Reconciling RFID technology with data protection principles

Keuleers, Ewout

Publication date:
2005

Document Version
Publisher's PDF, also known as Version of record

Reconciling RFID technology with data protection principles

1 Avril 2005

Auteur: Ewout Keuleers (Avocat au barreau de Bruxelles - Cabinet ULYS (membre Eurojuris))
Thème: Vie privée et données personnelles
Lue par 2642 visiteurs
Citation: Ewout Keuleers, "*Reconciling RFID technology with data protection principles*", http://www.droit-technologie.org , 1 Avril 2005

The Data Protection working group of the European Commission, the so-called Group 29, recently released a working document on RFID technology and privacy issues.

Group 29 confirms that the use of low-cost Radio Frequency Identification technology (RFID) has substantial advantages in not only a number of sectors and industries, but also for individuals and public services, governments included. In addition to the more standard applications in the transport, distribution or retail sector, Group 29 underlines that RFID chips embedded in goods could also increase consumer safety.

It is clear that the wide spread implementation of RFID chips in consumer goods, such as razor blades, cars, identity cards, cell phones, etc., also triggers certain underlying privacy issues. Indeed, the ability to surreptitiously collect a variety of data all related to the same person; track individuals as they walk in public places (airports, train stations, stores); enhance profiles through the monitoring of consumer behaviour in stores; read the details of clothes and accessories worn and medicines carried by customers are all examples of uses of RFID technology that give rise to privacy concerns.

For this reason, Group 29 urges manufacturers and deployers of RFID technology to design and implement technology that is in line with the legal EU privacy framework. This framework consists mainly out of two European directives. In the first place, the data protection Directive 95/46 sets out the general principles for the processing of personal data, notably the rights of the consumer-data subject. Secondly, this general regime is contemplated by a sector specific directive. Directive 2002/58 on electronic communications and privacy deals with particular issues such as the use of hidden identifiers, e.g., RFID tags, and location data.

1. Application of general data protection directive 95/46

Directive 95/46 on the processing of personal data is only relevant to the extent that the RFID generated information is personal data. Group 29 acknowledges that this is not always the case. In some cases, tag information is not combined with other identifying material, for example someone's photograph or name and address, or with a recurring reference number.

However, one must be careful to come to this conclusion. Directive 95/46 defines "personal data" and "processing" in a very broad manner.

Processing is basically *"any operation or set of operations which is performed upon personal data* ", such as the collection, recording, organization, storage, retrieval, consultation, use, disclosure by transmission, dissemination or destruction.

According to article 2 (a) 'personal data' shall mean *"any information relating to an identified or identifiable natural person"* This also means that a person can be identified indirectly by reference to an identification number such as the one of the RFID tag. Moreover and to determine whether a person is identifiable or not, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person.

In contrast, the principles of protection do not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. In contrast to the notion of personal data, the one of "anonymous data" should be interpreted strict and one must be aware that it may be very difficult to achieve true anonymous data. From the moment a person can make a link between the 'anonymous RFID tag' and a person, even indirectly, Directive is applicable. Eventually, one may not forget that RFID tags are designed to identify goods and/or persons. Similar to the use of internet cookies, or other hidden identifiers, even if the individual consumer is not immediately and

directly identified at the item information level, he can be identified at an associative level because of the possibility of identifying him without difficulty via the large mass of information surrounding him or stored about him.

Once the use of RFID, or Electronic Product Codes (ECP), is considered as the processing of personal data the deployers, most likely to be considered as controllers, and RFID manufactures should pay attention to the legal data protection requirements.

2. Implications of the application of the general data protection directive

According to Group 29 it is not feasible to establish how all data protection requirements apply in each RFID scenario. It may be possible to give some general guidelines which data controllers can use and adapt in the light of the circumstances surrounding the data processing. Although it will be for the data controllers, e.g., deployers or distributors, to ensure the overall compliance with these requirements, Group 29 underlines that RFID manufacturers have a direct responsibility in ensuring that privacy compliant technology exists to help data controllers to carry out their obligations under the data protection Directive and to facilitate the exercise of the individual data subject's rights.

In this regard, the same EU body already recommended in November 2000 that *"the design and selection of data processing technologies, including hardware and software, shall conform to the objective of processing no or as less personal data as possible and shall facilitate the exercise of the data subject's rights".* Furthermore, Directive 2002/58 clearly states that *"it may be necessary to adopt measures requiring manufacturers of certain types of equipment used for electronic communications services, to construct their product in such a way as to incorporate safeguards to ensure that the personal data and privacy of the user and subscriber are protected"* .

Besides the general principles on data quality and the justifying legal grounds for data processing, notably the consent of the data subject, one must pay respect to the rights of the individual data subject. In particular and in order to allow the latter to exercise his rights, it is of predominant importance that the individual is informed and made aware of the existence of a RFID processing operation.

In this view, data controllers, e.g., shop owners or manufactures of consumption goods, processing information through RFID technology should provide the data subject at least with their identity, the purposes of the processing, information on the recipients of the data and the existence of a right of access. Furthermore, it can also be recommended that information is given on the means to discard, disable or remove tags from the products, thus preventing them from disclosing further information.

Eventually, one must be aware of the eminent risk that third parties shall use RFID tags for other purposes than the initial purpose determined by the data controller or for cross-profiling purposes. This re-routing of the initial purpose shall be easy to achieve when the RFID radio signal broadcasted by the RFID tag is not secured and can be read by third party readers. In this regard, Directive 95/46/EC states that all data controllers must adopt appropriate technical and organizational measures to protect personal data against unauthorized disclosure or unauthorized access. In this view, the use of Privacy Enhancing Technology (PET), notably encryption algorithms, should be welcomed.