General Data Protection Regulations

GDPR and RFID Privacy Impact Assessment (EN 16571)

A guide to understanding the links between GDPR and RFID Privacy Impact Assessment (PIA) as defined in EN 16571.

The GDPR has been big news but, if you operate any RFID applications, you also need to be aware of RFID Privacy Impact Assessments (EN 16571). This document explains the links between GDPR and EN 16751.

General Data Protection Regulations

GDPR and RFID Privacy Impact Assessment (EN 16571)

Introduction

Article 35 of the General Data Protection Regulation (GDPR) is entitled **Data protection impact assessment.** This unusual term is considered by many legal experts and some data protection authorities to be the equivalent of **privacy impact assessment** (PIA).

In this document we will attempt to link abstracts of some paragraphs of GDPR Article 35 with EN 16571 *Information technology – RFID privacy impact assessment process*s . We will also refer to some of the recitals, i.e. the preamble justifying the articles within GDPR.

The need for a PIA

> *Paragraph 1 states: Where a type of processing in particular using new technologies ... is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data.*

In turn this is supported by this abstract from recital [91]:

> A data protection impact assessment is equally required for monitoring publicly accessible areas on a large scale, **especially when using opticelectronic devices**[1] or for any other operations where the competent supervisory authority considers that the processing is likely to result in a high risk to the rights and freedoms of data subjects, in particular because they prevent data subjects from exercising a right or using a service or a contract, or because they are carried out systematically on a large scale.

EN 16571 defines a PIA process specifically designed to take account of the various features of specific RFID technologies and the design of the application. There are two key issues to remember about RFID. Some of the data, including the unique chip identifier on each tag, are defined as personal data by the various Data Protection Authorities (DPAs) under the existing Data Protection Directive of 1995. Generally speaking, RFID tags and smart cards **have no on/off switch**, which means that they can be read anywhere with an appropriate reader. This means that not only shall a new RFID system be subjected to an EN 16571 PIA process, but this should apply to established systems, particularly because older RFID products might not offer more recently developed privacy enhancement features.

[1] Our emphasis and interpretation that this includes RFID

The question of risk, and what is **high risk**, can be very subjective if a PIA process is not followed. You can leave it to the DPAs and lawyers and the courts to decide, or take a low cost precautionary approach. EN 16571 and the compliant CNRFID-CSL RFID Privacy Impact Assessment software eliminates the need for guesswork. With the ever-changing threat profile and increased availability of low cost readers not only is the data on the card exposed to personal privacy risks, but the RFID system's security might also be impacted.

Automated processing and public spaces

> *Paragraph 3 states: A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:*
>
> *(a) a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person*
>
> *(c) a systematic monitoring of a publicly accessible area on a large scale.*

Automated processing is the *raison d'être* of RFID. What is automated for the intended application can remain automated in a '*publicly accessible area*', as defined above. The untried legal position is what happens if someone other than the data controller's organisation has access to personal data on an RFID tag or smart card. We don't make any claim to be legal experts. We do note that if any form of memory device is lost or left exposed – even if the data has not been read – that this has resulted in the data controller organisation being held responsible and fined under existing data protection laws.

A properly undertaken EN 16571 RFID PIA can be used to assess the risk value of the data on the tag, the RFID threats and vulnerabilities to which that data might be exposed and the countermeasures that can be used to reduce the risk.

Some countries have laws that make it illegal to capture data from RFID tags by anyone other than the legitimate data processing organisation. Extensive fines and prison sentences are available as punishments that can be imposed by the courts. Having a criminal offence on the statute does put the onus on those exploiting RFID. We don't think that there are any such laws in place in Europe. The general approach, even under present European data protection laws, is to make the organisation

that enabled personal data to be leaked to be held responsible for this. Except with the highest level of protocol, RFID technology results in the tags being in what EN 16571 calls **the uncontrolled domain** as soon as the tag or smart card leaves the data controller's controlled domain. The question that remains unanswered is: **how is this deliberate action different from the accidental loss of a memory device?** At least a properly conducted RFID PIA process will identify what data is exposed and what measures have been taken by the data controller to protect that data.

Legally required RFID PIAs

> *Paragraph 4 states: The supervisory authority shall establish and make public a list of the kind of processing operations which are subject to the requirement for a data protection impact assessment pursuant to paragraph 1.*

Knowing that RFID applications have already been under the spot lights with the Recommendation issued in 2009, there is little doubt that it will be classified as processing operations that require a DPIA. Even organisations that lobbied to be excluded from the rigors of a PIA at that time have been called to order by the European commission.

Comparing the GDPR and EN 16571 processes

Paragraph 7 states. The assessment shall contain at least:

> *(a) a systematic description of the envisaged processing operations and the purposes of the processing, including, where applicable, the legitimate interest pursued by the controller;*
>
> *(b) an assessment of the necessity and proportionality of the processing operations in relation to the purposes;*
>
> *(c) an assessment of the risks to the rights and freedoms of data subjects referred to in paragraph 1; and*
>
> *(d) the measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data and to demonstrate compliance with this Regulation taking into account the rights and legitimate interests of data subjects and other persons concerned.*

EN 16571 requires the RFID application to be fully defined. The CNRFID-CSL software calls for the specific RFID protocol and products being used to be identified. The difference between protocols can be significant in terms of read range and the speed of data capture. Some protocols have proved to be more common than others, resulting in an increasing range of supportive products. For example in 2015 we assessed that there were three quarters of a billion readers (i.e. smart phones) that could read specific RFID protocols. This was not foreseen, nor planned, when the RFID protocols were first developed. The net result is that many devices are now available in the **uncontrolled domain** that not only have the potential to adversely impact on the data privacy of some applications, but even exposing the system performance and security to corrupt data. Corrupt data on a tag might render that tag useless to the application, but it could do worse by delivering malware.

> NOTE: The popular two dimension bar code known as QR code, was intended to be used primarily in the automotive and engineering manufacturing sectors. It never expected use for marketing purposes, and naive use has resulted in the delivery of malware[2].

It follows that while the basic popularity of some RFID protocols can result in a wider choice and

[2] http://resources.infosecinstitute.com/security-attacks-via-malicious-qr-codes/

sometimes less expensive products, that this can have an impact on the '*proportionality of the processing operations'* as set out in the paragraph. In the more challenging applications, our consulting service can be used to supplement the basic PIA software.

The EN 16571 software itself calculates an **initial risk score** based on EN 16571's score of the value of the different types of data element encoded on the tag or smart card, then factoring on this the RFID threats and vulnerabilities associated with the particular protocol.

EN 16571 identifies **RFID countermeasures** that are effectively *the 'measures envisaged to address the risks, including safeguards, security measures and mechanisms to ensure the protection of personal data'*. The countermeasures vary by protocol and even by product. Therefore these fundamental features can have a bearing on the privacy risks. Once a commitment has been made to use a particular set of RFID products, particularly the tags and the readers (also known as interrogators) this is not the end for applying countermeasures. This is because they are not automatically applied. For example, a protocol might support a command that can be a countermeasure. Even if the tag and the reader support the use of particular commands to support a countermeasure, the design of the RFID system needs to have '*processing operations'* that call up the commands to invoke the countermeasure. The EN 16571 software identifies all the countermeasures that can be applied. As these are selected, the initial risk score is recalculated to show the **residual risk**. The countermeasures that are not used can be considered as part of a continual improvement programme, thus contributing to compliance with ***Article 25 Data protection by design and by default***.

Codes of conduct

> *Paragraph 8 states: Compliance with approved codes of conduct referred to in Article 40 by the relevant controllers or processors shall be taken into due account in assessing the impact of the processing operations performed by such controllers or processors, in particular for the purposes of a data protection impact assessment.*

EN 16571 makes provision for the use of **templates**, which can be developed by an industry body or for a type of RFID system developed by a supplier. The CNRFID-CSL software is able to take this one step further. The order form for the software identifies specific applications, e.g. staff and visitor identification. When the software is downloaded any existing template can be pre-loaded. This ensures consistency across PIAs for the same application, and additionally save the data controller time in completing the RFID PIA.

Therefore this fully meets the objectives of recital [92]:

> There are circumstances under which it may be reasonable and economical for the subject of a data protection impact assessment to be broader than a single project, for example where public authorities or bodies intend to establish a common application or processing platform or where several controllers plan to introduce a common application or processing environment across an industry sector or segment or for a widely used horizontal activity.

The only caveat to this is that for RFID, a **common application** implies the use of the same products, encoded data, and implementation of the same countermeasures.

Review procedure

Paragraph 11 states: Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.

RFID is a dynamic technology with new features being continually introduced. EN 16571 calls for a periodic review of the PIA every year and or where the design of the system changes. The CNRFID-CSL software allows previous PIAs to be saved with only changes needing to be included during the review process.

CNRFID-CSL also provides a support service to clients using its software. As products come onto the market with additional privacy enhancing facilities, the client can be notified. In many cases this awareness will enable an RFID system to be improved progressively, and not require replacing expensive hardware. This can be done because CNRFID maintains an official catalogue of RFID and their privacy enhancing features.