HOW DOES GROUPCALL EMERGE SUPPORT YOUR GDPR COMPLIANCE?

groupcall Emerge

- Two-factor authentication
- Per-device authorisation
- Fine grained access controls
- AES mobile encryption
- Active Directory integration
- Minimum data transmission
- Multi-school single users
- Reflects your MIS data

By necessity your MIS contains all manner of personal and restricted data. There is a critical balance in being able to demonstrate how you grant safe and secure staff access to school data but provide useful access across the devices they want to use, where they want to use them. Emerge enables you to safely and securely access data on the move on mobile devices, on the web while working from home, or anywhere convenient for you and your staff.

Access to data

Emerge Desktop and Emerge Mobile **support fine grained per-user permissions** for access to areas of data, including whether the access is read or write. Data is **AES encrypted at rest** within Emerge Mobile and is subject to our multi-layer cloud platform security in Emerge Desktop which includes encryption where appropriate. Both services also integrate with your **Active Directory** to align with your existing user management solution, and Emerge Desktop can also support logging in with Office 365.

Access to Emerge Mobile is controlled on a **per-device** basis. The app will only work on authorised devices and we provide quick start options to help you get one or many devices easily authorised and connected. We're currently making further enhancements to Emerge Mobile to help further **minimise the data transmitted** to devices on a per-user basis.

When using Emerge Mobile, the device being used is one of your authentication factors – "something you have". When using Emerge Desktop we add additional authentication controls, including optional **two-factor PIN challenge** via mobile phone when accessing Emerge Desktop outside of your school. If you or your staff work across multiple academies, for example as a shared attendance officer, you can also link two schools under a **single secure account** so you have fewer passwords to remember.

Personal data rights

As an extension of your school MIS platform the Emerge suite doesn't hold any additional personal data other than that already contained in your MIS. In fulfilling any **Subject Access Requests** or the **Right to be Forgotten**, Emerge will automatically follow whatever actions you choose to make within your MIS within a maximum of 24 hours of those changes being made. If we develop Emerge modules in the future that store personal data from sources other than your MIS then a Subject Access Request module will be developed to accompany this.

As a safeguarding and operational tool used across your school, Groupcall does not currently believe there will be scenarios in which you would want to exclude a specific person's limited personal data from being accessible to authorised users from appropriately authenticated devices using Emerge. However, we will continue to review this position up to and after the GDPR deadline and ensure we provide products and services that best enable your GDPR compliance requirements.

Download the complete guide to GDPR compliance for schools
www.groupcall.com/gdpr-ebook

groupcall™
built on trust