GDPR FAQ's

Below are a number of frequently asked questions regarding Xeretec and our preparation for and compliance with the General Data Protection Regulation (GDPR).

What is the General Data Protection Regulation (GDPR)?

The GDPR is a new regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union, aiming to give control back to citizens and residents over their personal data. The GDPR comes into effect from 25th May 2018.

What client personal data do you hold and what is the legal basis for processing it?

Xeretec holds contact details for points of contact within our customers' organisations that are necessary in the delivery of contracted services. This typically includes:

- Those who contact the Helpdesk to log problems or requests in relation to equipment or services that we supply
- Those who need to be contacted in the course of fulfilment of contracted services, such as nominated recipients of invoices and SLA reports
- For some services we obtain print metrics on a per-user basis in order to supply data analytics for customers who have subscribed to this

The data that we hold is the minimum required to fulfil these purposes. Mostly it is limited to name and contact information (address, email, phone and fax numbers). We do not hold any sensitive personal data for client contacts.

How will your organisation comply with GDPR?

Xeretec takes data security and data privacy very seriously and is working on a plan to ensure we are compliant for GDPR by 25th May 2018. Xeretec has appointed a Project Manager for GDPR (Ian Stevenson). We also have a cross-functional business team working with our Project Manager which includes Senior Management and a member of the board (Group Managing Director: Adam Gibbons).

Where is client personal data held?

All client personal data is hosted on servers within the European Union. Where we use an external cloud hosting service, we are seeking assurance from our suppliers that they are compliant with GDPR legislation.

What security measures do you have in relation to the processing of information?

All data held on internal servers are subject to logical and physical security controls and are backed up to a UK-based ISO 27001/PCI accredited datacentre. All servers and data storage systems are protected by physical enterprise grade firewalls which incorporate various security protections. All our servers and client computers are protected by enterprise grade managed endpoint protection software. All storage data is protected by hourly/daily/weekly storage level snapshots which can be called upon as and when required. The entire network is replicated offsite to a UK based ISO27001/PCI certified datacentre and our network can be brought online in a DR scenario within 4 hours.

We have a comprehensive set of security policies covering all aspects of acceptable use and data privacy and require all staff to agree to the terms of these policies as part of the induction process.

We are running a comprehensive internal programme to raise awareness for GDPR.

We are working towards ISO27001 certification.

Do you have a data protection officer?

We are currently seeking to appoint one and we are developing Terms of Reference for it.

Do you have a data retention policy?

Yes. We have undergone a data discovery and categorisation process and defined appropriate retention stategies.

Do you have a process in place for notifying us of a security breach involving our data?

Yes - we are working on this as part of our ISO 27001 accreditation which includes having a robust incident response and management process in place to report any security incidents through our internal helpdesk. We will launch an awareness campaign to ensure that all users understand the importance of reporting all security and potential data protection incidents. Our internal processes will ensure that appropriate authorities and affected parties are notified within the mandated timeframes.

In the event a customer exercises their 'right to be forgotten', are features available within your system(s)/application(s) to help us delete personal data?

Yes - we will ensure our systems/applications enable us to exercise the "right to be forgotten". Our master customer data resides in our Customer Relationship Management (CRM) system. If a customer contact exercises the "right to be forgotten" and this is deemed by us to be reasonable in the first instance, the data will be deleted from our CRM and cascaded to any local contact systems.

Do you delegate any services to third parties or entities in their group. Where are they located?

Some services require data to be sent to third parties. Specifically:

- Xerox for Device Agent Installation data (name, address, email and phone number) is held within Xerox Service Manager
- NewField IT (Xerox) for User Analytics

We are seeking assurances from Xerox and NewField IT around their controls and certifications.

How will you deal with any complaint or request made in relation to data subject rights?

We are setting up a GDPR specific email address for customers to make requests and/or complaints and will have a process in place to respond within the GDPR mandated timeframe.

Who can we use as a point of contact for any questions regarding GDPR compliance in relation to our data?

Please contact your Account Manager in the first instance - we can then guide any questions to the relevant personnel in Xeretec.