THE BUNKER

Part of the CYBERFORT group

FACTSHEET

GDPR-READY OFFICE 365 BACKUP-AS-A-SERVICE

For many businesses the availability of data is central to day-to-day operations, and we are acutely aware of the challenges that data controllers and data processors will face during the compliance journey.

If your organisation uses Office 365, you are ultimately responsible for protecting your own data – Microsoft says so.

Without a disaster recovery plan, your emails, attachments, calendar events and contact details are at risk if mistakenly deleted, breached or made unavailable. And under GDPR, the inability to recover information when needed could result in hefty penalties.

Our Office 365 Backup-as-a-Service solution has been built with compliance in mind at every stage, eliminating the risks and giving you absolute control over your data retention.

Underpinned by contractual agreements which guarantee continuous compliance with specific aspects of GDPR, this solution offers assurance that your business-critical information is always available. Not only that, it also helps you minimise your on-premise footprint and free up IT services. That's why we're your partner of choice.

OUR GDPR-READY OFFICE 365 BACKUP-AS-A-SERVICE INCLUDES:

- **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

Telephone: 01304 814800 Email: info@thebunker.net

Our GDPR-ready Office 365 Backup-as-a-Service has been developed specifically to address the following key principles outlined in the regulation:

ARTICLE 4:
Definitions

UNDER GDPR, A PERSONAL DATA BREACH CAN OCCUR IF BACKUP DATA IS LOST, DESTROYED OR ACCESSED BY UNAUTHORISED PERSONNEL. OUR BAAS HELPS TO AVOID THESE SCENARIOS BY:

- Encrypting personal data and offering the ability to ensure the ongoing confidentiality, availability, integrity and resilience of processing systems and services
- Enabling you to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Regularly testing, assessing and evaluating the technical and organisational measures for ensuring the security of processing

ARTICLE 5:
Principles relating to processing of personal data

- Our service offers peace of mind that data is adequate, relevant and limited to what is necessary in relation to the purposes for which it is being processed.

WE ENSURE THAT PERSONAL DATA IS KEPT UP TO DATE AND ACCURATE THROUGH:

- Automated backup capabilities and reporting

ARTICLE 5 CONTINUED:
Principles relating to processing of personal data

WE ENSURE THE CONTINUOUS AVAILABILITY, INTEGRITY AND CONFIDENTIALITY OF DATA, AND OFFER PROTECTION AGAINST UNAUTHORISED OR UNLAWFUL PROCESSING AND AGAINST ACCIDENTAL LOSS, DESTRUCTION OR DAMAGE OF DATA BY:

- Enabling you to perform eDiscovery of email archives with advanced search capabilities, flexible recovery and export options
- Encrypting personal data and offering the ability to ensure the ongoing confidentiality, availability, integrity and resilience of processing systems and services
- Enabling you to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Regularly testing, assessing and evaluating the technical and organisational measures for ensuring the security of processing

OUR SERVICE MAKES SURE THAT YOU DON'T HOLD ON TO DATA SETS FOR LONGER THAN NECESSARY BY:

- Promising to return or delete any back-ups of data at the end of our contract unless European Union or Member State law requires us to hold it. Our media destruction capabilities are also in alignment with WEEE regulations.
- Aligning your data retention policies with our backup and archive retention policies

ARTICLE 28:
Processor

- Our service helps you demonstrate that the appropriate technical and organisational measures are in place to protect the rights of the data subject.
- The secure destruction of data offers peace of mind that no backups are kept by us at the end of the contract, unless European Union or Member State law requires us to hold it.
- This service allows you to protect hybrid cloud environments as well as migrate mailbox data between Office 365 and on-premises Microsoft Exchange Server.

ARTICLE 32:
Security of processing

WE ENSURE YOU HAVE THE RIGHT TECHNICAL AND OPERATIONAL MEASURES IN PLACE TO DEMONSTRATE THE ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE OF PROCESSING SYSTEMS AND SERVICES THROUGH:

- Our storage level corruption guard that performs scheduled health checks of backup data to ensure consistency if recovery from backup is required

OUR SERVICE ENABLES YOU TO RESTORE THE AVAILABILITY AND ACCESS TO PERSONAL DATA IN A TIMELY MANNER IN THE EVENT OF A PHYSICAL OR TECHNICAL INCIDENT BY:

- Offering multiple options to restore data from backups at a granular level

- As part of our service we carry out regular testing, assessments and evaluations of the effectiveness of our technical and organisational measures in ensuring the security of data processing.

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.

Telephone: 01304 814800 Email: info@thebunker.net