



Deutscher
Industrie- und Handelskammertag



INFORMATIONSFORUM RFID



Verband der
Automobilindustrie

EU Recommendation on RFID Privacy and Data Protection – Requirements for Implementation –

November 2009

On May 12, 2009, the EU Commission adopted a Recommendation on the implementation of privacy and data protection principles in applications supported by radio-frequency identification (2009/387/EC). The Recommendation is addressed to the EU Member States and is geared towards ensuring the privacy-compliant application of RFID technology. To support the implementation, the EU Commission created an Informal Working Group with members from business, academia, standardisation, and data protection and consumer protection organisations.

As representatives of the German private sector, the German chapter of AIM, the Federation of German Industries (BDI), the Federal Association for Information Technology, Telecommunications and New Media (BITKOM), the Association of German Chambers of Industry and Commerce (DIHK), GS1 Germany, the German Retail Association (HDE), the German Brand Association (Markenverband), the German Association of the Automotive Industry (VDA), and Informationsforum RFID request to make sure in the context of implementation that the planned measures do not result in unintended and undue burdens for businesses. Establishing high barriers for the broad introduction of the technology at this point in time jeopardizes the further deployment and the development of innovative applications.

A major weakness of the EU Recommendation is the lack of differentiation between applications that process personal data and those that do not. The current discussion already shows that the scope of the Recommendation is an issue of particular relevance, which will have to be especially addressed in the evaluation of the impact of the Recommendation. Therefore, in the upcoming implementation it must be ascertained that the necessary protection of an individual's privacy does not result in additional requirements for applications that do not process personal data and, thus, causes market entry barriers for operators. Finally, the implementation should not assume only risks for consumers; rather, potential benefits for citizens and consumers should be part of the risk analysis as well.

The following points are critical for a successful implementation of the Recommendation:

- Minimal requirements as regards privacy impact assessment (PIA) and information policy for applications that do not process personal data
- Involve the internal data protection officer as competent authority in the PIA context
- Develop a flexible PIA framework allowing for a differentiated classification of RFID applications
- Use sector specific templates for PIAs
- Ensure confidentiality of business secrets
- Informative and appropriate notification about presence of readers and tagged products
- Retail: Standard deactivation and deactivation upon request as equally valid solutions depending on the PIA result

These key points are based on the following considerations:

PRIVACY IMPACT ASSESSMENT (PIA)

Under paragraph 5 of the EU Recommendation all RFID operators should assess the implications for the protection of personal data and privacy before the deployment of a new application. This should include whether the application can be used to monitor an individual. The level of detail of the assessment depends on the possible privacy risks of the application. Operators should take appropriate technical and organisational measures to ensure data protection. The PIA should be made available to the competent authority at least six weeks before the deployment of the application.

Comment:

- Scope

RFID operators in the B2B area are especially critical of the wide scope of this Recommendation. Applications e.g. in logistics or manufacturing can as a rule be considered not problematic concerning the protection of privacy; conducting a PIA in these cases means additional effort without any benefit for consumers. Therefore, it is a key request that in the implementation there must be a clear distinction between applications that process personal data and those that do not. For the latter, a notification to the internal data protection officer should be sufficient to comply with the PIA requirement. For applications with reference to individuals it is necessary during the PIA process to come up with a clear differentiation to adapt the level of detail to the potential privacy risk.

- Competent Authority

It is unclear who should be the recipient of the impact assessment in Germany. Under section 4g of the German Federal Data Protection Act the internal data protection officer supervises the correct application of data processing programs processing personal data; to this end he must be informed in time about schemes of automated processing of personal data. As the PIA is designed to ensure the protection of personal data, it would make sense for the PIA report to also be presented to the internal data protection officer.

- Confidentiality

The Recommendation does not contain statements regarding the protection of the confidentiality of sensitive business information. As the detailed description of an RFID application and the data flows can contain business secrets, it must be ensured that the description can be sufficiently abstract to avoid negative consequences for the operator.

- Existing Applications

A retroactivity of the Recommendation should be excluded, i.e. a PIA should only be conducted for newly-established applications.

PIA FRAMEWORK

To support the PIA implementation, industry in collaboration with civil society stakeholders should develop a framework and submit it to the Article 29 Data Protection Working Party by May 2010 (paragraph 4).

Comment:

When developing the framework it has to be ensured on one hand that the above-mentioned points will be considered already in the framework. On the other hand, the framework must be sufficiently open and flexible to enable industry associations to develop PIA templates

based upon the framework for specific sectors or applications. The requirements of the framework can be supported e.g. by the use of privacy enhancing technologies.

INFORMATION

Paragraph 7 of the Recommendation provides for each RFID operator to publish for each application information regarding the identity of the operator, the purpose of the application, the data processed, if necessary whether personal data is processed, as well as likely privacy risks and mitigating measures. Also, a summary of the PIA should be published.

Comment:

With regard to the recommended information policy it must be taken into account that operators should not be burdened disproportionately. In case the PIA comes to the result that no personal data is processed in an application, the information to be published should be restricted to a minimum as well. Especially for B2B applications it should be considered what the added value of such an information obligation can be and whether a publication is really necessary. As a rule, general information about the RFID deployment e.g. on the operator's website should suffice.

TRANSPARENCY

A common European sign should inform of the presence of readers; this sign should be developed by European Standardisation Organisations with the support of concerned stakeholders (paragraph 5).

Comment:

Notification of the presence of readers can increase transparency regarding the use of RFID especially in publicly accessible areas. However, it is necessary that the notification happens in an understandable and sufficiently informative way. In particular regarding the notification of the presence of readers, general information would most likely make more sense than e.g. a small logo directly attached to the reader. When developing the sign, reference should be made to the level of knowledge and the needs of consumers, who do not necessarily know much about the technology. As there already are existing signs in the market such as e.g. the EPCglobal logo, an RFID sign should provide for the possibility of an extension so that existing signs can be combined with the common RFID sign.

RFID IN THE RETAIL SECTOR: NOTIFICATION

Especially for the retail sector the EU Commission provides for further measures. Under paragraph 9 of the Recommendation, consumers should be informed of the presence of tags on or in products on the basis of a common European sign. The sign should be developed by the European Standardisation Organisations with the support of concerned stakeholders.

Comment:

A notification pointing out the presence of transponders in or on products is generally to be supported. In the development process it should be taken into account that the sign informs the consumer in such a way that he can exercise his right to deactivate the tag. Therefore, it is not considered to make sense to add another logo onto the product respectively the packaging. On one hand, in light of numerous other references on products or packages it is doubtful if such a logo would fulfil its purpose. On the other hand, it is questionable whether a simple logo would have sufficient information value in light of the low level of knowledge of consumers. Thus, it would make more sense to use a sign that is e.g. part of the manual and possibly also attached to the shelf, and that informs consumers about the use of the technol-

ogy. This sign as well should refer especially to the needs of consumers and provide for an extension for existing signs.

RFID IN THE RETAIL SECTOR: DEACTIVATION

In addition, depending on the outcome of the PIA, retailers should deactivate tags in or on products either by default or upon the customer's request. A default deactivation is not necessary when the PIA result shows that the used tag does not represent a likely risk to the protection of personal data even if it remains operational after leaving the point of sale. In this case, the retailer should make available free of charge an easy means to deactivate or remove the tags. The recommendation regarding deactivation applies on to retailers that are RFID operators.

Comment:

It is to be welcomed that the provisions on deactivation refer to the risks for consumer privacy and differentiate accordingly. Details should be discussed in the context of implementing the PIA framework in the retail sector. It should be pointed out at this point in time that both ways of deactivation should be equally valid; any expectation that in specific application areas deactivation generally occurs by default would be counterproductive and inappropriate. The PIA in particular is expected to provide the RFID operator with clarity regarding data protection risks so that he can minimise them. Also, activated tags on products offer benefits such as e.g. the exercise of warranty rights without an invoice, the use of intelligent household appliances, the provision of additional information for consumers or for recycling.

Finally, in the further debate regarding deactivation in the retail sector it should be considered that applications are foreseeable already today where deactivation would run contrary to the purpose of the application. In the future, RFID can help e.g. in the automotive sector or in consumer electronics to monitor the lifecycle of a product and, thus, improve product safety, functioning and finally recycling. However, stable processes for such applications require that deactivation in these cases is excluded; these issues must be debated at the latest when reviewing the impact of the EU Recommendation.