Xelion and GDPR

GDPR Compliance

As of the 25th of May 2018, companies who store personal information should follow GDPR (General Data Protection Regulation). The Xelion platform offers functionality that can support a business in becoming GDPR compliant. However, use of the Xelion platform by partners and customers does not automatically make a business GDPR compliant. Xelion Limited never adds private data into Xelion platforms. Xelion only offers the Xelion platform to third parties who can store private data by using the Xelion applications. Data entered in to Xelion platform is stored within the Xelion partners instance of the platform, if this is managed by Xelion Ltd then the data will be stored within a high availability AWS virtual environment. If the platform is unmanaged then the Xelion Partner will advise on where and how the data is stored.

This document describes the data Xelion may store that relates to GDRP and how this is managed.

Xelion may store the following personal data

- Gender
- Title
- Given name(s)
- Name prefix
- Family name
- Name suffix
- Initials
- Language
- Photo
- Employment
  - Job title
  - Employment address including telephone numbers, e-mail, fax
  - Department name
  - List of colleagues
- Private Information
  - Addresses including telephone numbers, e-mail, fax
  - Date of birth
- Notes about contacts within the system
- Search tags
- Contacts added to lists
- Number of points of communications with contact
- Colleagues who have had contact with a person
- All communication that pass through Xelion with this person such as e-mails, telephone calls, chats, faxes, etc.

Xelion is a business tool, most of the data stored within the Xelion platform is business related, personal data however may also be stored and is governed by GDPR.

Availability of data

Data can be added in Xelion in various ways:

- By a user entering person data in to the applications
- By using the Outlook import tool to upload all contact information stored within outlook
- Importing a CSV file which contains personal information
- By using the Xelion API (Application Programmers Interface)
- Connecting Xelion to a company Office 365 or Exchange server to synchronise contacts

When a person’s information is added to Xelion, access of this information can be granted to the user only, any group of users, or all users. The permissions for this are managed by the customer and or the partner.

When the Xelion platform makes or receives calls or e-mails when there is no corresponding person , phone number or e-mail address, Xelion creates an unknown address which consists of just the telephone number or the e-mail address as an audit trail of communication.

Data storage

All data is stored in a central database. No data is stored locally on a PC, Smartphone or other device.

The database itself can only be accessed through Xelion applications or the API. There is no availability for users or administrators to access the database directly (for example through SQL). Partners and customers can make backup’s of the Xelion platform database, these are only readable via the Xelion platform.

Person data is sent in an encrypted form from the central platform to the application via SSL. Communication to the softphone and most hard phones is not encrypted. Xelion supports encrypted communication with some handset brands and will fully support encryption from all applications by Q4 2018.

Porting of data

Xelion has a tool for extracting person data to other systems. The Xelion administrator can perform this action.

Authentication

Users authenticate on Xelion based on a username and a password, this is managed by the customer or partner administrator of the platform. All authentication is encrypted.

Xelion stores a timestamp of when a user logs in to Xelion.

The Xelion administrator can add extra administrators to Xelion. Administrators have the right to see all the person information with no restrictions. Permissions can be given to allow users visibility of some or all data.

Any action which is performed through an API call in Xelion can only be performed under the credentials of a user.

Deleting person data

The user who has added personal data can delete this personal data at any time. Administrators can delete any person data.

All communication is automatically logged to a personal contact, all forms of communication made to and from Xelion is visible via the personal contact card. This allows for quick and simple access to extract and delete data where required.

Monitoring and improvements

Xelion has an appointed security officer who is responsible for ensuring Xelion protect customer data to the highest standards.

Security sits at the front of every new development Xelion deliver to customers. If at any time a security risk is raised, Xelion will act with the highest priority to ensure we keep customers safe and secure.

Xelion customers part of GDPR

Privacy impact assessment (PIA)

Each customer must make a PIA to assess the impact of processing private person information. Furthermore, there should be a document which describes:

- which information is stored and for what purpose
- where the stored information comes from
- who has access to the stored information

Users of the Xelion software must have training to inform them how to handle data in accordance with GDPR.

Permission for using data

Any end users data which is stored within Xelion must know their data will be stored and need to agree upon this storage. For children under 16, parental approval is required. Proof is required to demonstrate ah end user has agreed for you to store there data. You are required to state for what purpose you wish to keep a persons data and may not deviate from this purpose.

End user’s rights

Upon first request by a person, private data must be:

- viewed
- edited
- deleted (right to be forgotten)
- exported

Data leak

If private personal data is leaked, the end user needs to be informed about the leak within 72 hours of the leak taking place.