem späteren Zeitpunkt zu ergänzen, der auf drei Jahre nach der Veröffentlichung dieser Stellungnahme festgesetzt wird.

3 Fazit

Die Datenschutzgruppe befürwortet den überarbeiteten Rahmen, der am 12. Januar 2011 vorgelegt wurde. Dieser Rahmen tritt spätestens sechs Monate nach der Veröffentlichung dieser Stellungnahme in Kraft.

Eine Datenschutzfolgenabschätzung ist ein Instrument, mit dem der „eingebaute Datenschutz“ (privacy by design), eine bessere Informierung des Einzelnen sowie Transparenz und der Dialog mit den zuständigen Behörden gefördert werden sollen. Da einige RFID-Anwendungen in mehreren Mitgliedstaaten umgesetzt werden, ist es wichtig, dass die Berichte zu Datenschutzfolgenabschätzungen übersetzt und den zuständigen Behörden in der Sprache ihres Landes zur Verfügung gestellt werden.

Die Datenschutzgruppe wird auch weiterhin den Dialog mit der Branche unterstützen, damit Verbesserungen und Klärungen in Bezug auf den Aufbau und die Umsetzung des Rahmens für Datenschutzfolgenabschätzungen für RFID-Anwendungen durch die Erfahrungen und die Rückmeldungen aller Beteiligten in voller Kenntnis der Sachlage durchgeführt werden können.