EU Privacy Impact Assessment:

Quadro per la valutazione dell'impatto delle applicazioni RFID sulla protezione della vita privata e dei dati

11 Febbraio 2011

H&S Custom S.r.l. – Via Novara 349 – 28078 Romagnano Sesia (NO) - Italy
tel: +39 0163 818038 fax: +39 0163 818149 email: info@hscustom.it

Dal 2003 HSC propone soluzioni RFID e Wireless complete e chiavi in mano per l'identificazione e la gestione di merci e persone e per la raccolta e la comunicazione delle informazioni dal punto in cui esse si originano verso i sistemi che le utilizzano.

HSC ascolta le idee innovative dei propri clienti e li aiuta a trasformarle in realtà contribuendo a tutti i livelli, dalla definizione di un "concept", alla realizzazione di prototipi, con la selezione delle tecnologie, degli apparati, al disegno dei tag, fino alla messa in opera della soluzione funzionante.

CONTESTO

Il 6 aprile 2011 la Commissione europea ha sottoscritto un accordo volontario con le imprese, la società civile, l'ENISA (Agenzia europea per la sicurezza delle reti e dell'informazione), gli organismi garanti della privacy e della protezione dei dati in Europa, per fissare orientamenti destinati alle imprese europee nell'intento che le implicazioni poste dalle etichette intelligenti (dispositivi di identificazione a radiofrequenza - RFID) sul piano della protezione dei dati siano trattate prima della loro commercializzazione.

L'ACCORDO

L'accordo stabilisce che le imprese svolgano una valutazione globale dei rischi per la vita privata e adottino misure per far fronte ai rischi individuati prima che una nuova applicazione contenente un tag RFID sia introdotta sul mercato. Tra gli eventuali rischi vi sono gli effetti che potrebbero avere sulla sfera privata i collegamenti tra i dati raccolti e trasmessi ed altri dati. È questo un aspetto particolarmente importante nel caso di dati personali sensibili, come quelli biometrici, sanitari o inerenti all'identità.

IL DOCUMENTO

Il 12 maggio 2009 la Commissione europea ha emesso una raccomandazione sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza* In tale atto, la Commissione ha stabilito che dovesse essere sottoposto all'approvazione del Gruppo di lavoro "articolo 29" un quadro, predisposto dall'industria, per la valutazione dell'impatto delle applicazioni RFID sulla protezione della vita privata e dei dati. Tali valutazioni sono comunemente note come valutazioni dell'impatto sulla vita privata o PIA - Privacy Impact Assessment. Il quadro qui proposto ottempera a detto obbligo. Il documento elaborato dalla Commissione Europea, qui proposto nella sua versione integrale, tradotta in italiano, è applicabile a tutti i settori economici che utilizzano le etichette intelligenti e stabilisce per la prima volta in Europa una metodologia chiara per valutare e attenuare i rischi posti dalle etichette intelligenti per la vita privata. In particolare questo quadro non soltanto darà certezza del diritto alle imprese, garantendo loro che l'uso dell'RFID sia compatibile con la legislazione europea sulla privacy, ma offrirà anche una maggiore garanzia di protezione ai cittadini e ai consumatori europei.

* COMMISSION RECOMMENDATION of 12.5.2009 on the implementation of privacy and data protection principles in applications supported by radio-frequency identification.
http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid2009.pdf

L'accordo volontario "Privacy and Data Protection Impact Assessment (PIA) Framework for RFID Applications", siglato il 6 aprile 2011 dalla Commissione Europea, dai i rappresentanti dell'industria e della società civile, l' ENISA (European Network and Information Security Agency) e dal Gruppo europeo dei Garanti della Privacy stabilisce finalmente un punto fermo nel confuso quadro normativo relativo all'utilizzo dei tag RFID.

L'obiettivo dell'accordo, qui proposto nella sua forma integrale in italiano, è di garantire la privacy del consumatore prima dell'introduzione massiva dei tag RFID nei diversi mercati, in modo pragmatico e realistico. Indirizzare le preoccupazioni relative alla violazione del diritto alla privacy ed alla protezione dei dati personali con una valutazione preventiva dell'impatto della tecnologia sulla vita privata è il primo passo verso la eliminazione della diffidenza che circonda il mondo dell'RFID, in un contesto che nel 2011 prevede la diffusione di oltre 2.8 miliardi di tag a livello mondiale, un terzo dei quali in Europa ed una proiezione di una diffusione di oltre 50 miliardi di tag nel 2020.

H&S Custom, ha adottato da tempo processi e procedure di valutazione dell'impatto sulla privacy in Security of Things, il suo approccio metodologico per la sicurezza delle cose e delle persone che interagiscono con esse. E' con piacere che vediamo comprese nel framework PIA molte procedure da noi già adottate per garantire la protezione della privacy del consumatore e del cittadino.

Ci auspichiamo che il framework possa costituire una valida guida alla implementazione dei progetti RFID europei e globali e che, con la trasparenza e l'informazione abbatta le residue barriere di diffidenza del consumatore verso una tecnologia che può semplificargli e migliorargli la qualità della vita.

Romagnano, 12 aprile 2011

Renzo Ottina
Amministratore Delegato
di H&S Custom

IP/11/

Brussels, 6th April 2011

Digital Agenda: new guidelines to address privacy concerns over use of smart tags

Today the European Commission has signed a voluntary agreement with industry, civil society, ENISA (European Network and Information Security Agency) and privacy and data protection watchdogs in Europe to establish guidelines for all companies in Europe to address the data protection implications of smart tags (Radio Frequency Identification Devices – RFID) prior to placing them on the market. The use of such smart tags is expanding enormously (around 1 billion in Europe in 2011) but there are widespread concerns about their privacy implications. RFIDs can be found in many objects from bus passes to smart cards that pay motorway tolls. Microelectronic devices can process data automatically from RFID tags when brought close to 'readers' that activate them, pick up their radio signal and exchange data with them. Today's agreement forms part of the implementation of a Commission Recommendation adopted in 2009 (see IP/09/740) that inter alia indicates that when consumers buy products with smart tags, they should be deactivated automatically, immediately and free-of-charge unless the consumer agrees explicitly that they are not.

Neelie Kroes, European Commission Vice-President for the Digital Agenda said "I warmly welcome today's milestone agreement to put consumers' privacy at the centre of smart tag technology and to make sure privacy concerns are addressed before products are placed on the market. I'm pleased that industry is working with consumers, privacy watchdogs and others to address legitimate concerns over data privacy and security related to the use of these smart tags. This sets a good example for other industries and technologies to address privacy concerns in Europe in a practical way".

The agreement signed today, "Privacy and Data Protection Impact Assessment (PIA) Framework for RFID Applications", aims to ensure consumers' privacy before RFID tags are introduced on a massive scale (see IP/09/952). Around 2.8 billion smart tags are predicted to be sold in 2011, with about one third of these in Europe. But industry estimates that there could be up to 50 billion connected
electronic devices by 2020.

RFID tags in devices such as mobile phones, computers, fridges, e-books and cars bring many potential advantages for businesses, public services and consumer products. Examples include improving product reliability, energy efficiency and recycling processes, paying road tolls without having to stop at toll booths, cutting time spent waiting for luggage at the airport and lowering the environmental footprint of products and services.

However RFID tags also raise potential privacy, security and data protection risks.
This includes the possibility of a third party accessing your personal data (e.g. concerning your location) without your permission.

For example, many drivers pay tolls electronically to use roads, airport and car parks based on data collected through RFID tags on their car windscreens. Unless preventative action is taken, RFID readers found outside those specific locations could unwittingly lead to privacy leaks revealing the location of the vehicle. Many hospitals use RFID tags to track inventory and identify patients. While this technology can improve the overall quality of healthcare, the benefits must be balanced with privacy and security concerns.

Comprehensive assessment of privacy risks

Under the agreement, companies will carry out a comprehensive assessment of privacy risks and take measures to address the risks identified before a new smart tag application is introduced onto the market. This will include the potential impact on privacy of links between the data collected and transmitted and other data. This is particularly important in the case of sensitive personal data such as biometric, health or identity data.

The PIA Framework establishes for the first time in Europe a clear methodology to assess and mitigate the privacy risks of smart tags that can be applied by all industry sectors that use smart tags (for example, transport, logistics, the retail trade, ticketing, security and health care).

In particular, the PIA framework will not only give companies legal certainty that the use of their tags is compatible with European privacy legislation but also offer better protection for European citizens and consumers.

Background

In May 2009 all interested stakeholders from industry, standardisation bodies, consumers' organisations, civil society groups, and trade unions, agreed to respect a Recommendation from the European Commission laying out principles for privacy and data protection in the use of smart tags (see IP/09/740). Today's PIA Framework is part of the implementation of the 2009 Recommendation. Information gathered during the PIA framework drafting process will also make a valuable contribution to discussions on the revision of EU rules on Data Protection (see IP/10/1462 and MEMO/10/542) and on how to address the new challenges for personal data protection brought by technological developments.

For more information:

Link to the PIA framework

Digital Agenda website:

http://ec.europa.eu/information_society/digital-agenda/index_en.htm

Follow Neelie Kroes on Twitter:

http://twitter.com/neeliekroeseu

For more information, please contact:

Jonathan Todd: (+ 32-2) 299 41 07 ***jonathan.todd@ec.europa.eu***

Linda Cain: (+ 32-2) 299 90 19 ***linda.cain@ec.europa.eu***

Quadro per la valutazione dell'impatto delle applicazioni RFID sulla protezione della vita privata e dei dati

11 febbraio 2011

INDICE

1. Introduzione....3
1.1. Concetti fondamentali 3
1.2. Procedure interne 4

2. Il processo di valutazione dell'impatto sulla privacy 6
2.1. Fase di analisi iniziale 7
2.2. Fase di valutazione dei rischi 8

3. Disposizioni finali 12

ALLEGATO I – Descrizione della caratterizzazione delle applicazioni RFID 13

ALLEGATO II – Obiettivi della tutela della vita privata 14

ALLEGATO III – Rischi per la vita privata 15
ALLEGATO IV – Esempi di controlli sulle applicazioni RFID e di misure attenuanti....18

Appendice A: Riferimenti 22

Appendice B: Glossario 24

1. Introduzione

Il 12 maggio 2009 la Commissione europea ("la Commissione") ha emesso una raccomandazione sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza ("raccomandazione RFID"). In tale atto, la Commissione ha stabilito che dovesse essere sottoposto all'approvazione del Gruppo di lavoro "articolo 29" un quadro, predisposto dall'industria, per la valutazione dell'impatto delle applicazioni RFID sulla protezione della vita privata e dei dati. Tali valutazioni sono comunemente note come valutazioni dell'impatto sulla vita privata. Il presente quadro per la realizzazione di valutazioni dell'impatto delle applicazioni RFID sulla vita privata ("il quadro") ottempera a detto obbligo.

La conduzione di valutazioni dell'impatto delle applicazioni RFID sulla vita privata presenta numerosi vantaggi. Fra questi, si aiuta il gestore di applicazioni RFID:

- ad assicurare e mantenere il rispetto della normativa e della regolamentazione in materia di protezione della vita privata e dei dati;
- a gestire i rischi dell'applicazione RFID per la propria organizzazione e gli utenti (sia in termini di protezione della vita privata e dei dati, sia dal punto di vista della percezione da parte dei cittadini e della fiducia dei consumatori);
- a offrire al pubblico i vantaggi delle applicazioni RFID, valutando al contempo l'efficacia della tutela della vita privata fin dalla progettazione (privacy by design) già agli stadi iniziali del processo di specificazione o sviluppo.

Il processo di valutazione dell'impatto sulla vita privata si basa su un approccio alla gestione dei rischi per la tutela della vita privata e dei dati incentrato principalmente sull'attuazione della raccomandazione RFID dell'UE e in linea con il quadro giuridico e le migliori pratiche dell'UE.

Il processo in esame è stato studiato per aiutare i gestori di applicazioni RFID a individuare i rischi per la vita privata associati a un'applicazione RFID, a valutarne la probabilità e a documentare le azioni intraprese per contrastarli. Questi effetti (se esistenti) possono presentare differenze significative, a seconda della presenza o meno del trattamento di informazioni personali da parte dell'applicazione RFID. Il quadro fornisce orientamenti ai gestori di applicazioni RFID sui metodi di valutazione dei rischi, ivi comprese misure adeguate per attenuare il probabile effetto sulla protezione dei dati o della vita privata in modo efficace, efficiente e proporzionato.

Infine, il quadro per la valutazione dell'impatto sulla vita privata è sufficientemente generico da poter afferire a tutte le applicazioni RFID, pur consentendo di affrontare le particolarità e le specificità a livello di settore o di tipologia di applicazione.

Il quadro rientra nel contesto delle altre norme sulla garanzia della sicurezza delle informazioni, sulla gestione dei dati e delle norme operative atte a fornire strumenti adeguati di *governance* dei dati per le applicazioni RFID e di altro genere. L'attuale quadro potrebbe essere utilizzato come base di sviluppo per modelli di valutazione dell'impatto sulla privacy specifici per industria, settore e/o applicazione. Come succede per l'attuazione di qualsiasi documento teorico, il quadro potrebbe richiedere chiarimenti sull'applicazione dei concetti utilizzati, nonché orientamenti sulle prassi che dovrebbero essere basati sull'esperienza pratica, in modo da agevolarne l'attuazione.

1.1. Concetti fondamentali

Alcuni concetti fondamentali utilizzati nel quadro necessitano di una definizione. L'***RFID*** è una tecnologia che, utilizzando onde elettromagnetiche per comunicare con etichette RFID, offre la possibilità di leggere i numeri identificativi unici delle etichette RFID ed eventualmente anche altre informazioni ivi contenute. Le ***etichette RFID*** sono in genere di piccole dimensioni e possono assumere varie forme, ma spesso sono costituite da una memoria elettronica leggibile e talvolta scrivibile, nonché da antenne. I ***lettori RFID*** sono utilizzati per leggere le informazioni sulle etichette RFID.

Le ***applicazioni RFID*** elaborano le informazioni ottenute attraverso l'interazione tra etichette e lettori RFID. Tali applicazioni sono gestite da uno o più ***gestori di applicazioni RFID*** e si basano su sistemi di *back-end* all'interno di un'infrastruttura di comunicazione in rete. Se un gestore di applicazioni RFID prende decisioni connesse alla raccolta o all'impiego dei dati personali, il suo ruolo potrebbe essere analogo a quello del responsabile del trattamento dei dati definito nella direttiva 95/46/CE, da intendersi come la persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti della gestione di un'applicazione RFID che ha effetti sulle informazioni personali.

Nel contesto della tecnologia RFID, si applica la tassonomia seguente.

- Una ***valutazione dell'impatto sulla vita privata*** è il processo con cui si compie uno sforzo consapevole e sistematico per valutare gli effetti di una specifica applicazione RFID sulla protezione della vita privata e dei dati al fine di adottare azioni atte a impedire o quanto meno a contenere il più possibile tali effetti.
- Il ***quadro*** individua gli obiettivi delle valutazioni dell'impatto delle applicazioni RFID sulla privacy, le componenti delle applicazioni RFID da considerare nel corso di dette valutazioni nonché la struttura e i contenuti comuni delle relazioni sulle stesse.
- Una ***relazione sulla valutazione dell'impatto sulla vita privata*** è il documento redatto in esito al processo di valutazione messo a disposizione delle autorità competenti. Le informazioni proprietarie e sensibili sotto il profilo della sicurezza possono essere rimosse dalle relazioni in esame prima che queste siano divulgate all'esterno (ad esempio, alle autorità competenti), nella misura in cui tali informazioni non siano specificatamente inerenti alle implicazioni per la protezione della vita privata e dei dati. Le modalità di diffusione delle relazioni (ad esempio, su richiesta o meno) saranno stabilite dagli Stati membri. In particolare, si possono prendere in considerazione l'impiego di categorie particolari di dati, nonché altri fattori come la presenza di un responsabile della protezione dei dati.
- Sulla base del quadro si possono sviluppare ***modelli per la valutazione dell'impatto sulla vita privata*** per fornire, ai fini della conduzione delle valutazioni e della redazione delle relative relazioni, formati specifici per settore o applicazione oppure seguendo altri criteri.

Ai fini del presente quadro, questi e altri termini (quali ***utente*** e ***persona***) sono definiti anche nel glossario riportato nell'appendice B. La terminologia della direttiva 95/46/EC in relazione alla protezione dei dati vi è inclusa.

L'esecuzione delle valutazioni dell'impatto sulla privacy e l'elaborazione di una relazione al riguardo, se del caso, si aggiungono agli altri obblighi cui i gestori di applicazioni RFID possono essere soggetti ai sensi di specifiche disposizioni legislative e regolamentari e di altri accordi vincolanti applicabili.

1.2. Procedure interne

I gestori delle applicazioni RFID devono disporre di proprie procedure interne per agevolare la conduzione delle valutazioni dell'impatto sulla privacy, come ad esempio le seguenti:

- *pianificazione del processo di valutazione dell'impatto sulla vita privata*, in modo che vi sia tempo sufficiente per effettuare eventuali adeguamenti necessari all'applicazione RFID e mettere la relazione sulla valutazione a disposizione delle autorità competenti quanto meno sei settimane prima che l'applicazione sia resa operativa;
- *riesame interno del processo di valutazione dell'impatto sulla vita privata (compresa l'analisi iniziale) e delle relative relazioni* per esaminarne la coerenza con altra documentazione connessa all'applicazione RFID, come la documentazione di sistema, quella di prodotto e gli esempi di imballaggi di prodotti e di applicazione delle etichette RFID. La revisione interna dovrebbe prevedere un ciclo di retroazione per fronteggiare eventuali effetti riscontrati dopo l'attuazione dell'applicazione e per tener conto dei risultati di valutazioni d'impatto precedenti;
- *compilazione dei giustificativi* (in cui possono rientrare i risultati di riesami della sicurezza, la progettazione dei controlli e le copie degli avvisi) a dimostrazione del fatto che il gestore delle applicazioni RFID ha ottemperato a tutti gli obblighi applicabili;
- *determinazione delle persone e/o funzioni all'interno dell'organizzazione responsabili delle azioni pertinenti* durante il processo di valutazione dell'impatto sulla privacy (ad esempio, completamento dell'analisi iniziale e della relazione sulla valutazione, firma della relazione stessa, conservazione dei documenti applicabili, nonché la separazione dei compiti per queste funzioni);
- *predisposizione dei criteri per le modalità di valutazione e documentazione del fatto che l'applicazione in esame è pronta o meno per la diffusione* in linea con il quadro ed eventuali modelli di valutazione dell'impatto sulla vita privata;
- necessità di *considerare/individuare i fattori che potrebbero richiedere una nuova relazione sulla valutazione dell'impatto o una revisione di quella esistente*. Tra i criteri si dovrebbero annoverare: modifiche significative dell'applicazione RFID, come modifiche materiali che si estendono oltre le finalità iniziali (come finalità secondarie); tipologie di informazioni trattate; impieghi delle informazioni che indeboliscono i controlli attuati; violazione inattesa dei dati personali[1] con un impatto determinante e che non rientrava nei rischi residui dell'applicazione individuati nella prima valutazione dell'impatto; definizione di uno scadenziario per la revisione periodica; risposta a riscontri o indagini sostanziali o significativi proveniente dalle parti interessate interne o esterne; oppure modifiche notevoli della tecnologia con implicazioni per la protezione della vita privata e dei dati per l'applicazione RFID in esame. Modifiche sostanziali tali da restringere il campo di applicazione della raccolta o dell'impiego dei dati non danno luogo di per sé alla necessità di una nuova valutazione dell'impatto sulla privacy. Nella durata di vita dell'applicazione RFID si rende necessaria una nuova relazione sulla valutazione dell'impatto o una revisione di quella esistente qualora l'applicazione cambi di livello, come riportato nella sezione sull'analisi iniziale;
- *consultazione delle parti interessate.* I pareri e i riscontri ricevuti dalle parti interessate in relazione all'applicazione RFID in esame andrebbero tenuti in debita considerazione nell'ambito della revisione della valutazione in merito a potenziali preoccupazioni e questioni. Le consultazioni dovrebbero essere adeguate all'entità,

[1] In questo caso è d'applicazione la definizione riportata nella direttiva 2009/136/CE che modifica la direttiva 2002/58 (cfr. pag. 29) http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:IT:PDF

alla portata, alla natura e al livello dell'applicazione RFID. All'interno delle imprese, vengono designati soggetti responsabili di vigilare e assicurare la tutela della privacy a livello di organizzazione o dipartimento. Questi soggetti sono attori essenziali del processo di valutazione poiché sono coinvolti nelle specifiche applicazioni RFID oppure nella loro sorveglianza. Anche gli addetti con competenze in discipline tecniche, di commercializzazione e di altro tipo possono essere attori necessari al processo, a seconda della natura dell'applicazione RFID e della loro relazione con la stessa. I gestori RFID possono disporre di meccanismi di consultazione tramite i quali le parti interessate esterne (che siano persone fisiche, organizzazioni o autorità) possano interagire con loro e fornire riscontri. Laddove opportuno, il gestore RFID dovrebbe utilizzare i meccanismi di consultazione per acquisire informazioni dai gruppi che rappresentano le persone fisiche la cui vita privata risente direttamente delle proposte, ad esempio i dipendenti e i clienti del gestore RFID.

2. Il processo di valutazione dell'impatto sulla vita privata

Scopo del quadro è fornire orientamenti ai gestori delle applicazioni RFID per la conduzione delle valutazioni dell'impatto sulla privacy riguardanti determinate applicazioni RFID, come sollecitato dalla raccomandazione, nonché definire la struttura organizzativa e le categorie dei contenuti comuni delle relazioni in cui si devono documentare i risultati di dette valutazioni. Inoltre, poiché è probabile che molti gestori delle applicazioni RFID all'interno di settori particolari stiano studiando applicazioni RFID identiche o simili, il quadro offre una base per lo sviluppo di modelli di valutazione dell'impatto sulla vita privata per applicazioni o settori dell'industria specifici. Tali modelli possono aiutare questi settori a condurre le valutazioni in questione e a produrre le pertinenti relazioni con maggiore efficienza per le applicazioni simili[2]. Poiché applicazioni RFID comuni potrebbero essere offerte in più Stati membri, il quadro è studiato per armonizzare i requisiti per i gestori delle applicazioni RFID in linea con le disposizioni legislative e regolamentari locali, delle migliori prassi e di altri accordi vincolanti a livello locale.

Il quadro affronta il processo di conduzione delle valutazioni dell'impatto delle applicazioni RFID sulla privacy prima della diffusione di tali applicazioni e precisa il campo di applicazione delle relazioni corrispondenti[3].

I gestori di applicazioni RFID devono predisporre una valutazione dell'impatto sulla vita privata per ciascuna applicazione RFID gestita. In caso di lancio di più applicazioni RFID connesse tra loro (potenzialmente nello stesso contesto o nei medesimi locali) possono redigere un'unica relazione sulla valutazione purché i limiti e le differenze delle applicazioni siano esplicitamente descritti in detta relazione. Se i gestori di applicazioni RFID riutilizzano un'applicazione RFID allo stesso modo per più prodotti, servizi o processi, possono redigere un'unica relazione sulla valutazione per tutti i prodotti, servizi o processi che siano simili (è il caso, ad esempio, di una casa automobilistica che utilizza i medesimi meccanismi antifurto in tutte le autovetture e con le medesime condizioni di servizio). L'esecuzione delle valutazioni dell'impatto e l'elaborazione della pertinente relazione, se del caso, si aggiungono agli altri obblighi cui i gestori di applicazioni RFID possono essere soggetti ai sensi di specifiche disposizioni legislative e regolamentari e di altri accordi vincolanti applicabili.

Il processo di valutazione dell'impatto sulla vita privata si articola in due fasi:

---

2 Andrebbe approfondito il concetto di riconoscimento reciproco o multiplo tra soggetti e settori per la diffusione di applicazioni RFID già verificate.

3 Cfr. il punto 5, lettera a), della raccomandazione della Commissione europea del maggio 2009 sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza, C(2009) 3200 definitivo.

1. **Fase di analisi iniziale**: il gestore di applicazioni RFID seguirà le tappe delineate nella presente sezione per stabilire:

   a) se è necessaria una valutazione dell'impatto sulla vita privata per la sua applicazione RFID e

   b) se occorre condurre una valutazione completa o semplificata.

2. **Fase di valutazione dei rischi**: definisce i criteri e gli elementi delle valutazioni dell'impatto sulla vita privata complete e semplificate.

2.1. Fase di analisi iniziale

Quale presupposto essenziale per la conduzione di una valutazione dell'impatto sulla vita privata per una determinata applicazione, ciascuna organizzazione deve comprendere come svolgere tale processo in funzione della natura e della sensibilità dei dati trattati, della natura e della tipologia del trattamento o della gestione delle informazioni in cui è impegnata, nonché del tipo di applicazione RFID in questione. I criteri di classificazione e le tappe della procedura sono suscettibili di aiutare le organizzazioni che già attuano procedimenti di valutazione dei rischi per la vita privata per altre applicazioni, a situare i loro procedimenti di valutazione rispetto al presente quadro.

Per condurre la valutazione iniziale, un gestore di applicazioni RFID deve percorrere l'albero decisionale illustrato nella figura 1: ciò lo aiuterà a stabilire se e in che misura è necessario condurre una valutazione dell'impatto sulla privacy per l'applicazione RFID in questione.

Il livello che ne risulta nella fase di analisi iniziale serve a determinare il livello di dettaglio necessario nella valutazione dei rischi (ad esempio, se occorre una valutazione completa o semplificata).

Questa analisi iniziale deve essere documentata e messa a disposizione su richiesta delle autorità incaricate della protezione dei dati. Per avere indicazioni sulla documentazione, si rimanda all'allegato I.

Valutazione completa dell'impatto sulla vita privata

Per le applicazioni classificate nel livello 2 o 3 nella fase di analisi iniziale di cui alla sezione 2.1 è necessaria una valutazione completa dell'impatto sulla privacy. Tra gli esempi di applicazioni che richiedono una valutazione completa rientrano quelle che trattano informazioni personali (livello 2) o quelle in cui le etichette RFID contengono dati personali (livello 3). Sebbene entrambi i livelli 2 e 3 diano luogo a una valutazione completa, essi individuano contesti di rischio diversi e, pertanto, saranno soggetti a strategie di attenuazione dei rischi differenti. Ad esempio, le applicazioni di livello 2 possono richiedere controlli per proteggere dati di *back-end* mentre le applicazioni di livello 3 possono richiedere controlli per proteggere dati sia di *back-end* sia delle etichette. L'industria può affinare ulteriormente questi livelli e il modo in cui si ripercuotono sul processo di valutazione dell'impatto sulla privacy con l'acquisizione di ulteriore esperienza. Dal momento che l'applicazione elabora dati personali, è necessaria una valutazione dei rischi molto dettagliata (completa) per assicurare che le misure di attenuazione dei rischi siano trattate in maniera adeguata. Ciò aiuterà il gestore di applicazioni RFID a individuare i rischi coinvolti e a sviluppare controlli appropriati. In questo contesto, i gestori dovrebbero anche considerare se è probabile che le informazioni dell'etichetta RFID siano utilizzate al di là della finalità o del contesto iniziale inteso dalla persona, soprattutto se essa possa essere impiegata per elaborare o collegarsi a dati personali, e se occorra una nuova analisi della valutazione

dell'impatto sulla privacy o se debbano essere attuate ulteriori misure di attenuazione dei rischi.

Valutazione semplificata dell'impatto sulla vita privata

Le valutazioni semplificate dell'impatto sulla privacy seguono il medesimo procedimento di quelle complete ma, in ragione del profilo di rischio minore, rispetto a queste ultime sono più limitate in termini di portata e grado di dettaglio, per quanto concerne sia l'indagine sia la relazione. Le valutazioni semplificate riguardano le applicazioni di livello 1. Benché una valutazione semplificata segua un procedimento analogo a quello delle valutazioni complete, i controlli richiesti e la documentazione corrispondente nella relazione sulla valutazione sono semplificati poiché i rischi insiti in un'applicazione di livello 1 sono inferiori rispetto al livello 2 o 3.

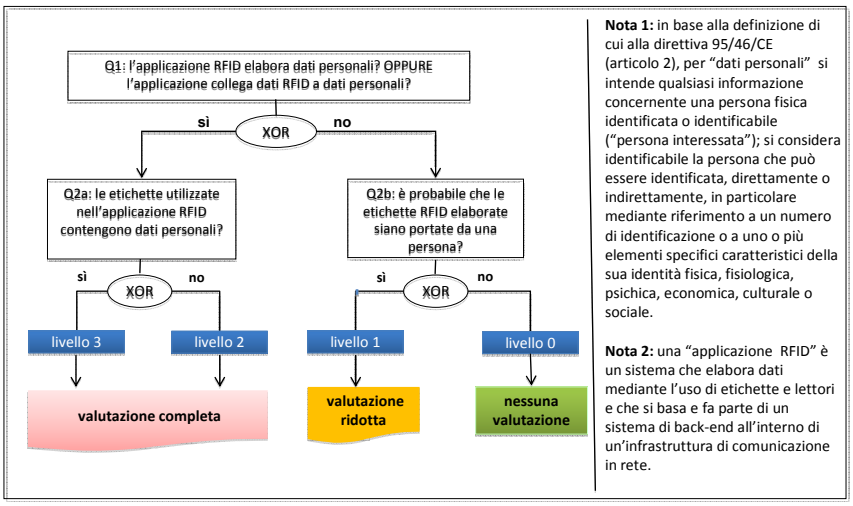


Figura 1 - Albero decisionale teso a determinare se e a che livello di dettaglio condurre una valutazione dell'impatto sulla privacy

2.2. Fase di valutazione dei rischi

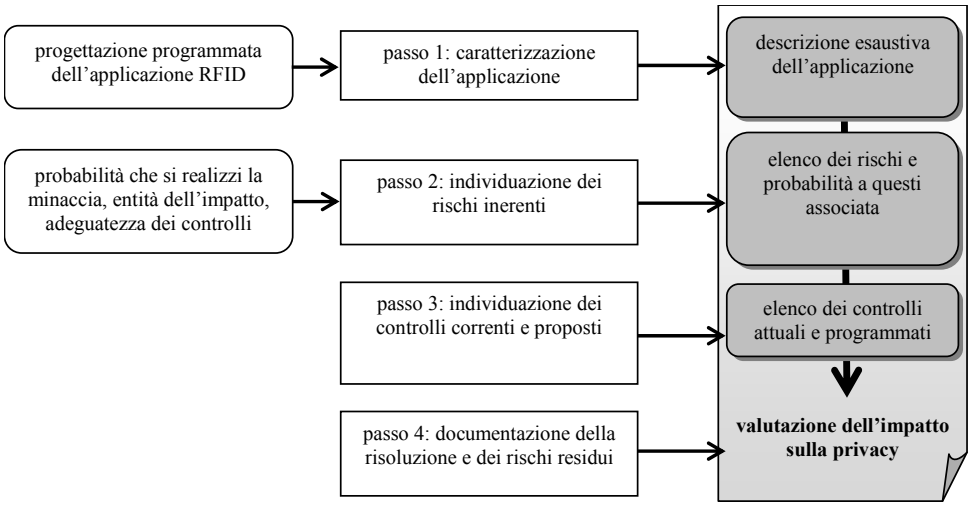
La valutazione dei rischi si propone di individuare i rischi per la vita privata causati da un'applicazione RFID (idealmente in una fase iniziale di sviluppo del sistema) e di documentare come questi rischi siano attenuati *proattivamente* attraverso controlli tecnici e organizzativi. In questo modo la valutazione dell'impatto sulla privacy svolge un ruolo importante nell'osservanza degli obblighi giuridici sulla tutela della vita privata (direttiva 95/46) ed è una misura con cui possiamo giudicare l'efficacia delle procedure di attenuazione dei rischi. Per ottimizzare i tempi e gli investimenti, si raccomanda di condurre questa fase di valutazione dei rischi molto prima di assumere decisioni definitive sull'architettura di un'applicazione RFID in modo che le strategie tecniche di attenuazione dei rischi per la tutela della vita privata siano insite nella progettazione del sistema e non debbano esservi integrate in un momento successivo.

Un processo di valutazione dei rischi considera in genere in primo luogo i rischi di un'applicazione RFID in termini di probabilità che tali rischi si verifichino e di entità delle

relative ripercussioni. I gestori di applicazioni RFID sono invitati a utilizzare gli obiettivi della tutela della vita privata della direttiva UE quale punto di partenza per la valutazione dei rischi (cfr. allegato II). I rischi per la vita privata possono essere elevati, poiché l'attuazione di un'applicazione RFID potrebbe essere suscettibile di attacchi dolosi oppure perché non esistono misure di controllo sulla privacy a livello di organizzazione o ambientale. I rischi per la vita privata possono anche essere modesti, semplicemente perché è improbabile che si verifichino nel contesto od organizzazione in esame, oppure perché l'applicazione RFID è già configurata in un modo altamente rispettoso della privacy. Il processo di valutazione dell'impatto sulla vita privata si propone di considerare tutti i rischi potenziali e poi riflettere sulla loro entità, probabilità e potenziale attenuazione. Il risultato di questa analisi è l'individuazione dei rischi per la vita privata che sono effettivamente rilevanti per la diffusione dell'applicazione RFID dell'organizzazione e che necessitano di essere attenuati attraverso controlli efficaci.

Il procedimento di valutazione dell'impatto sulla privacy (illustrato nella figura 2) impone a un gestore di applicazioni RFID di:

1. descrivere l'applicazione RFID;
2. individuare ed elencare in che modo l'applicazione RFID in esame possa minacciare la protezione della vita privata e stimare l'entità e la probabilità di tali rischi;
3. documentare i controlli tecnici e organizzativi in uso e proposti per attenuare i rischi individuati
4. documentare la risoluzione (i risultati dell'analisi) in merito all'applicazione RFID.



Passo 1: caratterizzazione dell'applicazione

La caratterizzazione dell'applicazione dovrebbe fornire un quadro completo e approfondito dell'applicazione, del contesto in cui opera e dei limiti del sistema. Vi sono descritti la progettazione dell'applicazione, le interfacce con questa confinanti e i flussi delle informazioni. Si raccomanda l'uso di diagrammi di flusso dei dati che mostrino il trattamento dei dati primari e secondari per visualizzare i flussi delle informazioni. Occorre documentare anche le strutture dei dati, in modo da consentire l'analisi dei potenziali collegamenti. Nell'allegato I sono sintetizzati gli elementi che caratterizzano un'applicazione RFID ai fini della conduzione di una valutazione dell'impatto sulla privacy.

Si raccomanda inoltre di riportare informazioni riguardanti il contesto operativo e strategico dell'applicazione. Fra queste possono rientrare la missione immediata e di più lungo termine del sistema, le parti coinvolte nella raccolta delle informazioni, i requisiti funzionali, tutti gli utenti potenziali e una descrizione dell'architettura dell'applicazione RFID e dei flussi di dati (in particolare, le interfacce con sistemi esterni che possono trattare dati personali).

Passo 2: individuazione dei rischi

L'obiettivo di questo procedimento è di individuare le condizioni che potrebbero minacciare o compromettere la riservatezza dei dati personali, utilizzando la direttiva UE come guida per le caratteristiche importanti degli obiettivi da proteggere in relazione alla vita privata. I rischi possono essere connessi alle componenti dell'applicazione RFID, alla sua operatività (infrastruttura per la raccolta, la conservazione e il trattamento dei dati) e al contesto di condivisione e trattamento dei dati in cui è integrata.

Nell'allegato III figura un elenco dei potenziali rischi per la vita privata, che serve da guida per un'individuazione sistematica di rischi potenziali che minacciano gli obiettivi della direttiva UE (allegato II).

Oltre all'individuazione dei rischi, la valutazione dell'impatto sulla privacy richiede una loro quantificazione relativa. Un gestore di applicazioni RFID deve considerare, in base ai principi di proporzionalità e in condizioni ragionevoli, la *probabilità* che si verifichino i rischi per la vita privata. I rischi possono derivare dall'interno e, se del caso, dall'esterno della specifica applicazione RFID in questione. Possono derivare sia dagli impieghi probabili sia dal possibile uso improprio delle informazioni, in particolare se le etichette RFID utilizzate nell'ambito dell'applicazione rimangono operative una volta in possesso delle persone**.**

La valutazione dei rischi impone di valutare i rischi applicabili in una prospettiva di protezione della vita privata; il gestore RFID dovrebbe considerare:

1. la significatività di un rischio e la probabilità che si manifesti,
2. l'entità dell'impatto qualora il rischio si concretizzi.

Il livello di rischio che ne emerge può essere classificato in basso, medio o alto.

Un rischio che ha causato un importante argomento di dibattito è la possibile utilizzazione delle etichette RFID per tracciare il profilo e/o seguire gli spostamenti delle persone. In questo caso le informazioni delle etichette RFID (in particolare il o i suoi identificatori) potrebbero essere utilizzate per reindividuare una persona specifica. I commercianti al dettaglio che cedono le etichette RFID ai clienti senza disattivarle o rimuoverle automaticamente all'uscita *possono* indurre involontariamente questo rischio. Una questione fondamentale, tuttavia, è stabilire se questo rischio è probabile e se di fatto si concretizza o meno in un rischio *ineliminabile*. Ai sensi del punto 11 della raccomandazione RFID, i commercianti al dettaglio dovrebbero disattivare o rimuovere nel punto di vendita le etichette usate nelle loro applicazioni, a meno che i consumatori, una volta informati della politica di conformità al presente quadro, acconsentano a mantenere attive le etichette. I commercianti non sono tenuti a disattivare o rimuovere le etichette qualora la relazione sulla valutazione dell'impatto sulla privacy concluda che le etichette utilizzate in un'applicazione del commercio al dettaglio che resteranno operative al di fuori del punto di vendita non rappresenta una probabile minaccia alla vita privata o alla protezione dei dati personali, come previsto al punto 12 della medesima raccomandazione. La disattivazione delle etichette va intesa come un qualsiasi processo che interrompe le interazioni di un'etichetta con l'ambiente circostante senza richiedere la partecipazione attiva del consumatore.

I modelli specifici per settore che vengono sviluppati nel tempo sulla base del presente quadro e destinati all'impiego in varie industrie possono circostanziare ulteriormente l'individuazione dei rischi.

Passo 3: individuazione e raccomandazione di controlli

Lo scopo di questo passo è di analizzare i controlli posti in essere o la cui attuazione è programmata, per ridurre al minimo, attenuare o eliminare i rischi individuati per la vita privata.

I controlli sono tecnici o di altra natura. I controlli tecnici sono inglobati nell'applicazione attraverso scelte di architettura o politiche tecnicamente applicabili, come ad esempio i parametri predefiniti, i meccanismi di autenticazione e i metodi di cifratura. Peraltro, i controlli diversi da quelli tecnici consistono nei controlli di gestione e operativi, come le procedure operative. I controlli possono essere suddivisi in preventivi o a posteriori. I primi inibiscono i tentativi di violazione, mentre i secondi rilevano le violazioni o i tentativi di violazione.

Possono sussistere anche controlli "naturali" creati dall'ambiente. Ad esempio, se non esistono lettori installati in grado di effettuare un tracciamento degli articoli o delle persone (perché non sussiste un motivo commerciale che li giustifichi), non esiste allora alcun (probabile) rischio.

I rischi individuati e i livelli di rischio a questi associati dovrebbero orientare la decisione in merito a quali controlli individuati sono pertinenti e quindi devono essere effettuati. La documentazione relativa alla valutazione dell'impatto sulla privacy dovrebbe spiegare in che modo i controlli si rapportano ai rischi specifici e spiegare in che modo questa attenuazione dei rischi determinerà un livello di rischio accettabile.

Nell'allegato IV si forniscono alcuni esempi di controllo.

Passo 4: documentazione della risoluzione e dei rischi residui

Una volta ultimata la valutazione dei rischi, la risoluzione finale in merito all'applicazione dovrebbe essere documentata nella relazione sulla valutazione dell'impatto sulla privacy, unitamente a ogni ulteriore osservazione riguardante i rischi, i controlli e i rischi residui.

- Un'applicazione RFID è ammessa all'operatività quando è stato ultimato il procedimento di valutazione dell'impatto sulla vita privata e, quindi, i rischi sono stati individuati e adeguatamente attenuati per assicurare che non rimanga alcun rischio residuo significativo al fine di ottemperare ai requisiti di conformità, con le appropriate revisioni e approvazioni interne.

- Allorché un'applicazione RFID non è ammessa a operare nel suo stato attuale, occorre sviluppare un piano d'azione correttivo specifico e elaborare una nuova valutazione dell'impatto sulla privacy al fine di stabilire se l'applicazione abbia raggiunto uno stato soddisfacente.

La risoluzione dovrebbe essere associata alle seguenti informazioni:

- nominativo della persona che sottoscrive la risoluzione,
- titolo della stessa,
- data della risoluzione.

Relazione sulla valutazione dell'impatto sulla vita privata

Le valutazioni dell'impatto sulla vita privata sono procedimenti interni che contengono informazioni sensibili suscettibili di avere implicazioni per la sicurezza, nonché informazioni potenzialmente riservate e di proprietà della società connessa ai prodotti e ai processi. Ciò detto, una relazione sulla valutazione dell'impatto sulla privacy deve in genere comprendere:

1. la descrizione dell'applicazione RFID riportata nell'allegato I,

2. la documentazione dei quattro passi descritti in precedenza.

La relazione sulla valutazione dell'impatto sulla privacy, firmata, che contempli una risoluzione approvata, deve essere consegnata al responsabile della sicurezza dei dati e/o della tutela della vita privata designato dalla società in conformità alle procedure interne del gestore di applicazioni RFID. Tale relazione è fornita fermi restando gli obblighi di cui alla direttiva 95/46/CE per i responsabili del trattamento dei dati, in particolare l'obbligo indipendente di notificazione all'autorità competente descritto nella sezione IX della direttiva 95/46/CE.

3. Disposizioni finali

Il quadro per la valutazione dell'impatto sulla vita privata entrerà in vigore entro sei mesi dalla pubblicazione e dall'approvazione da parte del Gruppo di lavoro "articolo 29" sulla protezione dei dati. Per le applicazioni RFID in essere prima dell'entrata in vigore del quadro per la valutazione dell'impatto sulla privacy, quest'ultimo si applicherà solo quando sono soddisfatte le condizioni previste per documentare una nuova valutazione o una revisione di quella esistente in conformità al quadro stesso.

ALLEGATO I – *Descrizione della caratterizzazione delle applicazioni RFID*

Il gestore di applicazioni RFID dovrà includere nella relazione sulla valutazione dell'impatto sulla vita privata, se del caso, le informazioni riportate di seguito.

Gestore di applicazioni RFID	• nome e indirizzo della persona giuridica • persona o ufficio responsabile della tempestività della valutazione dell'impatto sulla vita privata • punto o punti di contatto e metodo di indagine per raggiungere il gestore
Descrizione sintetica dell'applicazione RFID	• denominazione dell'applicazione RFID • finalità della o delle applicazioni RFID • scenari relativi all'uso di base dell'applicazione RFID • componenti dell'applicazione RFID e tecnologia impiegata (cioè frequenze, ecc.) • portata geografica dell'applicazione RFID • tipologie di utenti/persone su cui l'applicazione RFID ha un impatto • accesso e controllo individuale
Numero della relazione sulla valutazione dell'impatto sulla vita privata	• numero di versione della relazione (con una distinzione tra una relazione nuova o modificata solo in misura marginale) • data dell'ultima modifica apportata alla relazione
Trattamento dei dati RFID	• elenco dei tipi di dati trattati • presenza di informazioni sensibili nei dati trattati (ad es. dati sanitari)
Conservazione dei dati RFID	• elenco dei tipi di dati conservati • periodo di conservazione
Trasferimento interno dei dati RFID (se pertinente)	• descrizione o diagrammi dei flussi di dati delle operazioni interne che usano dati RFID • finalità del trasferimento dei dati personali
Trasferimento esterno dei dati RFID (se pertinente)	• tipologia del o dei destinatari di dati • finalità del trasferimento o dell'accesso in generale • dati personali (e relativo livello) individuati e/o individuabili che sono compresi nel trasferimento • trasferimenti all'esterno dello Spazio economico europeo (SEE)

ALLEGATO II – *Obiettivi della tutela della vita privata*

Attualmente la direttiva 95/46/CE prevede nove obiettivi per la tutela della vita privata. Il procedimento di valutazione dell'impatto sulla privacy è stato sviluppato in considerazione di detti obiettivi e dei rischi associati alle applicazioni RFID. Il presente allegato riassume questi obiettivi per la tutela della vita privata. Tutti gli obiettivi sono elementi essenziali per il rispetto delle disposizioni da parte dell'organizzazione, ma in molti casi solo un gruppo più limitato di questi requisiti è pertinente per l'applicazione RFID considerata. Pertanto, il ruolo di questi obiettivi è di fornire informazioni in merito all'istituzione e allo sviluppo del procedimento di valutazione dell'impatto sulla privacy più che sull'esecuzione di una determinata valutazione.

Descrizione degli obiettivi per la tutela della vita privata (ricavati e aggiornati in base alla o alle rispettive direttive dell'Unione; in questo caso si tratta della direttiva 95/46/CE)	
Garanzia della qualità dei dati personali	Gli obiettivi fondamentali che occorre garantire sono l'assenza e la riduzione al minimo dei dati raccolti, la specificazione e la limitazione delle finalità, la qualità dei dati e la trasparenza.
Legittimità del trattamento di dati personali	Occorre assicurare la legittimità del trattamento dei dati personali fondando quest'ultimo sul consenso, su un contratto, su un obbligo giuridico, ecc.
Legittimità del trattamento di dati personali *sensibili*	Occorre assicurare la legittimità del trattamento di dati personali sensibili fondando quest'ultimo sul consenso, su un contratto, su un obbligo giuridico, ecc.
Rispetto del diritto dell'interessato a essere informato	È necessario assicurare che l'interessato sia informato tempestivamente della raccolta di dati che lo riguardano.
Rispetto del diritto dell'interessato ad accedere ai dati, rettificarli e cancellarli	Occorre assicurare che sia rispettata tempestivamente la volontà dell'interessato di accedere ai dati, rettificarli, cancellarli e bloccarli.
Rispetto del diritto dell'interessato a opporsi al trattamento	Occorre assicurare che i dati dell'interessato cessano di essere trattati qualora questi vi si opponga. Deve essere assicurata in modo particolare la trasparenza delle decisioni automatizzate che riguardano le persone.
Tutela della riservatezza e della sicurezza del trattamento	Gli obiettivi fondamentali che occorre garantire sono: impedimento dell'accesso non autorizzato, registrazione cronologica del trattamento dei dati, sicurezza della rete e del trasporto e impedimento della perdita accidentale dei dati.
Adempimento degli obblighi di notificazione	Gli obiettivi principali da conseguire sono la notificazione in merito al trattamento dei dati, la verifica preventiva della conformità e la documentazione.
Adempimento degli obblighi relativi alla conservazione dei dati	La conservazione dei dati dovrebbe essere limitata al periodo di tempo minimo in funzione della finalità della conservazione o di altri obblighi giuridici.

ALLEGATO III – *Rischi per la vita privata*

Questa sezione riporta un elenco di possibili rischi per la vita privata connessi all'uso dell'applicazione RFID considerata. Si raccomanda che, soprattutto nel caso di valutazioni complete dell'impatto sulla privacy, i rischi siano individuati sistematicamente con l'ausilio di procedure di valutazione dei rischi convenzionali che comprendano minacce e vulnerabilità di un'applicazione RFID.

Nella tavola seguente figurano esempi di rischi che possono compromettere la capacità di un soggetto di conseguire gli obiettivi per la tutela della vita privata descritti nell'allegato II. I gestori di applicazioni RFID possono impiegare questo elenco come punto di partenza; è possibile tuttavia che non tutti questi rischi si applichino a ogni singola applicazione RFID. I gestori RFID dovrebbero accertarsi che ciascun rischio individuato sia attenuato in maniera adeguata con uno o più controlli in funzione della probabilità che si verifichi e dell'entità dell'impatto. I gestori di applicazioni RFID possono avere la necessità di abbinare i controlli o di rafforzare quelli esistenti in funzione di fattori come, tra l'altro, la tecnologia impiegata, la natura della loro attuazione, la tipologia delle informazioni e le politiche applicabili.

Rischi per la vita privata	Descrizione ed esempi
Finalità imprecisata e illimitata	La finalità della raccolta dei dati non è stata precisata e documentata o sono utilizzati più dati di quelli richiesti per la finalità indicata. Esempio: finalità non documentate per le quali sono utilizzati dati RFID e/o impiego di dati RFID per tutti i generi di analisi fattibili.
Raccolta eccessiva rispetto alla finalità	I dati sono raccolti in forma identificabile in misura superiore a quella precisata nella finalità. Esempio: le informazioni ottenute da una carta di pagamento RFID non sono usate unicamente ai fini del trattamento delle transazioni, ma anche per costruire profili individuali.
Informazioni incomplete o mancanza di trasparenza	Le informazioni fornite all'interessato sulla finalità e l'uso dei dati non sono complete, il trattamento dei dati non è trasparente oppure le informazioni non sono fornite tempestivamente. Esempio: le informazioni RFID messe a disposizione dei consumatori non forniscono sufficienti chiarimenti sulle modalità con cui i dati RFID sono trattati e utilizzati, sull'identità del gestore o sui diritti dell'utente.
Combinazione eccessiva rispetto alla finalità	I dati personali sono combinati in una misura superiore a quanto necessario a conseguire la finalità specificata. Esempio: le informazioni tratte dalle carte di pagamento RFID sono abbinate ai dati personali ottenuti da terzi.
Assenza di politiche o meccanismi di	I dati sono conservati più a lungo di quanto

cancellazione	necessario per conseguire la finalità precisata. Esempio: i dati personali che sono raccolti come parte dell'applicazione sono conservati per un periodo più lungo di quanto consentito per legge.
Consenso esplicito privo di validità	Il consenso è stato ottenuto con la minaccia di uno svantaggio. Esempio: i prodotti non possono essere resi o cambiati oppure usufruire delle garanzie previste per legge quando l'etichetta RFID è disattivata o rimossa.
Raccolta segreta di dati da parte del gestore RFID	Alcuni dati sono registrati in segreto all'insaputa dell'interessato, come i profili degli spostamenti. Esempio: si leggono informazioni sui consumatori mentre questi camminano davanti a negozi o centri commerciali senza che nessun pittogramma o simbolo li avvisi delle rilevazioni RFID in corso.
Incapacità di consentire l'accesso	L'interessato non ha alcun modo di apportare una rettifica o effettuare una cancellazione dei suoi dati. Esempio: il datore di lavoro non può fornire al dipendente un quadro esaustivo di quanto registrato al suo riguardo attraverso dati RFID e di produzione.
Impedimento delle opposizioni	Non esiste alcun modo tecnico od operativo per consentire di applicare l'opposizione di un interessato. Esempio: chi fa visita presso un ospedale non può impedire la rilevazione delle informazioni personali sensibili sulle etichette che lo riguardano (terapie).
Mancanza di trasparenza delle decisioni automatizzate che interessano le persone	Sono utilizzate decisioni automatizzate che interessano dati personali ma gli interessati non sono informati della logica del processo decisionale. Esempio: senza avvisare i consumatori, un gestore RFID legge tutte le etichette portate da una persona, comprese le etichette fornite da un altro soggetto, e sulla base delle stesse determina che tipologia di messaggio commerciale questi dovrebbe ricevere.
Gestione insufficiente dei diritti di accesso	I diritti di accesso non sono revocati quando non sono più necessari. Esempio: attraverso una carta RFID, un ex-tirocinante accede a parti di un'impresa che dovrebbero essere inaccessibili.
Meccanismo di autenticazione	Non è impedito un numero sospetto di tentativi di

insufficiente	identificazione e autenticazione. Esempio: i dati personali riportati nelle etichette non sono protetti per impostazione predefinita da una parola d'accesso o da un altro meccanismo di autenticazione.
Trattamento dei dati illegittimo	Il trattamento dei dati personali non si basa sul consenso, su un contratto, su un obbligo giuridico, ecc. Esempio: un gestore RFID condivide con terzi le informazioni raccolte senza preavviso o consenso, come sarebbe previsto per legge.
Meccanismo insufficiente di registrazione cronologica dell'attività	Il meccanismo di registrazione cronologica è insufficiente. Non riporta i procedimenti amministrativi. Esempio: non è registrato chi ha effettuato un accesso ai dati RFID sulla carta del dipendente.
Raccolta dati incontrollabile dalle etichette RFID	C'è il rischio che le etichette RFID possano essere utilizzate regolarmente per tracciare un profilo e/o seguire gli spostamenti degli individui. Esempio: i commercianti al dettaglio leggono tutte le etichette che riescono a vedere.

ALLEGATO IV – *Elenco di esempi di controlli e di misure di attenuazione delle applicazioni RFID*

La presente sezione fornisce una serie di esempi di potenziali controlli che possono aiutare un gestore di applicazioni RFID a individuare strategie adeguate di attenuazione. I rischi individuati come rilevanti per un gestore di applicazioni RFID nel passo 2 del processo di valutazione dell'impatto sulla privacy possono essere attenuati mediante una o più strategie mirate, alcune delle quali sono delineate nel presente allegato IV. L'obiettivo è di far individuare e applicare dal gestore di applicazioni RFID, mediante la conduzione di un processo di valutazione dell'impatto sulla privacy, i controlli necessari per attenuare i rischi per la vita privata.

Tra i potenziali meccanismi di controllo rientrano:

- pratiche di disciplina delle applicazioni RFID,
- accesso e controllo individuale,
- misure di protezione del sistema (compresi i controlli di sicurezza),
- protezione delle etichette,
- misure di responsabilità.

Queste pratiche integrano il quadro esistente dell'Unione europea per la protezione dei dati e non sono intese a sostituirlo o a modificarne il campo di applicazione.

Pratiche che disciplinano le applicazioni RFID

Vi rientrano:

- pratiche di gestione adottate dal gestore di applicazioni RFID,
- politiche di cancellazione e soppressione dei dati RFID,
- politiche connesse al trattamento legittimo delle informazioni personali,
- disposizioni vigenti per la riduzione al minimo dei dati nella gestione dei dati RFID, laddove fattibile,
- trattamento o stoccaggio delle informazioni desunte da etichette che non appartengono al gestore RFID,
- pratiche di gestione della sicurezza.

Accesso e controllo individuale

- fornitura di informazioni circa le finalità del trattamento e le categorie di dati personali interessate,
- descrizione delle modalità per opporsi al trattamento dei dati personali o per revocare il consenso,

- individuazione del procedimento per richiedere la rettifica o la cancellazione di dati personali incompleti o inesatti.

Protezione del sistema

In questa sezione della relazione sulla valutazione dell'impatto sulla privacy occorre documentare anche la **protezione del sistema** in relazione alla tutela adeguata della vita privata e dei dati personali. Il concetto di protezione del sistema si applica ai sistemi di *back-end* e all'infrastruttura di comunicazione nella misura in cui è coinvolta l'applicazione RFID. Laddove applicati, va riconosciuto che i sistemi di back-end sono spesso complessi e possono essere stati sottoposti essi stessi a una valutazione dell'impatto sulla privacy. Può rivelarsi necessario riesaminare tale analisi per assicurare che si sia tenuto conto del tipo di informazioni utilizzate dall'applicazione RFID. Qualora tale valutazione non esista, si devono considerare i seguenti componenti del sistema di *back-end*:

- devono essere attivi i controlli sull'accesso in relazione alla tipologia di dati personali e di funzionalità dei sistemi;

- devono esistere controlli e politiche per assicurare che il gestore non colleghi i dati personali nell'applicazione RFID in modo non coerente con la relazione sulla valutazione dell'impatto sulla privacy;

- occorre verificare che siano adottate misure adeguate volte a tutelare la riservatezza, l'integrità e la disponibilità dei dati personali nei sistemi e nell'infrastruttura di comunicazione;

- esistono politiche sulla conservazione e sulla cancellazione dei dati personali;

- devono esistere ed essere effettuati controlli sulla sicurezza delle informazioni come:

    - misure che garantiscono la sicurezza delle reti e del trasferimento dei dati RFID,

    - misure che agevolano la disponibilità dei dati RFID attraverso sistemi adeguati di back-up e recupero.

Protezione delle etichette RFID

Occorre indicare le misure di controllo per la **protezione delle etichette RFID** in relazione alla vita privata e ai dati personali. Tali misure sono particolarmente rilevanti per le applicazioni RFID che utilizzano etichette RFID contenenti dati personali.

Queste misure di controllo della protezione comprendono:

- il controllo dell'accesso a funzionalità e informazioni, comprese l'autenticazione di apparecchi di lettura e di scrittura, nonché i processi sottostanti, e l'autorizzazione a intervenire sull'etichetta RFID;

- metodi per garantire la riservatezza delle informazioni (ad esempio mediante la cifratura dell'intera etichetta RFID o di determinati suoi campi);

- metodi per garantire l'integrità delle informazioni;

- conservazione delle informazioni dopo la raccolta iniziale (ad esempio, durata della conservazione, procedure di cancellazione dei dati al termine del periodo di conservazione o di soppressione delle informazioni nell'etichetta RFID, procedure per la conservazione o la cancellazione selettiva di campi);

- impossibilità di falsificare l'etichetta RFID stessa;

- disattivazione o rimozione, se richiesto o altrimenti disposto.

Le misure di attenuazione possono comprendere controlli basati sull'utenza che permettono di far fronte a situazioni in cui si deve tener conto di particolari esigenze o gradi di sensibilità diversi in relazione alla vita privata. La disattivazione o la rimozione sono attualmente le due forme più comuni di attenuazione dei rischi per l'utente finale e/o il consumatore. Queste possono essere richieste nell'ambito dell'analisi relativa alla valutazione dell'impatto sulla privacy, in talune circostanze sono previste per legge, oppure possono essere decise liberamente dal cliente, una volta lasciato il punto di vendita, in modo da rafforzarne la fiducia. Inoltre, la raccomandazione della Commissione sulle applicazioni RFID in relazione alla protezione della vita privata e dei dati personali suggerisce alcune metodologie e migliori prassi associate alla disattivazione o alla rimozione di etichette RFID nella fase del commercio al dettaglio[4].

Misure di rendicontazione

Queste misure sono studiate per rafforzare la protezione dei dati in termini procedurali, nell'ambito del dovere di rendicontazione. Attraverso queste misure si svolge un'azione di sensibilizzazione esterna in merito alle applicazioni RFID.

- Assicurare il facile accesso a una **politica di informazione** esaustiva che indichi:

    - l'identità e i recapiti del gestore di applicazioni RFID,

    - le finalità dell'applicazione RFID,

    - i tipi di dati trattati dall'applicazione RFID, in particolare se sono elaborati dati personali,

    - se si seguirà la localizzazione delle etichette portate da singole persone,

    - i probabili effetti sulla protezione della vita privata e dei dati, se esistenti, connessi all'uso di etichette RFID nell'applicazione RFID e misure disponibili per attenuare gli stessi.

- Assicurare l'esistenza di **avvisi** concisi, accurati e di facile comprensione della presenza di lettori RFID, che indichino:

    - l'identità del gestore di applicazioni RFID,

    - un punto di contatto a cui le persone possono rivolgersi per prendere visione della politica di informazione.

---

[4] Ai punti 12 e 13 della raccomandazione della Commissione del 12 maggio 2009, {SEC (2009) 585}, si raccomanda che *i metodi di disattivazione o rimozione delle etichette vengano messi a disposizione gratuitamente, immediatamente o in una fase successiva, senza comportare alcuna riduzione o cessazione degli obblighi del commerciante al dettaglio o del costruttore nei confronti dei consumatori.*

- Segnalare se esistono **mezzi di ricorso** e come funzionano:

    - indicare il o i soggetti giuridici responsabili che agiscono da gestore di applicazioni RFID (potrebbe essere un soggetto per giurisdizione o area operativa);

    - i punti di contatto della persona o dell'ufficio preposto al riesame delle valutazione e della costante adeguatezza delle misure tecniche e organizzative connesse alla protezione dei dati personali e della vita privata;

    - i metodi di consultazione (ad esempio, come si può contattare il gestore di applicazioni RFID per porre una domanda, avanzare una richiesta, presentare un reclamo o esercitare un diritto);

    - i metodi per opporsi al trattamento, esercitare i diritti di accesso ai dati personali (compresa la cancellazione e la rettifica dei dati personali), revocare il consenso o modificare i controlli e altre scelte concernenti il trattamento dei dati personali, se necessario o altrimenti previsto;

    - altri mezzi di ricorso, se necessario o altrimenti disposto.

Appendice A: Riferimenti

La presente sezione riporta i riferimenti ai documenti ufficiali serviti a sviluppare il quadro.

- Commissione delle Comunità europee, *Raccomandazione della Commissione sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza*, 12 maggio 2009, C (2009) 3200, reperibile all'indirizzo internet http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:122:0047:0051:IT:PDF

- Commissione delle Comunità europee, *Documento di lavoro dei servizi della Commissione che accompagna la raccomandazione della Commissione sull'applicazione dei principi di protezione della vita privata e dei dati personali nelle applicazioni basate sull'identificazione a radiofrequenza*, Sintesi della valutazione d'impatto, 12 maggio 2009, SEC(2009) 586, consultabile all'indirizzo internet http://ec.europa.eu/information_society/policy/rfid/documents/recommendationonrfid200i9impact.pdf

- Direttiva 95/46/CE del Parlamento europeo e del Consiglio, del 24 ottobre 1995, relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati, GU L 281 del 23.11.1995, pag. 31, reperibile alla pagina internet http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:IT:HTML

- Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche), GU L 201 del 31.7.2002, pag. 37, disponibile alla pagina internet http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2002:201:0037:0047:IT:PDF

- Direttiva 2009/136/CE del Parlamento europeo e del Consiglio, del 25 novembre 2009, recante modifica della direttiva 2002/22/CE relativa al servizio universale e ai diritti degli utenti in materia di reti e di servizi di comunicazione elettronica, della direttiva 2002/58/CE relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche e del regolamento (CE) n. 2006/2004 sulla cooperazione tra le autorità nazionali responsabili dell'esecuzione della normativa a tutela dei consumatori, GU L 337 del 18 dicembre 2009, pag. 11, consultabile alla pagina internet http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:IT:PDF

- Articolo 29 Gruppo di lavoro per la protezione dei dati personali, *Parere 4/2007 sul concetto di dati personali*, 20 giugno 2007, 01248/07/EN WP 136, disponibile sul sito internet http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp136_it.pdf

- *Privacy Impact Assessment Handbook*, consultabile alla pagina internet http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf

- *Status of Implementation of Directive 95/46 on the protection of Individuals in regards to the Processing of Personal Data*, disponibile alla pagina internet http://ec.europa.eu/justice_home/fsj/privacy/law/implementation_en.htm

- Articolo 29 Gruppo di lavoro per la protezione dei dati personali, *Working document on data protection issues related to RFID technology*, 19 gennaio 2005, 10107/05/EN WP 105, reperibile alla pagina internet http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2005/wp104_en.pdf

Appendice B: Glossario

Nell'ambito del quadro si fa ricorso a una serie di termini connessi ai concetti di tutela della vita privata e dei dati personali, nonché all'applicazione della tecnologia RFID in un'ampia gamma di contesti. Ai fini del presente quadro, in merito alla tutela della vita privata e dei dati personali si applicano le definizioni di cui alla direttiva 95/46/CE.

Le seguenti definizioni, rilevanti ai fini del quadro, riguardano la tecnologia RFID e le sue applicazioni.

Applicazione RFID – Un'applicazione che elabora dati mediante l'uso di etichette e lettori e che si basa su un sistema di *back-end* e di un'infrastruttura di comunicazione in rete.

Controllare – Condurre un'attività allo scopo di individuare, osservare, copiare o registrare l'ubicazione, il movimento, le attività o lo stato di una persona.

Dati personali – Qualsiasi informazione connessa a una persona fisica identificata o identificabile ("soggetto"); si considera identificabile la persona che può essere identificata, direttamente o indirettamente, in particolare mediante riferimento a un numero identificativo oppure a uno o a più elementi specifici caratteristici della sua identità fisica, fisiologica, psichica, economica, culturale o sociale.

Etichetta RFID o etichetta – Un dispositivo RFID in grado di produrre un segnale radio o un dispositivo RFID che riaccoppia, retrodiffonde o riflette (a seconda del tipo di dispositivo) e modula un segnale portante ricevuto da un apparecchio di lettura o di scrittura.

Gestore di applicazioni RFID – La persona fisica o giuridica, l'autorità pubblica, il servizio o qualsiasi altro organismo che, da solo o insieme ad altri, determina le finalità e gli strumenti della gestione di un'applicazione RFID, compresi i responsabili del trattamento dei dati personali che utilizzano un'applicazione RFID.

Identificazione a radiofrequenza (*Radio Frequency Identification*, RFID) – L'uso di onde elettromagnetiche o l'accoppiamento di un campo reattivo nella porzione di radiofrequenza dello spettro per comunicare a partire da o verso un'etichetta mediante una varietà di sistemi di modulazione e codifica allo scopo di leggere, in modo univoco, l'identità di un'etichetta di radiofrequenza o altri dati in essa registrati.

Informazioni sull'etichetta RFID – Le informazioni racchiuse in un'etichetta RFID e trasmesse quando questa è interrogata da un lettore RFID.

Lettore RFID o apparecchio di lettura RFID – Un dispositivo fisso o mobile per la cattura e l'identificazione di dati che utilizza un'onda elettromagnetica a radiofrequenza o l'accoppiamento di un campo reattivo per stimolare ed eseguire una risposta modulata di dati da un'etichetta o gruppo di etichette.

Persona – Una persona fisica che interagisce o è altrimenti coinvolta in una o più componenti di un'applicazione RFID (ad esempio, sistema di *back-end*, infrastruttura di comunicazione, etichetta RFID), ma che non gestisce un'applicazione RFID né ne esercita una delle funzioni. A tale riguardo, una persona è diversa da un utente. Una

persona non ha alcuna relazione diretta con la funzionalità dell'applicazione RFID, ma può, ad esempio, semplicemente portare su di sé un articolo recante un'etichetta RFID.

Sicurezza delle informazioni – Mantenimento della riservatezza, dell'integrità e della disponibilità delle informazioni.

Utente – Nello specifico, un utente di applicazioni RFID, ovvero una persona (o altro soggetto, quale una persona giuridica) che interagisce direttamente con una o più componenti di un'applicazione RFID (ad esempio un sistema di *back-end*, un'infrastruttura di comunicazione, un'etichetta RFID) allo scopo di sfruttare un'applicazione RFID oppure esercitarne una o più funzioni.

Security on Things – Un approccio programmatico alla sicurezza delle cose

"Security on Things" è un originale paradigma di HSC che include tecnologie, policy e practices di sicurezza e privacy applicate alla difesa delle merci dalle attività illegali, sia che si tratti di contraffazione, produzione non autorizzata, mercato grigio o il vero e proprio furto dagli scaffali dello store. **SoT** si basa su certificati elettronici di originalità applicati ai prodotti, su un robusto sistema di tracking item-level integrato con i sistemi produttivi, logistici e distributivi attraverso cui transitano le merci, e, non meno importanti, su policy e procedure di sicurezza, a difesa del prodotto e degli archivi in cui risiedono le sue informazioni di tracking, e di privacy, a difesa delle persone che possiedono o utilizzano le merci. HSC, insieme ai propri partners, offre la capacità di progettare certificati elettronici di originalità "ad hoc" e di definire architetture di integrazione che permettono di raccogliere e tracciare le informazioni di prodotto che provengono da HSCLeanFlow, da HSCStorePoint e dai sistemi aziendali e dei partner produttivi, logistici distributivi permettendo di seguire ogni passaggio dei prodotti dal produttore al consumatore.

HSC, con partner specializzati nella sicurezza informatica aiuta il cliente a definire policy e procedure per difendere i certificati elettronici, gli archivi del sistema del tracking, ma anche i sistemi aziendali esistenti, da attacchi esterni e interni che intendono attentare alla sicurezza informatica e delle cose.

La difesa della proprietà degli oggetti è un altro aspetto della Security of Things. HSC utilizza sistemi tradizionali di **EAS** basati su sistemi RFID o misti (RFID e Magneto-acustico), ma ha anche sviluppato sistemi anti-taccheggio proattivi basati su SmartShelf RFID, in grado di prevenire il furto di merci dagli scaffali fin sul nascere. **SoT** è un approccio multidisciplinare, frutto di importanti collaborazioni con aziende del fashion e del retail, che mette insieme tecnologie, organizzazione e sicurezza.

HS Custom S.r.l.
Wireless & Consulting
Via Novara 349
28078 Romagnano Sesia - Italy
tel. + 39 0163 81 80 38
fax. + 39 0163 81 81 49
www.hscustom.it info@hscustom.it