

FACTSHEET

GDPR-READY ENCRYPTION

We recognise the importance of basic security measures in order to achieve GDPR compliance and we understand the obstacles that data controllers and data processors will need to overcome during their journey.

Encrypting data when stored and when in transit is an essential safeguard for modern businesses. Post-GDPR, failure to encrypt sensitive information could result in regulatory action and severe penalties following a breach. The ICO will simply have no time for excuses.

Implementing strong encryption means that reporting a breach may not be necessary, and can therefore help to avoid reputational damage and other related consequences, while saving time and resource.

So, we've created a cost-effective pay-as-you-go encryption service that has been designed with compliance in mind from the very beginning. It's simple to set up and means that you will be able to demonstrate the technical and operational measures that you have in place to protect personal data, should a breach occur.

With contractual agreements in place to ensure continuous adherence to the regulation, our GDPR-ready encryption services deliver peace of mind that your data is always safeguarded, which is why we're your partner of choice.

OUR GDPR-READY ENCRYPTION SERVICES INCLUDE:

- **Contractual agreements** to guarantee continuous adherence to specific aspects of GDPR
- **Technical organisational measures** to guarantee the safety and availability of your data
- **Auditable assurance**, site visits and full transparency of our services, processes and accreditations to satisfy auditors
- Strict adherence to **codes of conduct** and certificates to prove compliance
- **GDPR consultancy** services offered by the wider Cyberfort Group

Our GDPR-ready encryption services have been developed specifically to address the following key principles outlined in the regulation:

ARTICLE 6: Lawfulness of processing

- ☐ ☐ We ensure that the necessary and proportionate measures to safeguard personal data have been taken when processing data for a purpose other than for which it was collected.

ARTICLE 23: Restrictions

- ☐ ☐ Our encryption also demonstrates the existence of appropriate safeguards when ascertaining whether personal data can be used for another purpose than for which it was collected.

ARTICLE 32: Security of processing RECITAL 83

- ☐ ☐ We help you demonstrate the appropriate technical and organisational measures to ensure the level of security needed to mitigate the risks to the rights and freedoms of the data subjects.

WE MAINTAIN THE HIGHEST LEVELS OF SECURITY DURING PROCESSING BY:

- ☐ ☐ Continuously evaluating the risks associated with processing personal data
- ☐ ☐ Implementing encryption to mitigate any potential risks when processing data

ARTICLE 33:

Notification of a personal data breach to the supervisory authority

ARTICLE 34:

Communication of a personal data breach to the data subject

OUR ENCRYPTION MEANS THAT:

- ☐ ☐ All personal data will be unintelligible to anyone other than those who are authorised to access it and have the correct decryption keys
- ☐ ☐ A data breach is 'unlikely to result in a risk to the rights and freedoms' of the people affected
- ☐ ☐ Sensitive data will be safeguarded to the correct level
- ☐ ☐ You may not have to report it to the ICO or the people affected if you were to suffer a breach

THE GDPR SERVICE SUITE

We offer a suite of contractually-backed pay-as-you-go services that address specific articles within GDPR and are designed to help you become compliant. From data storage to processing and backups, we're your trusted adviser at every stage of your compliance journey.