ITALY(PEAKS) Technical consultation (to-do) - Request #1028

[LIST #3] GDPR instruments compliance (GDPR □ □)

07/14/2026 10:39 AM - Kang Min

Status:	in progress (□□)	**Start date:**	07/14/2026
Priority:	□□ (critical)	**Due date:**	
Assignee:	Kang Min	**% Done:**	0%
Category:		**Estimated time:**	0.00 hour
Target version:		**Spent time:**	0.00 hour

Description

GDPR instruments compliance how the system are GPDR compliance (Labeller, Sorters, and Flextrac)

□□□□ □□ □□□□ □□□□□ □□ GDPR □□

History

#1 - 07/14/2026 10:40 AM - Kang Min

[PEAKS]

03/03: EN doesn't know if it is feasible or not. Still under evalauation about feasibility and schedule.

29/04:
1. GDPR responsibility
Under Article 32 of EU Regulation 2016/679 (GDPR), the end-user healthcare organisation is the Data Controller. The Data Controller is responsible for the security of personal data, including encryption in transit.
The end customer therefore:

defines the TLS security policy (TLS version, cipher suites, mutual TLS if required);
issues or procures the TLS certificate through its own Certification Authority (CA);
provides the certificate to the suppliers involved in the integration.

2. Product responsibility
As the manufacturer of the preanalytical system, you are responsible for ensuring that your product supports TLS according to current standards (TLS 1.2 or higher, secure cipher suites, correct trust chain handling).
This is a product requirement. It falls under the principle of privacy by design and by default set out in Article 25 GDPR.
In short:

The certificate is provided by the customer.
The technical capability to use the certificate must be provided by you.
The installation and configuration of the certificate on your system must be carried out by you, using the certificate supplied by the customer.

The same applies to the LIS supplier on its own side.

3. Impact on public tenders
We would like to draw your attention to an important point.
In Italy and in the European Union, healthcare public tenders increasingly require TLS support as a mandatory technical requirement. Lack of TLS support, or non-compliance with current TLS standards, may lead to:

exclusion from public tenders;
rejection during technical evaluation;
non-acceptance at the customer site during integration testing.

For this reason, full TLS support is not optional. It is a precondition for selling the preanalytical system into the European healthcare market.

4. Next steps
We kindly ask you to confirm:

that your system supports TLS 1.2 or higher;
which cipher suites are supported;
whether mutual TLS (mTLS) is supported;
the procedure to install and renew the certificate on your system;
the contact person on your side for the integration with the LIS supplier.

#2 - 07/14/2026 10:41 AM - Kang Min

[ENERGIUM]

20/05: The work regarding this inquiry is scheduled to be completed by end of October or the begining of November

10/06:
① Support for TLS 1,2 or higher: EN can support TLS 1,2 protocol
② Supported type of cipher suite:
Cipher suites are designed to follow the Windows operating system's Secure Channel (Schannel) policy, which operates without hardcoding specific algorithms into the program source code.
Therefore, all of the following standard cipher suites provides by default on modern operating systems, such as Windows 10 or Windows Server 2016 or later are supported.

[Key Supported Encryption Suites]
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_RSA_WITH_AES_256_CBC_SHA256

[Security and Operational Benefits]

This design allows the client's IT security team to block specific encryption suites (e.g., CBC-based suites) based on GDPR certification or internal security audit results. This can be done solely through the client server's operating system settings (registry or local security policies), without the need to update or modify our program.

If the client has internal policies regarding specific encryption suites that must be used or blocked, you can configure them at the Windows OS (Schannel) level on the relevant server. Our system will then automatically negotiate securely in accordance with those policies to perform communication.

③ Mutual TLS (mTLS) Support: mTLS is planned to be provided as an option. Procedure for System Certificate Installation and Renewal:
Development for system certificate installation and renewal will proceed either by loading the certificate (.pfx) file for registration when distributing it directly, or by specifying the registry path (Thumbprint). We will proceed with development in accordance with the answers to your questions.
For renewal, we plan to select a method that updates the certificate in memory by specifying a date or by querying the relevant path upon program execution.

[Questions]

1. Does the hospital primarily use a certificate referencing method for TLS communication, or does it mainly use the Thumbprint lookup method in the registry?

2. When encrypting data, must all data, such as specimen barcodes and patient IDs, be encrypted?

3. To what extent should historical (log) data be encrypted for mitigation purposes?

4. Is TLS 1.2 applied to all communication between internal programs, or is it applied only to communication with the LIS?

#5 - 07/14/2026 10:43 AM - Kang Min

Man-day Requirement ($300 per Day/Person): 10 weeks (2 persons)

Development Initiation Date: 2026. 06. 10

Development Completion Date: In progress

#6 - 07/14/2026 10:45 AM - Kang Min

- Status changed from Receipt ( ) to in progress ( )

#7 - 07/14/2026 10:46 AM - Kang Min

- Assignee set to KIM Dooki

#8 - 07/14/2026 12:07 PM - KIM Dooki

- Project changed from Technical consultation (to-do) to ITALY(PEAKS) Technical consultation (to-do)

- Assignee changed from KIM Dooki to Kang Min