

Xarios Call Recorder

General Data Protection Regulation (GDPR) Datasheet

Intro on GDPR

GDPR is an updated data protection regulation that comes into force on the 25th May 2018. It applies to all businesses that collect, store and process the personal data of EU citizens, even if the business itself is not located within the EU.

What rights and controls do EU citizens have?

GDPR provides individuals with increased rights and control over how their data is used. GDPR includes the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to be forgotten
- The right to restrict processing
- The right to data portability
- The right to object
- The right not to be subject to automated decision-making, including profiling

In addition, businesses wishing to record personal data will need to ensure that at least one of the following six conditions be met to legally record the data:

- Individuals involved in the call have given consent to be recorded
- Recording is necessary for the fulfilment of a contract
- Recording is necessary for fulfilling a legal requirement
- Recording is necessary to protect the interests of one or more participants
- Recording is in the public interest, or necessary for the exercise of official authority
- Recording is in the legitimate interests of the recorder, unless those interests are overridden by the interests of the participants in the call

How does this affect businesses?

Any business that processes personal data will need to ensure they have policies and processes in place to meet the rights of the individual's data they hold. In addition, they need to ensure they have a legal right to store the data, they are not storing data on minors, and that they have processes in place to report data breaches.

How does this effect Call Recording in general?

Any business that records telephone calls will need to ensure that they have a legal right or requirement to do so. Where call recording is not explicitly required by regulations (such as MIFID II), consent will usually be required.

Any personal data stored in the call recording system will need to be documented as part of the business' GDPR policies, with specific references on how data can be identified and modified/removed if required.

How consent for call recording is sought, recorded and managed is of vital importance. The ICO has published a detailed guidance on consent under GDPR:

<https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf>

If existing forms of consent held by businesses do not meet the new requirements, they must be refreshed so that they meet the new GDPR requirements.

How does this effect Xarios Call Recorder?

Xarios Call Recorder stores data in the following locations:

Employee/User Data

The call recorder will store limited personal data for users/employees. User accounts configured on the system will have an email address for the employee but no other specific information about the user. The call recorder does store audit information about what users of the system have done; when they logged in, settings changed, recordings played etc.

In addition to usage data, any call recordings involving employees may contain personal data if discussed.

Customer Data

It is possible for the call recorder to store the personal data of a company's customers in 3 locations:

- Contact Directory Data - Imported into the system
- Call Data - Logs of calls to/from the customer including their phone number and possibly their name if there is a contact match. This could also include custom notes added or data tagged to a call using the API
- Call Recordings - Any information about the customer recorded on a call

It is important to understand what information is being collected by the call logging/recording system to ensure that any customer requests can be responded to.

How does this effect a Xarios Call Recorder Implementation?

The following items identify the main areas of a Xarios Call Recorder implementation which are affected by GDPR.

Document what is stored and ensure it contains no sensitive data

The previous section listed what types of personal data may be stored in the system. It is important to add to your existing GDPR documentation the data that is being stored in the call recorder. If any of the features listed are going to be used as part of the call recorder implementation (Contact Directories, Call Notes, Call Tagging), the type of data stored must be documented.

Consent / Provide callers with option to opt out of recordings

It is important to ensure that you have consent to record customer calls and that they have opted in. Using the Persistent Exclusion List feature of the system in combination with a call routing announcement, callers can be asked for consent to record at the beginning of any inbound call.

Secure/Audit Access to the System

It is important to ensure that only the relevant users have access to the system and that they only have the minimum permissions that they require. In addition, ensure that the server the solution is installed on is appropriately secured and that no unauthorised users can gain direct access.

Tag recordings with Customer ID for Transparency

To ensure that customer records can quickly and easily be identified, the Communication Gateway API can be used to tag calls with a customer ID or other method of identification which offers improved searching over caller ID/telephone number searching.

Tools Available to Modify/Remove Data

Tagged data fields against call records and contact data can be updated or removed from the system. To remove call recordings themselves, the 'Recording Deletion' license must be applied to access the Recording Deletion features.

End-User Training

Ensure that all users of the system are trained on data protection and are informed that their own calls are being recorded (if applicable). Provide users with a non-recorded extension that they have access to so that they can make personal calls that are not recorded.

Update Internal Documents on where data is stored

When installing the system, ensure that your GDPR policy documentation is updated to refer to any personal data that is being stored within the call recorder.

Disclaimer

This document cannot and does not contain legal advice. The information is provided for general informational purposes only and is not suitable for legal advice. Accordingly, before taking any actions based upon such information, we encourage you to consult with the appropriate legal professionals. We do not provide any kind of legal advice. The use or reliance of any information contained in this document is solely at your own risk.

Xarios Technologies

7 Digital Park, Pacific Way, Salford Quays, Manchester M50 1DR

www.xarios.com | 0161 786 4350

