The GDPR and RFID Applications: The Implications of Consent and Transparency

Introduction
This document is one of a series where we look at specific aspects of the General Data Protection Regulation and how the European Standards on RFID privacy inter-relate with it. The series of articles is available at http://rfid-pia-en16571.eu/ressources/documents/.

This particular article looks at consent and transparency. We will attempt to link some clauses and paragraphs of the GDPR with EN 16571 Information technology – RFID privacy impact assessment process. We also refer to EN 16570 Information technology — Notification of RFID — The information sign and additional information to be provided by operators of RFID application system.

Although the numbered articles in the GDPR do not explicitly call out “RFID” – nor do they call out other technologies – Recital [30] is very clear that RFID has to be taken into consideration:

Natural persons may be associated with online identifiers provided by their devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers such as radio frequency identification tags¹. This may leave traces which, in particular when combined with unique identifiers and other information received by the servers, may be used to create profiles of the natural persons and identify them.

Lawfulness of processing
Before looking at the specific articles on consent in the GDPR, it might be worthwhile starting the discussion by looking at selected parts of paragraph 1 of Article 6 dealing with lawfulness of processing.

Processing shall be lawful only if and to the extent that at least one of the following applies:
(a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
(b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party

This abstract from Recital [39]

Personal data should be processed in a manner that ensures appropriate security and confidentiality of the personal data, including for preventing unauthorised access to or use of personal data and the equipment used for the processing.

The need to be both lawful and ensure appropriate security and confidentiality is the real challenge. An RFID application can be designed to be lawful for the specific purposes of data capture. With open systems, the organisation capturing data from a tag does not do the encoding. It knows that data that it wants is, or is not encoded on the tag, but might be unaware of any other data on the tag. Then after the tag has been read lawfully for the application, the tag is released into what has been called the uncontrolled domain. This uncontrolled domain applies equally to closed system applications if the tag leaves the application and is still readable.

Let’s look at the implications of the uncontrolled domain:

¹ Our emphasis

©2016 CNRFID-Centre national de référence RFID Convergent Software Ltd.
First, almost all RFID protocols support a tag having a unique identifier – so as Recital [30] implies this is the first step to being able to create a profile.

Most tags and smart cards (considered to be RFID by the European Commission) have no off switch, so are still readable when they leave the RFID operator’s domain.

There are only a few common RFID protocols, so to achieve interoperability, devices are commonplace and effectively off-the-shelf items. Although some hackers have gone to extreme lengths to construct devices to read tags, the reality is that they can purchase any brand of reader and even buy them second-hand on eBay. There are even devices on the dark web that can harvest data on an industrial scale.

There is also some misunderstanding about read range. Generally it is related to power output. So while a legitimate RFID application may turn down the power of a reading device to achieve a controlled read range (e.g. to stop cross-talking with other tags), devices in the uncontrolled domain can have their power set to the highest limit specified by the radio regulations. And this is before any bad guy tries to break the limits of the legal radio regulations.

The point of all of this is to stress that the GDPR currently has a narrow focus on the system developed by what EN 16571 calls the RFID operator. It is only in Recital [39] that more emphasis is placed on the uncontrolled domain. In other words, if read to narrowly the GDPR is looking for failures to achieve privacy within the operation, rather than extend this to areas where tags can continue to be read. This is in marked contrast to views expressed a few years ago by members of the Article 29 Working Party when they were participating in an RFID Expert Group set up by the European Commission. There was a quote at the time of being “tracked by my shoes”; all of this was well ahead of sports shoes being linked to phone apps. It also differs from some US state laws where any form of eavesdropping and illegal reading RFID tags is considered a criminal offence.

Consent
Paragraph 3 of Article 7 Conditions for consent present some interesting challenges with the use of technologies like RFID.

3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Technology push is well known; and data subject have little choice. When credit cards were first issued there was a requirement to sign (still the norm in the USA until recent years), then chip and pin was introduced, and more recently contactless payment cards. This latest development is supported by extensive marketing efforts of the benefits of the technology with little mention of the downsides. One of the unforeseen consequences was the risk of cross-talking with the wrong tag, also known as card clash. We have covered this before in our newsletters. It is no coincidence that public transport organisations like Transport for London now provide specific advice.

---

2 As we reported in our newsletter just have a look on eBay and search “contactless payment terminals”. These devices don’t get there by accident.

3 We have made a copy of the promotion to avoid our readers being hacked: http://www.centrenational-rfid.com/docs/users/file/The%20CC%2OBuddies%20_%20Contactless%20Infusion%20X5(1).pdf

The consent that any older reader of this discussion first provided when signing up to use a credit card did not then extend to such cards being contactless. The new card just arrives, and unsurprisingly has all the features to support contactless payment. It is also difficult to opt-out of having a contactless card, but still retain the benefits of having a credit card. A survey undertaken by the UK consumer group Which? shows that contactless cards are automatically sent out⁵. While it seems possible to opt-out, the clause for doing so must be in exceedingly small print, because it does not seem to be on the author’s credit card statements.

Of course it is not just about consent and contactless cards. As RFID is introduced to new applications (e.g. libraries, retail, employee id badges, airline baggage, toll payments, etc – the list is almost endless) the general assumption by the RFID operator is that that is a good thing and technological progress. But how much thought is given to the risks and the need for consent? Card clash was not a risk initially identified, yet the very nature of RFID protocols have been designed to read multiple tags a second. So as soon as two card providers adopted smart card, card clash was inevitable. But it was quite easy for each provider not to take responsibility.

Consent is an even bigger challenge with children. Paragraph 1 of Article 8 Conditions applicable to child’s consent in relation to information society services states:

1. Where point (a) of Article 6(1) applies, in relation to the offer of information society services directly to a child, the processing of the personal data of a child shall be lawful where the child is at least 16 years old. Where the child is below the age of 16 years, such processing shall be lawful only if and to the extent that consent is given or authorised by the holder of parental responsibility over the child.

Member States may provide by law for a lower age for those purposes provided that such lower age is not below 13 years.

There have been examples around the world, where school authorities have thought it a great idea to either directly tag children, or their school bags, to make registration easier. A school in Texas is one example⁶. Little or no thought has been given to the need for consent. This article from Wikipedia⁷, shows the variety of technologies being used. They each have different privacy risks. In our opinion, little has been done to understand the implications of RFID for this type of application.

There are some reasonable RFID applications that focus on children. One example is the use of RFID bracelets within an amusement centre. Applied correctly this can enhance the visit by identifying shorter wait times for some events and is useful for identifying a lost child. Another application is the RFID tagging of new born babies, where the system can be used to trigger alarms to prevent kidnapping, no matter how rare. Both applications should require parental consent and be supported by a rigorous PIA process. Most importantly, the time span that any child’s data record is on the system should be minimised.

---

⁵ http://www.which.co.uk/money/banking/banking-security-and-new-ways-to-pay/guides/new-ways-to-pay/contactless-cards
From Consent to Transparency

As we have already mentioned, a significant challenge with adding RFID to an existing application is that there can be an over-emphasis on the benefits as illustrated by this future looking 10-year old cartoon 8.

The right marketing package, or poor analysis as with school children being tagged, makes it easy to ignore concerns.

There are three articles about transparency in the GDPR that are relevant to RFID:

- **Article 13** Information to be provided where personal data are collected from the data subject
- **Article 14** Information to be provided where personal data have not been obtained from the data subject
- **Article 12** Transparent information, communication and modalities for the exercise of the rights of the data subject

Paragraph 1 of Article 13 states:

> 1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

---

8 © David Farley, included with the artist’s permission https://www.ibiblio.org/Dave/Dr-Fun/df200601/df20060116.jpg
There are RFID applications where the person carrying the RFID tag can be uniquely identified, whether this is from an employee badge, membership card, smart card, or travel card. There are three types of identification from the tag:

- Any encoded personal data, or personally identifiable data on the tag including any identifier code, which can be the starting point for creating a profile.
- Any such data that might be encrypted or obfuscated, where encryption is not an inherent part of the communications protocol. Very few RFID air interface protocols support encryption, so in such protocols all that happens is that the encoded data gets scrambled and is just a bit more difficult to interpret when there are only a few examples. Increase the sample size and any hacker will crack the code. The reality is that in true open systems, there is no option but to expose the encoding rules so that some other organisation in the sector can read the tags.
- Many RFID protocols also require the tag to have a unique identifier created at the point of manufacture. While this can be quite remote from being as obvious as a person’s name in plain text, it can be the first step to profiling. If the Court of Justice of the European Union can rule that a dynamic IP address can be personal data, then the question arises – but not tested – whether a permanent and unique chip identifier is similar.

This all centres around the risk of profiling as mentioned in point (f) of paragraph 2 of Article 13:

(f) the existence of automated decisionmaking, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.

Some years ago privacy advocates in the US library community where concerned about the risk of hotlisting outside libraries. The scenario put forward was that because of the location, any captured RFID data could be used to create a meaningful list, which could subsequently be processed to extract relevant data. The issue in not whether the RFID identifier, per se, is sufficient to identify an individual, but whether it can be combined with other data to do so.

Article 14 provides detailed conditions for the situation where “personal data have not been obtained from the data subject”. We think that this raises interesting issues where data is collected automatically. A contactless card identifier is issued by a card provider, but in a contactless payment transaction has to be captured at the point-of-sale by the retailer. Following the strictest Payment Card Industry rules this should be a transient identifier in the payment terminal and then no longer be available once the transaction has been processed. A set of fine lines then emerges. For a refund to be provided the original card details need to be provided. If part of the card provider’s system this is justified, but what if the retailer holds the information? Some retailers have been known to go further and card details are kept for longer periods, as various hacks have shown.

The GDPR and RFID Applications: The Implications of Consent and Transparency

The situation is not limited to contactless payment cards, but to any type of RFID identifier where a service or product is provided by a party other than the original provider. Examples might include cross service membership cards, employee cards used for other services, airline baggage identifiers provided by one airport or provided by another. As a really up-to-date example about airline baggage, there are indications of Uber collecting and delivering luggage independently of carrying the passenger. There are other such services, some in Japan are over 10 years old. Not only should the tag provider assess the privacy risks, but so too should additional service providers.

Article 12 states in paragraph 1:

1. The controller shall take appropriate measures to provide any information referred to in Articles 13 and 14 and any communication under Articles 15 to 22 and 34 relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child.

There are thousands of RFID applications in Europe. How many of our readers have seen such notifications? The PIA process specified in EN 16571 produces a detailed report of the PIA process. The software from CNRFID-CSL\(^\text{10}\) produces a detailed internal report for the RFID operator to enable privacy enhancements to be applied and a PIA summary report for users. This summary includes:

- Operator details
- Application description (overview)
- Data on the tag
- Countermeasures applied by the operator
- Countermeasures the individual should apply
- The risk score

As such it provides the core input for EN 16570. This standard additionally addresses the:

- Placement of RFID Signs notifying the presence of RFID interrogators;
- Notification of multiple applications in an area, such as in public areas such as shopping malls, public transport stations;
- Notification of the presence of tags on or in items;
- Use of the common RFID emblem.

The emblem is intended to appear on products, RFID cards and the notifications, with a minimum size of 5mm X 5mm on products.

The emblem and other notification mechanisms should be the basis of the availability of transparent information about the RFID operation.

\(^\text{10}\) http://rfid-pia-en16571.eu/why-use-the-software/how-it-works/