

Keyfort Limited

General Data Protection Regulation (GDPR)

Statement

Keyfort provides IT engineering and cloud computing services for its customers comprising small medium enterprises (SMEs), corporates, not for profit organizations, education and local government sectors. For its own corporate data relating to its current, past and prospective customers Keyfort is designated the Data Controller. The legitimate business interests is the lawful basis under which this data is held. All such data is securely held within the United Kingdom. See Keyfort's Data Location, Security & Privacy document for security practices.

Keyfort provides a range of services for its customers including but not limited to automatic data backups off site, encrypted data links, network security services, hosted servers, managed servers, remote support, remote monitoring, configuration backups, corporate Wifi management, VoIP services, resiliency services, software as a service including booking, payment, document storage, membership and attendee details. For all this customer data Keyfort is designated the Data Processor. All such data is securely held within the United Kingdom. See Keyfort's Data Location, Security & Privacy document for security practices.

Keyfort as Data Processor for its customers who are the nominated Data Controllers for their own data, Keyfort undertakes to:

- provide IT Engineering and Cloud Computing services as set out in the applicable Keyfort Network & ICT Systems Managed Service agreement for the service term therein defined which may be ongoing subject to written notification of service termination;
- define the nature and purpose of the processing as per the appropriate Network & ICT Systems Managed Service agreement;
- work with the type of personal data and categories of data as defined by the controller;
- act only on the written instructions from the controller unless otherwise required by law;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- not to engage sub-processors, with written contract, without the prior consent of the controller;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the appropriate Network & ICT Systems Managed Service agreement;
- provide security of data in accordance with Keyfort's Data Location, Security & Privacy document for security practices and will provide the controller with information it needs, as reasonably expected of Keyfort, to ensure that they are meeting their Article 28 obligations, and will tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.