



Privacy and Data protection Impact Assessment

Frequently Asked Questions

1. RFID Privacy Impact Assessment

a. What is a Privacy Impact Assessment and where does it come from?

It is a tool for companies to perform a comprehensive assessment of privacy risks and measures taken to address them before a new RFID application is introduced onto the market.

The European Commission (EC) issued in 2009 an [RFID Recommendation](#) stating that “all RFID operators” should conduct a PIA on their applications at least six weeks before the deployment of new applications. The *Recommendation* also stated that these assessments should be based on a [PIA Framework](#) endorsed by the data protection authorities in the EU Member States and industry.

b. Why do a PIA?

The RFID PIA was introduced by an EU Commission Recommendation, therefore is not mandatory. At the same time, while it has no specific enforcement mechanisms this Recommendation suggests very precise steps RFID operators should take with the ultimate goal to raise consumer acceptance of RFID technology. As a result, the EC Recommendation creates a strong expectation for the public and on EU and national legislators that encourages RFID users to comply with those provisions. GS1 recommends that all members of the EPCglobal community perform a PIA on their RFID applications as a Best Practice, regardless of what region they are in.

By performing a PIA for its application a company will:

- establish and maintain compliance with the EU legal framework and best practices on privacy and data protection;



- increase the public benefits of EPC RFID and increase customer confidence in the technology by building privacy controls in at the early stages of the specification or development process, utilizing the privacy principles of [Privacy By Design](#);
- protect the company's reputation by properly protecting customer privacy;
- ensure compliance with the [GS1 EPCglobal Guidelines on EPC for Consumer Products](#) .

c. Is it a legal obligation?

No, the requirement is contained in the above mentioned European Commission Recommendation, which is a non-binding instrument under EU Treaties that relies on the voluntary compliance and commitment by the relevant stakeholders and, in particular, all actors involved in the implementation and deployment of RFID applications.

d. Who should be doing this?

All RFID Operators should complete a PIA for each RFID application.

An RFID operator is: *“the natural or legal person [...] that determines the purpose and the means of the RFID application [..]”* (RFID Recommendation, art. 3 (a)).

In other words, the RFID operator is the entity that is ultimately responsible for the RFID application, such as the manufacturer tagging cases and pallets, the retailers tagging items for sale or the logistics provider using RFID in their services for clients. There might be many actors in a particular RFID application, but there is typically one that makes the final decisions on a particular application and that entity is defined as the RFID operator.

A tagged product might be part of different RFID applications along its lifespan, and the RFID operator will typically be different in each case: for example, a product is initially tagged by the manufacturer for its particular supply chain application, but it might also later be used by the retailer in a store, or in a different post sale RFID application (recall or recycling for example).



e. Is there a deadline?

No, the Recommendation just states that operators should conduct the PIA and make available the assessment to the competent authority at least 6 weeks before the deployment of the application. However, GS1 recommends starting to evaluate privacy risks at the beginning of the application's design phase so that privacy controls can be built in from the beginning. Starting work on the PIA at the beginning of the design phase will prevent the need for last minute corrections that could take more than six weeks to implement.

2. GS1 RFID Privacy Impact Assessment Tool

a. Why is GS1 providing the tool?

GS1 is providing this tool to assist in efficient implementation of the EC Recommendation.

b. What does this tool do?

This tool is designed to assist companies in conducting PIA according the rules set out in the [PIA Framework](#).

Collecting, processing, and storing personal information of customers or others should be done in accordance with the EU legal framework, relevant national and local laws and best practices.

c. Is this tool available for all?

Yes, the tool is available free of charge from the GS1 local Member Organisations and at the GS1 EPC Global website.



d. What are the recommended steps in the run-up to deployment?

The report based on the PIA should be made available to National competent Authorities (Data Protection Authorities) at least 6 week prior to deployment of the application. The specific means to communicate with the competent Authorities will be determined by each Authority.

e. Who needs to complete it? Which companies? Who in the company?

The PIA should be used by all RFID operators for each RFID application. The process should be completed primarily by the privacy officer and/or risk management team with input from other persons where relevant. If an application does not link an RFID tag to personal information, the PIA is easily completed by a manager of the application.

f. What Level PIA is needed?

A Full Scale PIA is required for Applications that are determined to be Level 2 or Level 3 by the initial analysis phase in Section 2.1. Examples of Applications requiring a Full Scale PIA include Applications that process personal information (Level 2) or where the RFID Tag contains personal data (Level 3). While both Level 2 and Level 3 result in a Full Scale PIA, they identify different risk environments and as such will have different mitigation strategies. For example, Level 2 Applications may have controls to protect back-end data while Level 3 Applications may have controls to protect both back-end data and tag data. Industry may further refine these levels and how they impact the PIA process with further experience.

Small Scale PIAs follow the same process as Full Scale PIAs, but given the lower risk profile a Small Scale PIA is more restricted in scope and level of detail in both the inquiry and the report than a Full Scale PIA. Small Scale PIAs are relevant for Level 1 Applications. While a Small Scale PIA follows a similar process to the Full Scale PIA, since the relevant risks of a Level 1 Application are lower than Level 2 or Level 3, the required controls and corresponding documentation in the PIA Report are simplified.



g. If I use this tool, will I be certified “RFID privacy compliant”?

No, the Tool is intended as a guide in conducting the assessment so as all the relevant issues are addressed. Companies have to make the final decision as to their compliance with relevant privacy legislation.

3. Using the GS1 RFID PIA Tool

a. What do I need to do? Where do I start? Where do I download it?

To begin a new PIA assessment, download the GS1 PIA tool (either through your local GS1 Member Organisation or the GS1 EPC Global website (links) and follow the directions on the “Instructions and Updates” page.

b. How do I assess risks likelihood, impact and effectiveness of control measures? Is this not very subjective?

Guidance is provided throughout the PIA tool to assist with rating and categorization.

4. What to do if you have further suggestions or questions

Official text of the EC Recommendation and Framework can be found on the EU Commission official website at: http://ec.europa.eu/information_society/policy/rfid/index_en.htm

We would welcome your feedback and suggestions on the GS RFID PIA Tool. Please send them to GS1 Global Office at : pia@gs1.org.

For all information on the GS1 Tool contact your local GS1 Member Organisation at: <http://www.gs1.org/contact> or GS1 Global Office at: pia@gs1.org