How to use Harmony XB5S biometric switch in order to comply with EU General Data Protection Regulation (GDPR)?

According to your organization and your activities, you may need to comply with the European General Data Protection Regulation (GDPR). In that case, a risk assessment about GDPR compliance should be conducted within your organization.

When using an *Harmony XB5S* biometric switch range, your organization processes biometric data from your personal.

The design of *Harmony XB5S* range does not allow to re-create the fingerprint image from the recorded fingerprint template, thus, reducing the risk of appropriating the image of the fingerprint.

Besides, we recommend implementing all those specific rules of utilization:

- For all versions:
    - Before installing the biometric switch, implement a process which requests systematically to the involved personal their written authorization of the use of their fingerprint template;
    - After installation, to reduce the risk of physical attack against the biometric switch, restrict the use of *Harmony XB5S* biometric switch for indoor applications, and in areas which are accessible by your staff only; and regularly check that the biometric switch's hood has not been mechanically damaged;
- For *XB5S3/4* versions (with USB port): Considering *Harmony XB5SSoft* software, to be used specifically for *XB5S3/4* devices, and to reduce the risk of malicious cyber-access to biometric data: install the software and its configuration, including the database of fingerprint templates, in a secured and hardened environment, that is a hard disk area which is encrypted, not connected to any network and on which an updated antivirus is running; archiving the database of fingerprint templates should be prohibited.
- For *XB5S5* version (connected to an operator terminal), because the operator terminal is connected to a network, the device cannot comply by design, with GDPR.