

FACTSHEET

GDPR-READY COLOCATION

We know the importance of privacy by design and we understand the different challenges your business will come across in your journey towards compliance, whether you are the data processor or data controller.

GDPR will place a spotlight on compliance within the supply chain. That's why our bespoke GDPR-ready colocation services have been designed with compliance in mind from the get-go, supporting your compliance framework and relieving the burden whilst making auditing simple.

Not only that, but we go one step further by including adherence to these regulations in our contracts, meaning that compliance accountabilities are aligned to the regulation, making us your partner of choice.

OUR GDPR-READY COLOCATION 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 colocation services have been developed specifically to address the following key principles outlined in the regulation:

ARTICLE 32: Security of processing

THE ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES IS ENSURED BY:

- Hosting data in our ISO 27001 accredited ex-military facilities, with escorted access, 24/7 on-site security and internal monitoring systems
- Business-wide service-oriented architecture and IOG fully-meshed resilient networks
- Fire suppression systems in all racks
- Rigorous business continuity planning, testing and full disaster recovery capabilities

WE HAVE THE ABILITY TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT THANKS TO OUR:

- 24/7 service desk, remote-hand capabilities, incident management and on-site engineers
- Site-to-site fail over capabilities
- Standard operating and escalation procedures
- Dual feeds and UPS back-up power supplies

OUR TECHNICAL AND ORGANISATIONAL MEASURES ARE TESTED AND EVALUATED TO ENSURE THE SECURITY OF PROCESSING:

- IMS management and BCP testing procedures
- IL Official, G-Cloud and IGSoC testing procedures
- ISO 27001 data centres independently audited by the British Standards Institute
- Over 200 daily checks on data centres as well as regular risk assessments
- Both facilities annually QSA-assessed and controls tested

WE HELP YOU MITIGATE THE RISKS PRESENTED BY PROCESSING THROUGH OUR:

- Breach notification procedures
- Regular data centre black building testing
- Annual risk assessments
- WEEE regulated media destruction services

ARTICLE 44-50:

Transfers of personal data to third countries and international organisations

- ☐ ☐ All of our data centres, data sovereignty and co-located areas are based within UK borders and no data is transferred to international third parties.

ARTICLE 32:

Security of processing

ARTICLE 40:

Codes of conduct

ARTICLE 42:

Certificates

- ☐ ☐ The Bunker maintains certificates and codes of conduct including ISO27001, PCI DSS (to full managed services hosting provider status), IGSOC, G-Cloud and IL official. Our technical and organisational measures are independently audited in alignment of these standards.

- ☐ ☐ However, we understand that accreditations are no guarantee that a service provider is GDPR-compliant. This is why we work to ensure we – and our customers – continually meet the regulatory standards set, and our extensive knowledge of data privacy and GDPR allows us to advise on the entire supply chain.

ARTICLE 28:

Processor

ARTICLE 37:

Designation of the data protection officer

ARTICLE 39:

Tasks of the data protection officer

- ☐ ☐ Our dedicated on-site data protection officer is responsible for continuously assessing our technical and organisational measures to ensure we continue to uphold and adhere to the highest industry standards.

ARTICLE 28: PROCESSOR

WE ENSURE THE HIGHEST LEVELS OF CONFIDENTIALITY WHEN PROCESSING YOUR PERSONAL DATA THROUGH:

- Strict physical and access controls including an approval process for anyone wanting to access the site
- Trained service desk staff who only act on behalf of authorised customer contacts
- As part of your supply chain we have firm commitments to working with you in order to provide the evidence and validation to meet compliance standards.
- At the end of our contract, if requested, we ensure that any tapes or cloud back-ups of data are returned to you or deleted unless European Union or Member State law requires us to hold it. Our media destruction capabilities are also in alignment with WEEE regulations.

WE MAKE IT SIMPLE TO DEMONSTRATE COMPLIANCE BY:

- Issuing certificates of compliance upon request
- Welcoming site inspections and customer audits to test and validate our controls
- Working with your compliance teams to provide auditable assurance

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 advisor at every stage of your compliance journey.