



Issue Paper on Data Protection and Privacy – Comments by Informationsforum RFID e.V.

July 2007

The Informationsforum RFID welcomes the opportunity to contribute to the discussion on RFID and privacy in the context of the RFID Expert Group of the EU Commission. The protection of privacy is a key issue when implementing RFID in the consumer sphere. In this context, it is particularly important to clearly distinguish the type of data stored. Whenever personal data is stored by means of RFID technology the European data protection laws apply. However, many applications only store non-personal data such as product codes. While data protection laws do not apply to these applications, self regulatory measures may help to inform consumers about RFID technology and provide for transparency and consumer choice.

As RFID technology is the basis for a large variety of applications, general statements about privacy are impossible. Rather, it is important to judge each application by itself and by the specific data it collects or stores.

As regards the Issue Paper on Data Protection and Privacy presented to the Expert Group, the Informationsforum RFID would like to raise the following points:

INFORMING THE PUBLIC ON RFID

The Informationsforum RFID shares the view that creating transparency regarding the use of RFID is crucial to create trust and acceptance for the technology. Already various activities exist to inform the public about RFID. One example for a private sector initiative is the website www.rfidabc.de provided by the Informationsforum RFID. It educates consumers about the technology and its applications and addresses potential concerns regarding privacy and consumer protection.

- As regards **codes of conduct** there are examples of existing guidelines established e.g. by EPCglobal or the International Chamber of Commerce. On the national level there is an ongoing discussion in Germany regarding a code of conduct for the retail sector involving in particular GS1 Germany and the German consumer protection organization vzbv. In drafting the European Policy Outlook, stakeholders agreed on the following key elements for a code of conduct: (1) Information and awareness, (2) labelling, (3) compliance with data protection laws, (4) deactivation, and (5) choice.

The element of deactivation is particularly relevant in a retail scenario where consumers need to have the choice to deactivate tags after the purchase. However, this will only be necessary after introduction of item-level tagging. In many other application areas deactivation would not be in the consumer interest, e.g. when sensor tags serve to monitor food safety or RFID is used in electronic car keys or for purposes of identifying emergency personnel in critical environments. This example shows that a general code



of conduct will most likely not be the right choice given the wide variety of application scenarios for RFID.

In addition, any guidelines to be drafted today must be sufficiently flexible to adapt to the technological development and the timing of implementation. Therefore, the Informationsforum RFID cautions Member States and other stakeholders against providing detailed guidance at this point in time that exceeds the above-mentioned general elements of a code of conduct. Rather, a collection and evaluation of existing guidelines and codes of conduct might be a good way to identify best practice cases to serve as example for successful implementation of privacy codes of conduct.

- As far as the **use of images or icons** is concerned, the Informationsforum RFID agrees that this might be a good way to alert consumers to the presence of RFID tags and, thus, create the necessary transparency. EPCglobal in its guidelines requests the use of the EPCglobal logo for this purpose. However, it should be debated whether the use of icons should cover all potential applications of RFID in the consumer sphere or should be restricted to scenarios of particular concern from a consumer protection perspective. Otherwise, there is a risk that consumers will cease to notice the logo or icon.
- Concerning the **rights and freedoms of natural persons**, the Informationsforum RFID would like to reiterate that they are already protected by general data protection laws. These provide for obligations to inform natural persons about the collection of their personal data and to obtain the necessary consent. Data protection officials both on the Member State and the EU level monitor and enforce compliance with existing laws. In addition, in Germany there are data protection commissioners within the private sector, who are tasked with monitoring their companies' compliance with data protection laws.

PERSONAL IDENTIFICATION

- The current data protection framework provides a clear definition of personal data as any information relating to an identified or identifiable natural person. **Uncertainty as to the character of processed data** should be addressed by this definition and by the instruments offered by data protection laws. For example, non-personal data such as a product code turns into personal data if and when it is linked to a natural person through the use of a loyalty card at checkout.

Admittedly there is some concern that the large number of data collected in future ubiquitous computing scenarios may create challenges in terms of deciding when non-personal data turns personal. However, the mere fact that more and more data may be stored in the future does not warrant changing the definition of personal data. Rather, this issue needs to be addressed by discussing ways to comply with data protection laws even in such environments and ways to enable consumers to protect their personal data. Privacy-enhancing technologies offering e.g. automated consent models or on/off modes can strike a balance between protection of personal data and the added convenience ubiquitous computing solutions will provide.



Finally, it is important to bear in mind that privacy laws are and should remain technology-neutral. Even when in single cases the distinction of the type of data involved might be a challenge, the possible compilation of personal profiles is not a matter of the technology used to collect data, but rather regards the back-end system used to store and – if applicable – combine the data. Current laws do not allow for establishing user or consumer profiles without prior consent. This will not change when RFID will be in widespread use.

- **Member States** have a significant role in monitoring and enforcing compliance with data protection laws and in providing policy advice regarding new technologies used to collect and store personal data.
- The **tracking of identified natural persons** e.g. as patients or workers falls under the scope of existing data protection laws. Thus, it is only permissible with the consent of the person concerned.

PRIVACY-FRIENDLY AND SECURE PROCESSING OF PERSONAL DATA

Ensuring privacy and data security is of utmost importance in an environment in which more and more personal data is collected and processed. Given the sensitivity of the public when personal data is found to be disclosed, organizations controlling personal data have a vital interest and a legal obligation to ensure security through technical and organizational measures.

- It can be expected that the large majority of RFID tags to be used in the consumer sphere will be passive tags with very limited memory. Especially in the retail context, transponders will contain nothing but an electronic product code referring to a product identified in a database. Even in scenarios where sensitive personal data is concerned such as in hospitals, tags themselves usually do not contain personal data. Rather, the patient data is stored in a hospital database, as it is the case today, while the tag contains merely a unique identifier.

Therefore, the **risk of data being compromised** does not present a new challenge and is not uniquely connected with the use of RFID. As in existing database solutions, it is the responsibility and the legal obligation of the data controller to protect personal data against unauthorized disclosure.

- While the law is an important tool to protect personal data against unauthorized collection it can usually only punish offences after they have been committed. Therefore, it could be beneficial to complement the legal framework with measures protecting privacy that are built into the technology. **Privacy-by-design** and privacy-enhancing technologies (PETs) play an important role in this context. In addition to data protection laws, PETs can also contribute to enhance awareness for and increase trust in technologies.
- As regards the **appropriateness of technical and organizational measures** one must bear in mind that RFID technology and applications develop very quickly. Therefore,



there is the risk that anything but very general criteria for the appropriateness will not keep up with technological developments and implementation of the technology.

MONITORING AND ENFORCEMENT

- Europe has a high level of data protection that sets an international standard. No personal data can be collected or stored without the consent of the person affected. Persons also have rights to information and the right to deletion of the data collected. The EU Data Protection Directive and the corresponding data protection laws in the Member States already cover the fields of application and possibilities for the use of RFID in which personal data is processed.

In line with the fundamental principle of technology neutrality, **the current legal framework** offers sufficient possibilities to address violations independent of the technology used to collect or store personal data. Information technology and the internet in general pose a challenge to the enforcement of privacy rules. However, rather than changing the law, it is necessary to address these challenges through a combination of law enforcement, self-regulation, technological solutions and consumer education.

- It is said that applications in the field of ubiquitous computing will pose challenges to privacy that can no longer be addressed by existing legal measures such as information and consent. Therefore, it is possible that future scenarios will lead to a debate about the adaptation of privacy laws to a new technical environment. Hence it will be important to monitor technological developments in this area, but it is not possible to develop prescriptive legislation that will not endanger future innovation. Ubiquitous computing is a vision that will take a long time to realize and it is still much too vague a concept to address with legal provisions. Against this background there is no need for any **further provisions** to be added to the existing legal framework.

SPECIFIC SCENARIOS

As stated above, the technological and privacy challenges in the use of RFID can only be addressed on a **case-by-case or application-specific level**. Even a sector-specific approach, e.g. for the use of RFID in the health care sector, might be too broad to deliver satisfactory results. Therefore, an exchange of best practices and possibly joint pilot programs offer the best chance to assess specific challenges.

As with any innovation, trying to address any possible open question beforehand might thwart its potential for consumers, businesses and society alike. Therefore, the European Commission and the Member States should encourage real-life applications of RFID in order to assess the need for further research, consumer education, regulation, or stakeholder dialogue.