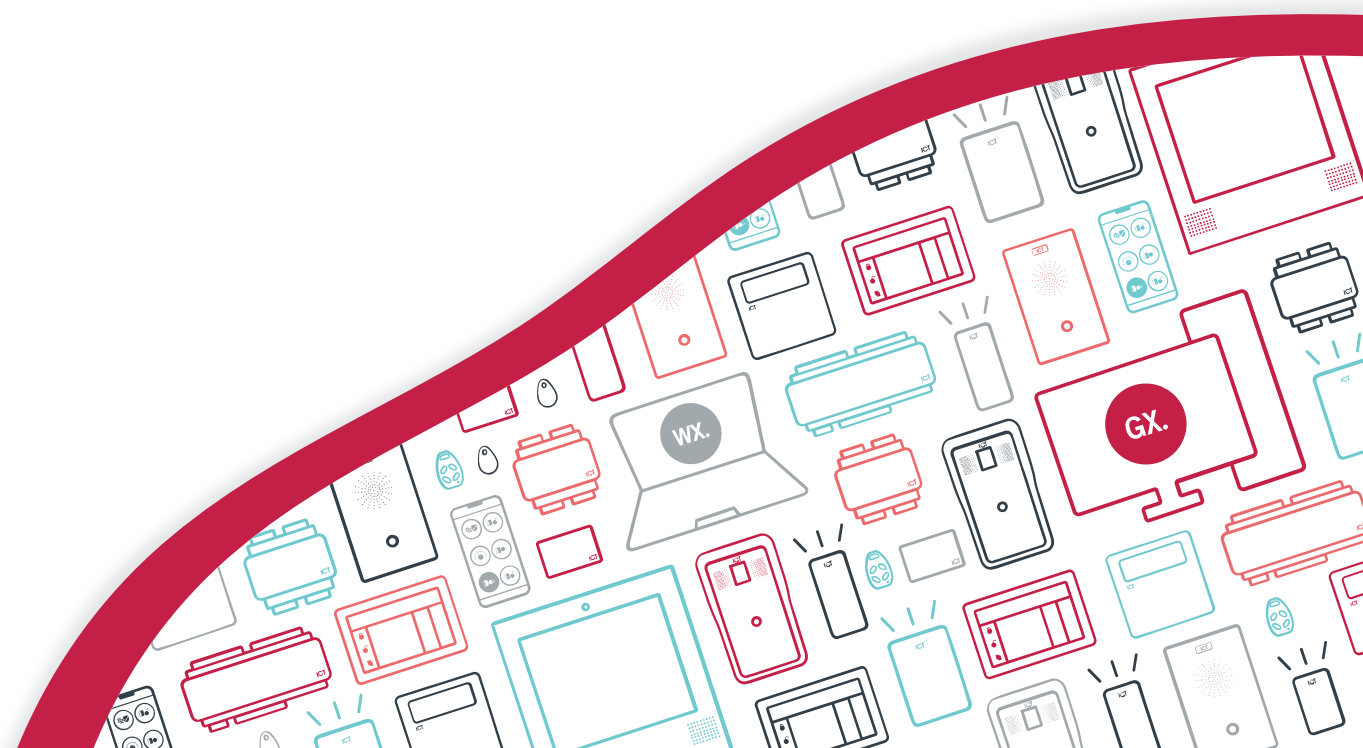
AN-258

Protege GX Compliance with GDPR

Application Note



Last Published: 11-May-22 11:13 AM

Contents

Background to GDPR 4

What Constitutes Personal Data 4

General Requirements 4

How GDPR impacts on Protege GX 5

Technical Protection Measures 5

Organizational Measures 5

Data Retention And Deletion 6

Transparent Data Encryption 6

End To End Data Encryption 7

Reference and More Information 8

Background to GDPR

The European Union General Data Protection Regulation (GDPR) replaced the Data Protection Directive 95/46/EC. This regulation aligns laws across Europe and is designed to protect the data privacy all EU citizens, enable self-management of data privacy and reshape the way organizations across the region approach data privacy.

The GDPR also applies to organizations located outside of the EU if they offer goods or services to, or monitor the behavior of, EU data subjects. It applies to all companies processing and holding the personal data of data subjects residing in the European Union, regardless of the company's location.

What Constitutes Personal Data

Personal Data is defined as "any information related to a natural person or 'Data Subject', that can be used to directly or indirectly identify the person". It can be anything from a name, photo, an email address, bank details, medical information, IP address, or an RFID tag.

General Requirements

The GDPR requires personal data to be processed in a manner that ensures its security and includes protection against unauthorized or unlawful processing and against accidental loss, destruction or damage. It requires that appropriate technical or organizational measures are used. The GDPR also details the rights of an individual regarding the provision, consent to use, upkeep, retention and deletion of their personal data.

How GDPR impacts on Protege GX

Within Protege GX, personal data items that are stored and used are usually First and Last names, and a card or tag number. Some installations may go further and add custom fields for data such as: Employee/Student ID number, DOB, Company, Department, Vehicle registration etc. All these items fall within the scope of GDPR, and therefore need to be safeguarded and managed within the GDPR's requirements.

Technical Protection Measures

Within the Protege GX system, the End to End transmission of data is secured using encryption and security features at many levels as outlined below.

- Controller - Server communications are carried out over an encrypted local area network or 3G mobile connection using NIST Certified AES 128, 192 and 256 Bit Encryption
- Controller - Module communications use an encrypted proprietary RS-485 module network
- Protege GX Web Client/SOAP Interface utilizes TLS1.2 Certificates and Encryption
- Mobile application communications to the Mobile App Cloud Server utilizes the HTTPS protocol
- MS SQL Database separation of programming and event databases
- Transparent Data Encryption is an option in MS SQL Enterprise edition only (see next page)
- Protege GX operator logins are secured using a username/password combination

Organizational Measures

ICT products are intended for use by organizations for the purpose of enabling access control and security services. Any organization administering the individual use of ICT products will need to manage the data privacy in line with any legislation, employee agreements, customer use and visitor obligations.

It is therefore the responsibility of the system owner (e.g. End user Company, Property management Company or Integrator) to implement procedural measures to obtain and manage the personal data of users within the system. Within the scope of GDPR this includes (but is not limited to) the following:

- The recording of what data is stored and transmitted
- Obtaining users' consent to obtain and use personal data
- Detailing the specific use of personal data
- Processes of personal data retention, update and deletion
- Protection and management of access to personal data (operator management and separation of duties)

Example of a Human Resource Statement or Consent Form

As part of the access control and security system in the building personal details of individuals are stored and used for event logging and tracking. The Personal information stored is used for this explicit purpose and is not transferred to any other party in any form.

The Personal data used are First Name and Last name (add others here as appropriate e.g. employee ID, Department etc)

By signing below, you acknowledge and consent that your personal data can be stored and used in this manner

Signed: _____ *Date:* _____

Data Retention And Deletion

The ability to automatically disable or delete inactive cards and/or users was released in Protege GX version 4.2.216. This allows you to program the system to automatically delete user records after specific periods of inactivity which would satisfy any retention/purge requirements. Communicating this setting to users adds to their "peace of mind" that their personal data is not being held without requirement for extended periods.

Set Automatic User Inactivity On Existing User Records in Protege GX

1. Navigate to **Users | Users**
2. Multi select the user records you want to apply this setting to. There may be some records you don't want to automatically delete.
   - To select all user records press CTRL+A
   - To select user records adjacent to each other, click the first record, then press and hold the SHIFT key, then click the last record and release the SHIFT key
   - To select individual records that aren't adjacent, hold the CTRL key and click the records to select
3. Set the Disable and/or Delete Period for the period you require

To enable Automatic User Inactivity defaults in Protege GX

Navigate to **Global | Sites | Site Defaults | User Inactivity Defaults** and select one or both options.

- **Disable Inactive Users:** Optional setting enabling you to set a period in minutes, hours or days to test for User inactivity. Any new User added to the system will automatically have these defaults applied.
- **Delete Inactive Users:** Optional setting enabling you to set a period in minutes, hours or days to test for User inactivity. Any new User added to the system will automatically have these defaults applied.

Transparent Data Encryption

Microsoft SQL provides database encryption via its TDE feature, also known as "encrypting data at rest", which is available only in the Enterprise edition of SQL. TDE protects the data in the database itself using encryption keys and performs real-time encryption and decryption during normal operation. This feature prevents data from being read where the database files may be obtained by a malicious party. They will not be able to simply restore the database files and browse the data they contain without also obtaining the encryption keys.

To Enable TDE In MS SQL (Enterprise Edition)

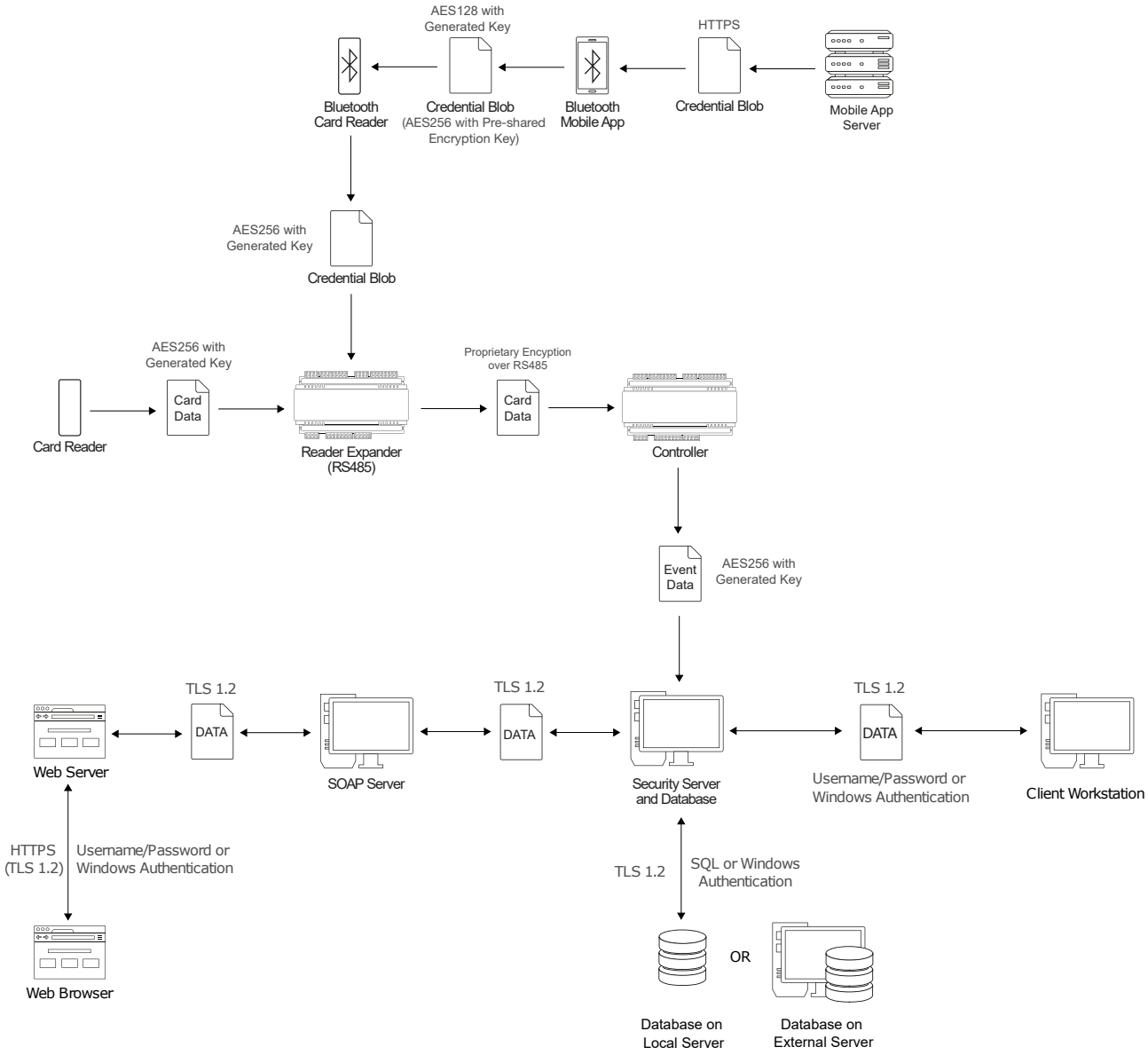
1. Create a Database Master Key in the MASTER database, if it doesn't already exist.
2. Create a certificate in the MASTER database for securing the Database Encryption Key
3. Create the Database Encryption Key in the user database to be encrypted
4. Enable TDE on the user database

It is recommended that further reading/research into the exact procedure for enabling TDE be carried out prior to implementation. See helpful links to related websites at the end of this document (see page 8).

End To End Data Encryption

The diagram below shows the end to end encryption of data for Protege GX and will help answer any questions regarding the security of data during transmission within the system.

Protege GX End to End Data Encryption



Reference and More Information

The United Kingdom's independent authority

- https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

General Data Protection Regulation

- https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

Data Protection in the European Union

- https://ec.europa.eu/info/law/law-topic/data-protection_en

Transparent Data Encryption for SQL

- https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption?view=sql-server-2017
- https://www.sqlshack.com/how-to-configure-transparent-data-encryption-tde-in-sql-server/

Microsoft Docs - How to enable TLS 1.2

- https://docs.microsoft.com/en-us/sccm/core/plan-design/security/enable-tls-1-2
- For further information refer to Application Note 277: Configuring Protege GX to use TLS 1.2

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.