

A banner image featuring the word "RFID" in large, white, 3D-style letters on the left. To the right, a pair of hands is shown holding a glowing green starburst shape with radiating lines, set against a background of a blue sky with white clouds.

RFID

The EU & RFID Privacy

A summary of the European Union's recommendations on RFID and personal privacy and CoreRFID's advice to users.

To address concerns over the risks to privacy and personal data protection the European Data Protection Registrar developed advice to the EU Commission. Using this advice, the Commission has now published recommendations to EU member states that will impact all implementations of RFID based systems.

What's It Got To Do With The EU?

The European Union has had a role to protect personal data and the free movement of data since 1995. It has established a Europe-wide policy on the protection of personal data. RFID represents an important potential carrier of personal data and a mechanism by which personal data can be derived from these of products tagged with RFID devices. As a result, the EU considers that the use of RFID needs measures to protect the privacy of citizens and, as a secondary consideration, believes that improving public confidence through such measures will create a climate for speedier adoption of the technology than would otherwise be the case.

What has the Commission Recommended?

The full details of the Commission's recommendations were published on 12/05/2009 as the [EU Recommendations on RFID Applications](#). In addition to this, the Commission has also published a shorter [Citizen's Summary](#) and the [assessment](#) that was developed to consider the impact of alternative recommendations.

The overall scope of the recommendations is that:

- operators of RFID systems will need to assess their potential impact on privacy and will have to protect the public against possible privacy invasions, including monitoring and reviewing protective measures.
- they will have to submit their assessments to a monitoring authority 6 weeks prior to deployment.
- they will be obliged to inform individuals of the presence of RFID readers by agreed signage.
- in retail, systems they will have to inform individuals of the presence of tags on or embedded in products.
- in retail, operators will also be required to deactivate or remove tags at the point of sale unless the assessment indicates that the data held or derivable from the presence of the tag does not constitute a threat to privacy or personal data protection.



EU recommendations will affect the use of RFID in retail most of all but all RFID systems will need to meet EU approved rules.

As a result of these recommendations EU Member States have to "develop a framework for privacy and data protection impact assessments". The framework is supposed to be developed by "industry in collaboration with relevant civil society stakeholders" and has to be submitted within 12 months. Since each of the member states are expected to develop their own frameworks, it can be expected that there may well be differences in the approaches adopted across Europe. It is not yet clear whether this will be a legislative framework in the UK or whether it will simply be a code of practice for RFID operators.

Which ever is the case the impact assessments will have to include at least the identity and address of the organisation operating the system; the purpose that the RFID application has; what data is to be processed and in particular what personal data is to be processed and whether the location of tags is monitored in relation to personal data; and an assessment of the risks to privacy and data protection as a result of deploying the system. The assessment of risks to privacy is likely to also need a definition of the steps that the operator will take to mitigate the risks and a statement of any measures that individuals should take to minimise the risks to themselves.

The assessments will need to be more rigorous in applications for the retail trade or in other areas (e.g. transport ticketing) where members of the public carry the tags. Operators of such systems will need to assess whether tags on products sold through retailers could present a threat to personal privacy or data protection. They will also need to devise ways of deactivating tags (both at the time of purchase and later) for customers that do not wish to continue to carry the tags and will have to provide consumers with a means of satisfying themselves of the fact that the tags have been deactivated. Operators will not be able to discriminate against customers that opt to have tags deactivated so that, for example, a company using RFID to track products when they are returned for service could not charge customers a higher service fee if they decide to have their product's tag disabled.

The European Standards Organisation has been charged with developing signage to inform consumers of the presence of readers and (in retail applications) tags.

More details will appear at the European Union's RFID page which can be accessed [here](#).

Issues For Systems Designers

CoreRFID has already published guidelinesⁱ on privacy in RFID systems that anticipate these recommendations. In addition to those suggestions (which continue to be relevant) organisations planning for RFID deployments need to:

1. Monitor the progress of the UK (or other national government as relevant) in creating the framework for the data protection and privacy impact assessments.
2. Consider how the Commission's recommendations on signage for readers and (in retail applications) RFID tagged products will be implemented in the planned solution

About CoreRFID

Contact us at:

CoreRFID Ltd, Dallam Court, Dallam Lane, Warrington, U.K. WA2 7LT

T: +44 (0) 845 071 0985 F: +44 (0) 845 071 0989 W: www.corerfid.com E: info@corerfid.com

ⁱ Privacy Fact Sheet : CoreRFID : Updated May 2009