The General Data Protection Regulation (GDPR) is a regulation on the protection and free movement of personal data of all individuals within the European Union. The regulation was put together by the European Parliament and the Council of the European Union and is effective from the 25th of May 2018. The regulation applies to organizations that collect or process data from EU residents or cooperate with EU-based organizations that process the data on their behalf.

For example, you need to comply with the GDPR in the following cases:

- Your company uses Kentico EMS and is based in the EU.
- You provide products or services to customers based in the EU.
- A company that provides you with services such as system administration, hosting, or help desk is based in the EU.

For more information about the GDPR, see the Official Journal of the European Union.

Kentico provides features and guidelines that help you comply with the GDPR. For more information, see the following sub-sectons and pages:

- Managing personal data
- Securing personal data
- Working with consents
- Personal data in Kentico

Managing personal data

Prerequisite

The **Data protection** application does not provide any data collection or erasure functionality by default. These features require exact knowledge of how your website gathers, processes and stores personal data. Your developers need to implement the functionality based on the specifics of your website and any other legal requirements that you wish to fulfill.

For a technical implementation guide, see:

- Implementing personal data collection
- Implementing personal data erasure

Kentico EMS required

The **Data protection** application and its features are only available in the **Kentico EMS** license edition.

Collecting personal data

The **Data protection** application allows you to search for personal data related to a specific person (data subject). The data is typically available both as human-readable text and in a machine-readable format (such as XML). You can use the data collection features if you need to provide stored personal data to a data subject, or transfer personal data to an external system or application.

1. Open the **Data protection** application.
2. Select the **Data portability** tab (for data in a machine-readable format) or **Right to access** tab (for data in a human-readable format).
3. Fill in the available inputs to identify the user (data subject) whose personal data you wish to find. By default, the page allows you to input an email address into the **Email** field.
4. Click **Search for personal data**.

The system collects the personal data related to the specified identifiers and displays it in the selected format.

Erasing personal data

To delete personal data related to a specific data subject from the system:

1. Open the **Data protection** application.
2. Select the **Right to be forgotten** tab.
3. Fill in the available inputs to identify the user (data subject) whose personal data you wish to delete. By default, the page allows you to input an email address into the **Email** field.
4. Click **Search for personal data**.
5. Check whether the displayed results contain the data you wish to delete and click **Select data to delete**.
6. Configure the available parameters in the **Delete personal data** dialog.
7. Click **Delete**.

The specified data is removed. You can verify the result by clicking **Search for personal data** again with the same identifiers.

Securing personal data

To comply with personal data laws, regulations, and guidelines, such as the GDPR, it might be necessary to protect your data at rest, i.e. the digital data stored physically on a server, hard drive, etc. This type of protection (typically using encryption) prevents malicious parties from taking advantage of personal data in cases where the physical medium holding the data is stolen or accessed in an unauthorized way.

The following data encryption technologies are recommended if you wish to secure your Kentico database on a physical level.

Transparent Data Encryption

Transparent Data Encryption (TDE) is a feature of Microsoft SQL server (2008 and later) that ensures real-time I/O encryption and decryption of data and log files. By using TDE, the data is encrypted via an encryption algorithm, such as AES, without requiring any changes in the related application. Encryption of the database files is performed at the page level and it does not increase the size of the encrypted database.

Transparent Data Encryption is available only in the **Enterprise** edition of MS SQL server (for on-premise or hosted database servers). If you use Azure SQL Database, TDE is available and all newly created SQL databases are encrypted by default using service-managed TDE.

BitLocker

If you have full control over the server hosting your Kentico database, you can use the BitLocker full disk encryption feature. BitLocker is available in supported Windows and Windows Server operating systems. It is intended to be used with a Trusted Platform Module (TPM) cryptoprocessor version 1.2 or later. BitLocker integrates with the operating system and protects the system and data from being misused in case of a theft, loss, or inappropriate decommission of the computer.