



# **RFID usage and informed consent**

Using and removing of RFID functionality

by Andreas Krisch

Version: 1.0

## Contents

<a href="#">1 Preface.....</a>	<a href="#">3</a>
<a href="#">2 Information on RFID use.....</a>	<a href="#">3</a>
<a href="#">3 Retaining or Removing RFID functionality.....</a>	<a href="#">5</a>
<a href="#">3.1 Opt-in vs. Opt-out.....</a>	<a href="#">5</a>
<a href="#">3.2 Removal, data-alteration, modification of functionality.....</a>	<a href="#">6</a>
<a href="#">3.2.1 Modification of functionality (deactivation).....</a>	<a href="#">6</a>
<a href="#">3.2.2 Data alteration.....</a>	<a href="#">6</a>
<a href="#">3.2.3 Disablement.....</a>	<a href="#">7</a>
<a href="#">3.2.4 Removal.....</a>	<a href="#">7</a>
<a href="#">3.3 Responsibility for removing RFID functionality.....</a>	<a href="#">7</a>

## 1 Preface

As the results of the European Commission's public online consultation showed, a majority of the respondents feel that there is insufficient information available to make an informed analysis of RFID technologies<sup>1</sup>. Furthermore the use of RFID technology raises a lot of privacy concerns. For instance when used in supermarkets “66% asked for a clear indication of the presence of a tag”.<sup>2</sup>

Therefore it is of special importance, that reliable, accurate and understandable information on the implications of RFID use is provided and provisions to protect individuals privacy rights are in place.

## 2 Information on RFID use

Information on RFID technology and RFID use should be provided on two levels: First there is a need for general information on the technology, how it works and what potentials it provides in terms of benefits and risks. Ideally this information should be provided by an independent body, having no commercial interests in the deployment of RFID technology. To provide this information to the general public, it will be necessary to use various means of communication. This may be websites, brochures, leaflets, documentary films and the like.

Secondly individuals need information on the use of RFID technology wherever they are confronted with this technology. This includes on the one hand information on the presence of RFID readers and Tags and on the other hand information on which information is processed for which purposes by the RFID system in place.

Information on the presence of RFID readers is of special importance for individuals that carry RFID tagged objects, since this is the only way they can be made aware that the information stored on their objects can potentially be read by an RFID application in their surrounding.

To inform individuals of the presence of RFID systems, the use of a RFID Logo could be an appropriate solution. Such a Logo should not only be used to indicate that RFID readers are operated in a certain area but also to indicate that a certain object is equipped with an RFID Tag. The latter is necessary to give individuals a possibility to easily distinguish tagged from untagged objects, without which any object has to be considered to potentially carry an RFID tag.

The meaning of this Logo should be restricted to the mere indication that RFID technology is in place. Attaching more meaning to a Logo (for example: if data is only checked to grant access to a restricted area or if data will be collected and stored permanently or if personal data is involved at all) would require the creation of a series of Logos and most likely rather lead to confusion than accurate information.

Other relevant information, like the compliance of a given RFID application with certain privacy standards, should be indicated by other means or additional Logos. The

---

1 Results of the Public Online Consultation on Future Radiofrequency Identification Technology Policy "The RFID Revolution: Your voice on the Challenges, Opportunities and Threats", SEC (2007) 312

2 *ibid.*

compliance with privacy standards for example could be indicated with the European Privacy Seal<sup>3</sup>, after passing the required auditing process.

As defined in the relevant European Data Protection legislation the processing of personal data requires the informed consent of the individual. Therefore any RFID application processing personal data not only needs to be registered with the data protection authorities but also has to provide detailed information on the information processed and the purpose of this processing.

Therefore any processing of personal data by means of RFID technology (for example analysis of customers movements in a supermarket) is not only subject to prior approval by the data protection authorities but also to explicit informed consent by the affected individuals.

When an RFID Tag remains active after an individual gained its ownership or possession (which includes the rental of objects), detailed information has to be provided on what information is stored on the Tag and by whom this information can possibly be accessed (is it freely accessible by anyone or are access restrictions – if yes, which? – in place). This information is needed by the individual since he or she has to decide on this basis if he or she is willing to enter any “RFID enabled areas” while being associated with this object. Additionally general information on RFID technology and its potential benefits and risks might be required at this stage, depending on the knowledge of the individual.

The means by which the individual is informed about the details of the RFID technology, the application in question and the information stored on the Tag may vary depending on the circumstances.

When a Logo is used to indicate the presence of a RFID reader, it might be an option to also provide information on the purpose of the data-collection and on the data processed, together with the Logo on a label<sup>4</sup>. The information provided on the label should however be standardised to avoid confusion. More detailed information on the application can then be provided on an additional leaflet or via other means.

Depending on the size of the object to which the RFID Tag is attached it might be possible to provide information about the data stored on the Tag directly on the object or it's packaging. For smaller objects the use of a leaflet might be the better choice.

Whatever means of communication is chosen to inform the affected individuals it is important to ensure that the individual is fully aware of the potential consequences when giving his or her consent to the processing of personal data.

---

3 The European Privacy Seal (EuroPriSe) is a European project funded under the eTEN programme, introducing a privacy certification procedure for IT-products and services. It transfers the very successful Privacy Seal offered by the Independent Centre for Privacy Protection Schleswig-Holstein (Germany) to the European level and offers certification on a purely voluntary basis. EuroPriSe currently is in the pilot phase in six EU member states. For more information see <http://www.european-privacy-seal.eu/>

4 For the possible amount of information on a rather small label see for example the energy consumption labels for household appliances (<http://europa.eu/scadplus/leg/en/lvb/l32004.htm>)

### **3 Retaining or Removing RFID functionality**

When an individual gains the ownership or possession of an RFID tagged object, the question arises what should be done with the Tag and which behaviour should be the default.

Actions that can be taken are to remove the Tag, to alter the data stored on it or to modify the functionality of the Tag so that it completely and irrecoverably ceases to transmit information. Finally the Tag and the data stored on it can remain unchanged.

Options for the default behaviour are, that an action to alter the Tag or the data stored on it is taken on explicit request by the individual (opt-out) or that this action is taken by default unless the individual explicitly requests different (opt-in).

#### **3.1 Opt-in vs. Opt-out**

When an individual gains the ownership or possession of an RFID tagged object, the default procedure should be to permanently remove the RFID functionality from the object. Only when explicitly requested by the individual the RFID functionality should remain functional for further usage (opt-in).

The benefit of an opt-in regime is, that it by default protects individuals even when individuals do not fully understand RFID technology and its implications on their personal data or privacy. Since there are until today no sufficient mechanisms in place to enable individuals to control access to data stored on RFID Tags, individuals have to understand completely, what it means to leave RFID functionality attached to an object in place. In most cases (for example in the retail environment) it will not be possible to properly inform every individual which implications it will have to leave RFID functionality active.

Therefore European Digital Rights strongly asks for an opt-in regime and a removal of RFID functionality from objects unless the affected individual requests different!

It is important to note that the implementation of an opt-in regime does not hinder the implementation of "post-sale" RFID based applications and services (like for example the intelligent refrigerator). Providers of such applications and services that offer significant benefits for their users will certainly be able to communicate these benefits properly to the interested individuals, which then always are free to explicitly opt-in to RFID use.

Given the current state of technology, which provides no means for the individual to decide which applications or services should be allowed to access data on an RFID Tag, it is necessary to take a decision on a general level. This should rather be done by an explicit informed opt-in to the use of this technology than by an opt-out setting that requires each individual to be knowledgeable about RFID technology to determine if his or her privacy is protected in a way that suits his or her individual preferences.

Furthermore it is essential to ensure, that individuals always have the opportunity to exercise their legal rights, regardless if they choose to opt-in or opt-out to RFID use. Legal guarantees for example must always be provided, be they claimed with paper-tickets or RFID Tags.

## **3.2 Removal, data-alteration, modification of functionality**

Current RFID technology basically provides three mechanisms to remove or reduce RFID functionality on a given RFID Tag. These three options are the removal of the Tag, the alteration of data stored on the Tag and the modification of the Tag's functionality. A fourth option would be to temporarily disable a Tag, but this seems not to be properly supported by current RFID technology.

### **3.2.1 Modification of functionality (deactivation)**

The modification of Tag functionality (the so called deactivation) via a “kill” command alters the RFID tag in a way, that it ceases to transmit any data. Regarding the large scale deployment of this option critics say that it on the one hand takes much more time to disable or kill a Tag than to read it (it is said to take approx. four times the read time) and that it would not be practical to do this in large quantities. And on the other hand that not every RFID Tag provides appropriate functionality to be deactivated.

While maybe the option to deactivate RFID Tags is not feasible in every environment, it might be an option in environments where only low quantities of RFID Tags are to be deactivated. It is however important to ensure, that the burden to deactivate the Tag is not put on the individual gaining ownership or possession but on the person or organisation providing the RFID tagged object. This also applies if there are low cost deactivation devices (so called RFID Zappers) available, since it is still cheaper and more effective to operate one such Zapper at the person or organisation providing RFID tagged objects, than to equip every individual with such a device. For the question of responsibilities for introduced technology please see chapter 3.3 below.

### **3.2.2 Data alteration**

The alteration of data stored on a Tag (by some stakeholders called disablement) aims to reduce the amount or accuracy of information stored on a Tag. For example an object's unique identifier could be removed while other information on the object will still be stored on the Tag and transmitted to RFID readers. Technology providing this functionality is said to be very expensive, which hinders a large scale deployment.

From a privacy point of view this kind of data alteration is anyway not sufficient for the protection of individuals, since it is still possible to automatically collect data on which objects an individual has in his or her possession when entering the operation area of an RFID reader. Depending on the objects a person carries with him or her this information can still be seen as being sensitive.

Therefore European Digital Rights asks to not support this kind of data alteration as a means of privacy protection. Especially it should be avoided to attribute this procedure with the term “disablement”, since this term is in common sense connotated with the meaning of changing to a temporarily not functional state and will therefore lead to the assumption, that the RFID Tag is not transmitting any information to RFID Readers in its surrounding, which definitely is not the case with this concept.

### **3.2.3 Disablement**

The disablement of RFID Tags means to alter their functionality to being temporarily not working. A disabled Tag transmits no data to RFID readers unless it is enabled again. As it seems, sufficient RFID functionality to temporarily disable Tags unless they are enabled again by an authorised party (for example the owner or possessor) is not available as of today.

As already mentioned earlier in this document future developments of RFID technology might provide sufficient means for individuals to control access to data stored on RFID Tags. One such means could be to temporarily enable an RFID Tag for being accessed by a certain application and then disable it again. Such a functionality would allow individuals to use RFID applications they feel to be beneficiary and to avoid such that they do not want to use.

With regard to the disablement of RFID Tags it is important to ensure, that only the authorised party is able to control the state of the Tag (enabled or disabled). To this end additional solutions, providing interfaces to manage all RFID Tags in one's possession, are required.

### **3.2.4 Removal**

The technically simplest method to remove RFID functionality from an RFID tagged object is to remove the Tag from the object. This only requires, that the Tag is attached to the object in a way that it can be easily removed (for example on a floating sticker).

Given the technological and practical difficulties with other mechanisms to remove RFID functionality from tagged objects, it seems that the removal of RFID tags is currently not only the most practical but also the cheapest and most reliable method to ensure that individuals are protected from unwanted RFID technology.

## **3.3 Responsibility for removing RFID functionality**

Regardless whether an opt-in or an opt-out regime for RFID functionality is chosen, the question arises who should be responsible to remove the functionality from an object.

There are basically two options available. On the one hand it could be the obligation of every individual to remove unwanted RFID functionality from the objects in his or her possession. On the other hand it could be the obligation of the persons or organisations that provide objects with RFID functionality to remove this functionality.

As already stated earlier European Digital Rights strongly asks to implement an opt-in regime for RFID functionality. This also implies that the burden to remove this functionality could not be put on the individuals, that most likely are not knowledgeable about this technology and do not have the necessary means to accurately perform this task.

Therefore the responsibility to remove RFID functionality from objects should be put on the persons or organisations that introduce this technology. These entities are not only most knowledgeable about the technology, since they are the ones who introduced and regularly use it, but they also know exactly where on an object a Tag is located, since they put it there in the first place.

This distribution of responsibilities should not only apply for the relationship between consumers and providers of RFID tagged objects but also for the relationship between manufacturers, wholesalers and retailers. Whoever in this supply chain introduces RFID functionality should be as well responsible for removing it. It however should be possible to pass this responsibility to the next level in the chain. If for example a wholesaler is ready to use RFID functionality and therefore accepts RFID tagged objects from manufacturers, then the wholesaler is responsible to remove RFID functionality from objects when passing them to retailers that are not willing or able to deal with this technology.

Given this chain of responsibilities it is possible to put the burden of removing RFID functionality even on very small retailers, since they only will get RFID tagged objects when they are ready to deal with it, which includes the ability to remove the functionality if necessary.

This concept of responsibilities is as it seems also consistent with the current practice regarding electronic article surveillance tags. Obviously it is already possible to ensure, that these tags are deactivated or removed properly after an item is bought by an individual, so that theft protection systems in other stores do not activate an alarm when this item passes their systems.

Furthermore individuals certainly expect that those parties that introduce a certain technology also ensure that this technology is secure for everyone confronted with it. For example it is reasonable to expect that providers of credit card payment systems for supermarkets take care to protect this system from fraud and misuse. Nobody will expect the individual, using this system for credit card payments of his or her purchases, to personally ensure the level of security he or she wishes to enjoy. The same should be true with RFID technology: by default a maximum protection of the individual and his or her privacy should be the responsibility of the party that introduces the technology.