

Privacy in RFID Anwendungen

RFID Datenschutz Folgeabschätzung

Ein Modell auch für andere technologiebasierte Anwendungen?

Bei RFID geht der Schutz der Privatsphäre künftig als ein Freigabe-Kriterium in jedes Anwendungsprojekt ein. In einer Selbstverpflichtung vom April diesen Jahres hat die Wirtschaft gegenüber der EU-Kommission erklärt, künftig für jedes Betriebsprojekt einer RFID Anwendung eine sogenannte Datenschutz Folgeabschätzung (DSFA) durchzuführen.

Als Industrie und Handel Ende 2005 mit dem „Internet der Dinge“ eine Kampagne zur Ablösung des Barcodes durch die Radiofrequenz – Identifikationstechnologie RFID begannen, beobachtete die Europäische Kommission diese Entwicklung mit Sorge. Insbesondere die Möglichkeiten der unbemerkten Auslesung und hiermit einhergehender Profilbildung, ließ die Kommission schließlich tätig werden. Zur Abwendung einer gesetzlichen Festlegung bot sie der Industrie 2009ⁱ an, im Rahmen der Selbstregulierung für einen angemessenen Datenschutz in RFID-Anwendungen Sorge zu tragen. Hierzu sollte ein Verfahren vorgeschlagen und abgestimmt werden, das am 6. April 2011 formell angenommen wurde.

Dieses Verfahren nennt sich im Originaltext „Privacy and Data Protection Impact Assessment Framework for RFID Applications“ⁱⁱ, auf deutsch Rahmenwerk zur Datenschutz Folgen-Abschätzung (DSFA) für RFID Anwendungen.

Es ist entwickelt worden, um den Betreiber einer RFID Anwendung bei der Aufdeckung von Datenschutz-Risiken in seiner Anwendung zu helfen, deren Eintrittswahrscheinlichkeit zu ermitteln und zu dokumentieren, wie diesen Risiken begegnet wird. Art und Umfang der zu treffenden Vorkehrungen können dabei von Anwendung zu Anwendung stark variieren.

Im Grunde ist die Datenschutz Folgeabschätzung mit der in Deutschland heute schon für bestimmte, sensible Anwendungen vorgeschriebenen Vorabkontrolle vergleichbar. Da es hierfür nur sehr wenige, teils sehr abstrakte Anleitungen gab, wurde sich bei der Festlegung des Verfahrens der DSFA vor allem am Beispiel des vom britischen Datenschutzbeauftragten herausgegebenen PIA Handbuchsⁱⁱⁱ orientiert

Spätestens ab September 2011 muss jedes Anwendungsprojekt für RFID vor seiner Inbetriebnahme eine DSFA durchgeführt und deren Ergebnis schriftlich dokumentiert haben. Inzwischen sind neue Stimmen vernehmbar, die sich eine DSFA auch für andere, sensible M2M Technologien als verpflichtend vorstellen können.

Wer soll wann eine Datenschutz Folgeabschätzung durchführen?

Grundsätzlich sollen alle Unternehmen und Behörden, die in Europa eine RFID Anwendung einzusetzen planen, eine DSFA durchführen, sofern von dieser Anwendung eine relevante Risikoeinstufung für den Datenschutz erreicht wird. Bei nur unerheblichen Risiken kann auf die DSFA verzichtet werden.

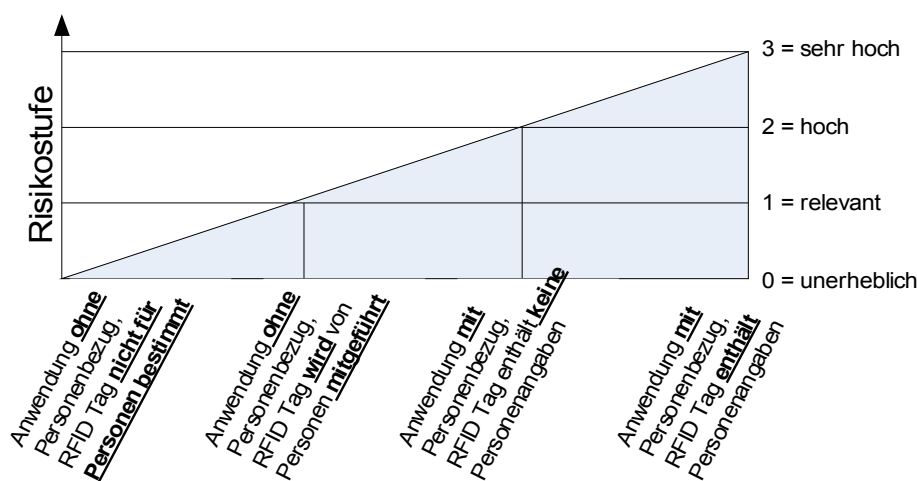


Abbildung 1: Risikostufen

Bevor Sie also in die Detailarbeit einsteigen, sollten Sie in einer Ausgangsanalyse feststellen lassen, ob für die von Ihnen geplante Anwendung eine DSFA erforderlich ist, und in welchem Umfang. Hierbei hilft Ihnen ein Entscheidungsbaum.

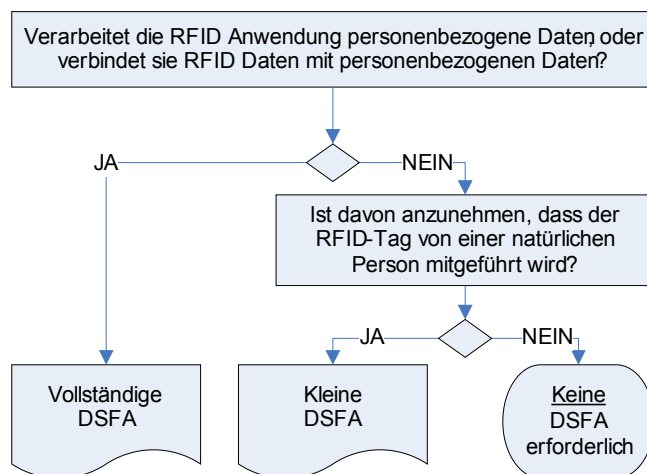


Abbildung 2: Entscheidungsbaum der Ausgangsanalyse

Ergibt die Ausgangsanalyse, dass Sie eine DSFA benötigen, sollten Sie sich als nächstes um die Rahmenbedingungen kümmern.

Die DSFA – idealerweise ein Unterprojekt im Projekt

Das verabschiedete Rahmenwerk stellt einige Anforderungen an die Datenschutz Folgeabschätzung, denen man am besten in einem eigenen Unterprojekt zum Entwicklungs- und Einführungsprojekt der RFID Anwendung, oder alternativ in einem daneben aufgestellten Projekt gerecht werden kann.

Zunächst ist die DSFA terminlich so anzuordnen, dass ausreichend Zeit bleibt, um notwendige Anpassungen vorzunehmen, und damit der Report spätestens 6 Wochen vor der Betriebsfertigstellung fertiggestellt und abgenommen ist.

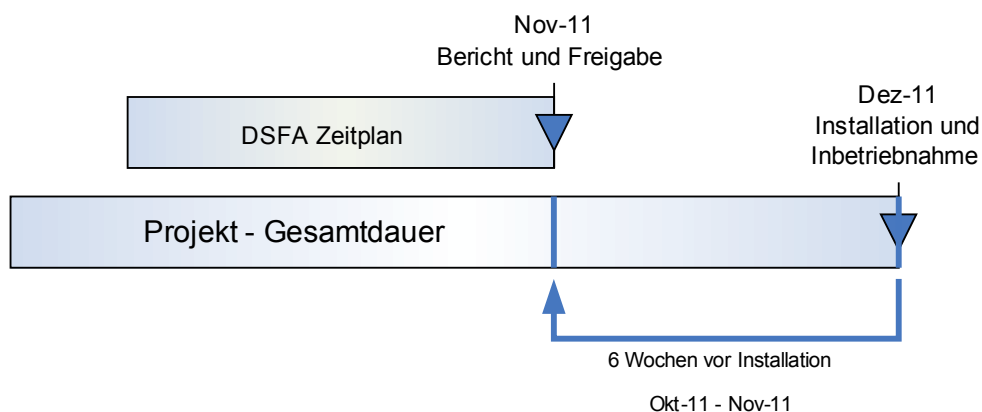


Abbildung 3: Auszug Projektplan exemplarisch

Wie auch in anderen Projektverfahren üblich, sollen die Verantwortlichkeiten und Rollen bei der Durchführung und Abnahme der DSFA benannt sein. Auch müssen die Bewertungskriterien, wann die Anwendung als betriebsbereit im Sinne der DSFA anzusehen ist, vorab schriftlich festgelegt werden.

Dabei wird erwartet, dass Sie Stakeholdern in die Analyse angemessen einbeziehen. Innerbetrieblich sollte neben dem betrieblichen Datenschutzbeauftragten, der schon auf Grund seiner gesetzlichen Aufgaben einzubeziehen ist, auch Projektteilnehmer aus Technologie, Marketing und anderen Disziplinen teilnehmen.

Außerbetrieblich kann im Einzelfall die Einbeziehung von Vertretern betroffener Personengruppen wie Betriebsrat oder Kundenbeirat und Verbraucherschutz als erforderlich angesehen werden.

Ablauf und Inhalt einer DSFA

Die DSFA ist ein Verfahren in 4 Schritten.

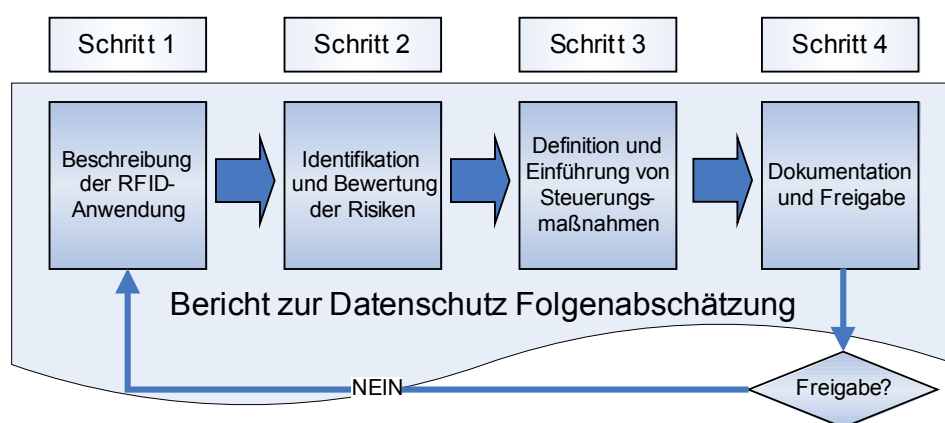


Abbildung 4: Die 4 Schritte einer Datenschutz-Folgenabschätzung

Schritt 1: Beschreibung der RFID-Anwendung

In diesem ersten Schritt wird Zweck und Aufbau der RFID Anwendung dargelegt. Hier soll ein umfassendes Bild der Lösung, ihrer Umgebung und ihrer Systemgrenzen gezeichnet

werden. Insbesondere die Datenflüsse sind detailliert zu beschreiben, hierfür werden Flussdiagramme empfohlen. Auch die Datenstrukturen sind zu dokumentieren, damit mögliche Verknüpfungen erkannt werden können.

Weiterhin soll die aktuelle Aufgabenstellung, aber auch die langfristige Fort-Entwicklung der Anwendung beschrieben werden. Schließlich sollen die Beteiligten an der Informationserfassung und Verarbeitung, sowie die Anwender- und Nutzerkreise benannt werden. Auch Übergänge zu externen Systemen sind konkret darzustellen.

Schritt 2: Identifikation und Bewertung der Datenschutz-Risiken

In diesem Schritt sollen zunächst die Szenarien festgestellt werden, unter denen personenbezogene Daten im Rahmen der vorgesehenen RFID-Anwendung gefährdet oder kompromittiert werden. Hierzu dient die EU Datenschutz Richtlinie^{iv} bzw. das Bundesdatenschutzgesetz^v als Maßstab.

Dabei ist zu beachten, dass Risiken aus der bestimmungsgemäß wie auch einer missbräuchlich erfolgenden Verwendung entstehen können. Ein besonderes Augenmerk legte die EU Kommission zum Beispiel auf RFID-Tags innerhalb der RFID-Anwendung, die noch betriebsbereit sind, während sie schon in den Besitz von Verbrauchern übergegangen sind.

Eine Liste möglicher Risiken für den Datenschutz findet sich im Anhang des DSFA Rahmenwerks. Sie kann als Leitfaden für die systematische Identifizierung von potenziellen Risiken dienen, sollte jedoch auf Vollständigkeit überprüft werden.

Nachdem die Risiken identifiziert sind, soll eine Bewertung der Risiken aus Sicht des Datenschutzes erfolgen. Hierfür soll

1. die Bedeutung der Gefahr und der Wahrscheinlichkeit des Auftretens, sowie
2. das Ausmaß der Auswirkungen bei Auftreten

ermittelt werden. Dies soll mit angemessenem Aufwand und unter Anlegen vernünftiger Bedingungen erfolgen.

Die sich daraus ergebenden Risiken können dann als gering, mittel oder hoch eingestuft werden. Aus den Risiko-Szenarien sind geeignete Schutzziele abzuleiten.

Schritt 3: Definition und Einführung von Steuerungsmaßnahmen

In diesem Schritt soll herausgearbeitet werden, welche bestehenden oder zusätzlichen Steuerungsmaßnahmen umgesetzt werden müssen, damit Eintrittsmöglichkeit und Auswirkung der identifizierten Risiken für den Datenschutz minimiert, abgeschwächt oder verhindert werden.

Diese Steuerungsmaßnahmen können in technischen wie auch organisatorischen Regelungen bestehen. Sie werden ihrem Charakter nach in vorbeugende oder aufdeckende Maßnahmen unterschieden. Vorbeugende Maßnahmen verhindern den Schadenseintritt, aufdeckende Maßnahmen informieren über gerade stattfindende oder bereits eingetretene schädigende Umstände.

Auch der bewusste Verzicht auf Risiko-ermöglichende Umstände kann eine Steuerungsmaßnahme darstellen. So kann eine als realistisch eingestufte Gefährdung z.B. vermieden werden, wenn im gefährdeten Bereich keine RFID Lesegeräte installiert werden.

Im Ergebnis dieses Schrittes ist zu jedem der ermittelten Risiken und den damit verbundenen Risiko Bewertungen eine Entscheidung zu treffen, welche der ermittelten Steuerungsmaßnahmen diesen wirksam begegnen soll und damit umgesetzt werden müssen. In der Dokumentation zur DSFA soll auch erläutert sein, wie die Steuerungsmaßnahmen sich auf die spezifischen Risiken beziehen, und wie deren Anwendung zu einem akzeptablen Risikolevel führen soll.

Auch für die Beschreibung von Steuerungsmaßnahmen finden sich Beispiele im Anhang zum DSFA Rahmenwerk.

Schritt 4: Dokumentation und Freigabe

Sobald die Risikobewertung mit den beschlossenen Steuerungsmaßnahmen abgeschlossen wurde, ist die DSFA in einem Bericht zu dokumentieren. Der Bericht umfasst die Beschreibung der Anwendung aus Schritt 1, sowie die Dokumentation von Ablauf und Ergebnissen der Schritte 2 und 3. Er wird dabei auch sensible, gegebenenfalls vertrauliche Unternehmens- und Produkt-Informationen enthalten.

Dieser Bericht ist dem vor Beginn der DSFA namentlich benannten Verantwortlichen zur Freigabe vorzulegen. Die Freigabe hat schriftlich zu erfolgen. Erst nach erfolgter Freigabe soll die Anwendung in Betrieb gehen.

Wird die Freigabe nicht erteilt, sind im Rahmen eines erneuten Durchlaufs der Schritte 1 bis 4 weitere Überlegungen anzustellen, bis das dokumentierte Ergebnis eine Freigabe für den Betrieb der Anwendung rechtfertigen kann.

Der unterzeichnete DSFA Bericht, mit dem unterschriebenen Freigabebeschluss ist dann bei der Unternehmen für den Datenschutz zuständigen Stelle aufzubewahren, und den Aufsichtsbehörden bei Verlangen vorzulegen.

Nutzung von Vorlagen – Vorteile und Grenzen

Das Rahmenwerk nimmt in einigen Passagen Bezug auf Vorlagen, die bei der Durchführung einer DSFA hilfreich sein können. Für Anwendungen des E-Ticketing im Personenverkehr und auf Veranstaltungen, Handelslogistik und den elektronischen Mitarbeiterausweis hat das Bundesamt für Sicherheit in der Informationstechnik BSI gemeinsam mit der Industrie technische Richtlinien^{vi} zu RFID erstellt, die in Teilen Ihrer DSFA als Vorlagen dienen dürfen.

Da diese technischen Richtlinien vorrangig auf die Datensicherheit abstellen, lassen sie eine Reihe der Grundfragestellungen zum Datenschutz wie

- der Berechtigungsgrundlage für die Verarbeitung,
- der Datensparsamkeit und

- der Transparenz

außer acht. Sie sollten daher nicht kritiklos und insbesondere nicht ohne eine Ergänzung dieser Aspekte angewendet werden.

Fazit

Mit der Datenschutz Folgeabschätzung kommt ein komplexes Analyseverfahren auf Anwendungsbetreiber zu, dass auch ohne gesetzliche Vorgabe die anzuwenden Compliance Regeln verbindlich erweitert. Mit einer Ausweitung auf andere Anwendungen außer RFID darf wohl mittelfristig gerechnet werden. Leider hat es die Industrie versäumt, Anhaltspunkte dafür zu geben wie sich der Beschreibungsumfang einer „Vollständigen DSFA“ von dem einer „Kleinen DSFA“ unterscheidet. Dies wird sich daher erst in der Praxis zeigen müssen.

- i Quelle: http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf
- ii Quelle: http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp180_annex_en.pdf
- iii Quelle: http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html
- iv Quelle: <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:DE:HTML>
- v Quelle: http://bundesrecht.juris.de/bundesrecht/bdsg_1990/gesamt.pdf
- vi Quelle: https://www.bsi.bund.de/ContentBSI/Publikationen/TechnischeRichtlinien/tr03126/index_hm.html