# Book Industry Communication Advisory on EU Mandate M/436 on RFID Privacy
## Overview of Part 1: EN 16570 and Part 2: EN 16571 (Version 1)

***Disclaimer: BIC is not a legal advisor and cannot give legal advice. Libraries and all other affected organisations should seek their own legal advice to enable them to fully comply with UK Law.***

**1. Introduction**

This advisory contains BIC's advice for libraries and their suppliers and other interested parties. It deals with the potential impact from EU Mandate M/436 on Privacy in RFID implementations, standards: EN 16570 and EN 16571. The EU has identified that privacy is important and that RFID could in some circumstances comprise a threat to privacy. Note that this is not yet in UK Law.

**2. Summary of EN 16570 and EN 16571**

These two standards if implemented in the UK would require several measures to be undertaken to protect the privacy of EU Citizens using UK libraries. Note that the standards cover all users of RFID including retail but that this applies to the library sector as well. More detailed information is available in the standards themselves although it is not yet clear if, when or to what extent the provisions of the standards will be enacted in UK law.

The standards require:

i **Appropriate signage** should be displayed wherever RFID is in use - A standardised logo will be displayed:


This logo should also be displayed on all items which contain an RFID tag. This could mean that all library books with RFID tags would have to be labelled with this logo.

RFID kiosks and devices capable of reading or writing tags must also be clearly labelled.

ii **A Privacy Impact Assessment (PIA)** should be undertaken to quantify the threat to privacy, together with any mitigation available via improved processes or technologies, and to monitor this threat and response over time.

This involves several key points:

- Who should undertake a PIA?
  - All RFID "Operators" (libraries and in some circumstances their suppliers or systems vendors).
- How is a PIA undertaken?
  - This is a very complex process involving input from suppliers, the participation of a registration agency, possibly involving the purchase of consultancy assistance or software.
  - The PIA seeks to quantify the risk given the various RFID technologies deployed, frequencies used, countermeasures (e.g. encryption) implemented etc.
  - The PIA would become a regular undertaking, triggered by any change in RFID

implementation or on a routine e.g. annual or similar basis.

- Workload associated with the PIA
  - The PIA as outlined in the standard is potentially very onerous for libraries.
  - The standard seeks to limit this burden by the use of templates, information from suppliers, the use of a Data Protection Agency and a Registration Authority and the reduction of effort on the part of smaller organisations as defined by their turnover and the number of employees.
  - An analysis process is required to define the RFID solution deployed in the library, to identify the assets, threats, vulnerabilities and thus the resulting risk.
  - The resulting calculation of risk is easy but the input analysis and the giving a value to every asset and threat etc. is complicated.
  - Several documents have to be written – Functional Statement (an initial analysis), Capability Statement (input from System Vendors), Privacy Impact Assessment Report (the main analysis of risk and countermeasures deployed), Privacy Summary (a summary of the above) and Privacy Policy (a document for public consumption to reassure library users of the measures in place to protect their privacy).

## 3. What is Privacy?

Privacy involves the protection of the EU citizen's personal data. This is information on a person's characteristics such as their religious, philosophical or political beliefs, their race, sexual orientation, health, membership of certain organisations e.g. a trades union.

## 4. The Risk to Privacy

Whilst the actual data on an RFID tag on a library book may not present a major privacy issue as it is often restricted to a barcode number or similar identifier, a book title could disclose information about the individual and the RFID tag itself may be used for location tracking or movement monitoring by appropriate equipment.

## 5. Privacy and Security

Privacy and security issues combine when for example via a library network the LMS communicates with the RFID Kiosk and the data transmitted could be seen as impacting on privacy. A threat to privacy could result from poor network security.

## 6. BIC Recommendations

1. Don't Panic (this is not yet UK law and the intention is to lobby for a reasonable implementation of the standards so that Privacy is protected but at sensible cost)
2. Don't be rushed into buying consultancy or software to analyse or calculate risk. This can wait until it comes into UK law when the detailed requirements will be made clear.
3. Don't be put off investing in RFID but ask your RFID vendor about their policy towards improving privacy capability.
4. Consider obtaining copies of the standards and informing staff and senior management.
5. Consider implementing the basic signage requirements as good practice.
6. BIC will be monitoring the situation and updates will be published at www.bic.org.uk