ClarionCall GDPR

The GDPR (General Data Protection Regulation) is EU legislation that will replace the existing UK Data Protection legislation on 25th May, 2018. It applies to every organisation that holds (data controllers) and/or processes (data processors) personal data. Full details can be found at the Information Commissioner's website.

The following information will be updated on a regular basis.

How does the GDPR apply to me?

All ClarionCall's customers are data controllers under the GDPR and ClarionCall is a data processor of your data. The GDPR requires that there is a formal agreement between your organisation and ClarionCall that details how all data is stored and processed.

Are you registered with the Information Commissioner?

ClarionCall has maintained data protection registration with the UK Information Commissioner's Office since 2005.

Where does ClarionCall store our data?

Data used as part of ClarionCall's services is stored on our dedicated servers which are located in a Tier 3 ISO 27001 datacentre in the UK. The datacentre is manned 24x7 and has CCTV and other security systems.

How do you make sure that our data is secure?

All ClarionCall applications have been designed to be secure. Firewalls block all public access to our systems with the exception of secure browser (https), email and mobile network connections necessary to provide our services. Key employees have VPN access to our systems with multi-layer security in order to provide essential maintenance and development activity. Our systems do not rely on any third party cloud services to store data. All your interactions with ClarionCall systems are carried out using https which means that they are authenticated and encrypted. The one exception is email which, by its nature, is not secure.

Does ClarionCall access or change our data?

ClarionCall does not routinely access your data although from time to time we may access your data in order to provide support. We also carry out performance monitoring on our systems to ensure smooth operation which may involve access on an aggregated, non-personal basis.

How is our data transferred to your systems?

ClarionCall offers a variety of methods ranging from entering data into a ClarionCall screen to automated API requests from our database to automated overnight transfer of files from your database to ours using proprietary connectors. Whether screen entered or file transferred, the data is authenticated by our system and encrypted and authenticated during transmission. All these methods are transparent – the organisation has complete visibility of the data being transferred.

What information do you store?

Depending on your customer type (School, College, Business or Sports Club) ClarionCall will hold certain details about your Employees, Members and/or your School's parents and pupils/students. The data held on these individuals mainly consists of names, contact details and membership of relevant groups within your organisation (for example, Department, a student's Year group, sports team etc.)
Using ClarionCall, you can send messages to the above individuals and/or allow them to access our portal and other applications. We store details of the messages sent, including delivery information. Your ClarionCall Administrator(s) can see all the above information when they log on to ClarionCall.

ClarionCall also stores business data about your organisation, in which case we are the data controller, in order to allow us to operate our business, for example to provide customer support, generate invoices, etc,

Are our login details secure?

Your login and password are authenticated and encrypted when entered into a ClarionCall screen and your passwords are encrypted on our servers – it is technically impossible for any of our employees to access your passwords. If you forget your password, the system can provide a temporary password which has to be used within 2 hours. The system then requires you to change the temporary password. You can stipulate the preferred complexity of the passwords used when your organisation uses ClarionCall.

How long do you retain data?

Individual contact details are retained in our database until they are removed by your removing them from the source of the data, either due to their leaving your organisation or by compliance with a right to be forgotten request.
Message data, such as email and text messages, is retained on a rolling 12 month basis, irrespective of whether the individual's contact details have been removed from the database, including where the message recipient's details have been removed per the above.

If a customer ceases services with ClarionCall, all contact details and message history for the account will be removed from our datdabase within a maximum of 4 weeks.

ClarionCall retains rolling backups of its databases for up to 12 months to meet potential operational and legal requirements.

How can I correct mistakes in our data?

Incorrect data in ClarionCall can immediately be updated by your Administrator in ClarionCall. If you use an automated method to update ClarionCall overnight, it will be necessary for you to update your database as well to prevent the incorrect data from being transferred to ClarionCall again. Data relating to messages that have already been sent cannot be corrected. Any errors in business data about your organisation can be corrected by emailing

How do I make a Subject Access Request?

ClarionCall's services allow your ClarionCall Administrator to create a report that will satisfy a Subject Access Request. Additional reporting functionality will be made available to enhance this functionality. Subject Access Requests made by your employees, or by a school's parents or pupils directly to ClarionCall will be referred to you.

How can I delete data to comply with the Right To Be Forgotten?

Your Data Deletion Policy should specify the circumstances under which you will delete data. However, this may be affected by a statutory requirement to retain the information.

Contact details that are the subject of a Right To Be Forgotten request can immediately be removed by your Administrator in ClarionCall. If you use an automated method to update ClarionCall overnight, it will be necessary for you to update your database as well to prevent the incorrect data from being transferred to ClarionCall again.

Message, other historical data and related data within our backups will be redacted within 10 working days of the written request of your Data Protection Officer, Data Handling Officer or other person responsible for data protection compliance.

ClarionCall reserves the right to make a charge for redacting records within our backups depending on the work involved.

When will ClarionCall be GDPR compliant?

We view good data protection as a continuous process and have always sought to uphold the highest data protection standards. We will meet or exceed all requirements of this GDPR legislation ahead of May 2018. We have consulted the ICO regarding our framework of policies and have confirmed that we have everything needed to comply. We are in the process of ensuring that our suppliers comply with GDPR and will update these FAQs when this is complete.

What are your next steps?

- Ensure that our suppliers are GDPR compliant
- Identify the Data Protection Officer, Data Handler or other responsible person at all our customers
- Update all our customer agreements to reflect GDPR requirements and execute them.

Last updated 14th March, 2018