THIS PERSONAL DATA PROCESSING AGREEMENT (this "**DPA**") is entered into and made between:

1. **Company**, hereinafter referred to as the "**Controller**", and

2. **Btwentyfour**, hereinafter referred to as the "**Processor**".

Each of Controller and Processor are individually referred to as a "**Party**" and jointly as the "**Parties**".

1 BACKGROUND

1.1 The Services rendered under the Service Agreement (the "**Agreement**") will include processing of personal data by Processor on behalf of Controller.

1.2 This DPA governs Controller's rights and obligations as a controller and Processor's rights and obligations as a processor when Processor processes personal data on behalf of Controller.

1.3 This DPA shall be deemed to form part of the Agreement. In the event of inconsistencies between the provisions of the Agreement and this DPA, this DPA shall prevail and take precedence.

2 DEFINITIONS

2.1 "**Data Protection Laws**" means all applicable laws, regulations, and binding regulatory guidance relating to the processing of personal data and privacy, including: (a) the General Data Protection Regulation (EU) 2016/679 ("**GDPR**") and any national implementing legislation in the European Economic Area; (b) the Privacy and Electronic Communications (EC Directive) Regulations 2003 (as amended); (c) any successor or replacement legislation to the foregoing; and (d) any other applicable data protection or privacy laws.

2.2 Unless otherwise stated, terms and expressions in this DPA shall be interpreted in accordance with Data Protection Laws. Accordingly, terms that are defined in GDPR shall have the same meaning as in GDPR when used in this DPA, including but not limited to the terms "*controller*", "*data subject*", "*personal data*", "*personal data breach*", "*processor*", "*processing*", and "*pseudonymisation*".

2.3 Any other terms and expressions used in this DPA but not defined herein or in Data Protection Laws, shall have the meaning ascribed to them in the Agreement.

3 APPENDICES

Specification of the processing of personal data	Appendix 1
List of pre-approved sub-processors	Appendix 2
Technical and organizational measures	Appendix 3

4 PROCESSING OF PERSONAL DATA

4.1 Processor undertakes to process personal data only in accordance with documented instructions from Controller, unless otherwise provided by applicable laws. Controller's instructions to Processor regarding the subject-matter and duration of the processing, the nature and purpose of the processing,

the type of personal data and categories of data subjects, are exhaustively set out in this DPA and Appendix 1.

4.2 Controller confirms that Processor's obligations set out in this DPA, including Appendix 1, constitute the complete instructions to Processor. Controller will ensure that its instructions comply with Data Protection Laws.

4.3 Any amendments to Controller's instructions shall be documented in writing and signed by both Parties in order to be valid. Any such amendments shall also include provisions in respect of changes (if any) of Processor's remuneration. Controller may not, without such written agreement, instruct Processor to process personal data regarding other categories of personal data or regarding other categories of data subjects than those specified in Appendix 1.

4.4 Processor shall without undue delay inform Controller if, in its opinion, an instruction from Controller regarding the processing of personal data infringes Data Protection Laws in accordance with article 28(3) GDPR.

4.5 Processor shall, to the extent required by Data Protection Laws and in accordance with Controller's written instructions, where applicable, assist Controller in fulfilling its obligations under Data Protection Laws.

5 SUB-PROCESSORS AND TRANSFERS TO THIRD COUNTRIES

5.1 Controller authorises Processor to engage sub-processors. Processor shall ensure that sub-processors are bound by written agreements which impose on them the same data protection obligations as set out in this DPA.

5.2 Appendix 2 contains a list of sub-processors that from the execution date of this DPA have been approved by Controller. If Processor intends to engage a new sub-processor or replace an existing sub-processor to process personal data covered by this DPA, Processor shall provide Controller with thirty (30) days prior written notice of any intended changes concerning the addition or replacement of sub-processors and give Controller the opportunity to object to such changes. Any objections by Controller shall be made in writing within fourteen (14) days from receipt of the information from Processor and must (i) be based on legitimate and substantial data protection concerns; (ii) specify the grounds for objection with reasonable particularity; and (iii) be based solely on considerations related to data protection.

5.3 Processor shall provide Controller with the information that Controller may reasonably request to assess whether compliance with the obligations under this DPA and Data Protection Laws is possible if the proposed sub-processor is engaged.

5.4 If Controller objects in accordance with this Section 5, the Parties shall discuss the objection in good faith and seek to resolve Controller's concerns through appropriate safeguards or alternative arrangements. If the Parties cannot resolve Controller's objection within thirty (30) calendar days, and Processor reasonably determines that the sub-processor is necessary for the provision of the Services, Controller may: (i) accept the new sub-processor; or (ii) terminate the affected Services by providing written notice to Processor, without penalty, provided that Controller pays all fees due for Services provided up to the effective date of termination.

5.5 The Processor may only transfer personal data outside EU/EEA with Controller's prior approval. If personal data is transferred to or made available outside the EU / EEA, Processor shall ensure that the transfer is subject to an appropriate safeguard under Data Protection Laws, such as standard data protection clauses adopted by the Commission as well as any necessary supplementary measures.

5.6 Processor shall remain fully liable to Controller for the performance of any sub-processor's obligations to the same extent as if Processor were performing the services of the sub-processor directly.

6 DATA SECURITY AND CONFIDENTIALITY

6.1 Processor shall implement appropriate technical and organisational measures to ensure the security of personal data in accordance with Data Protection Laws. Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of the processing, Processor shall maintain the technical and organisational measures specified in Appendix 3 to ensure the security of personal data. The agreed technical and organisational measures are subject to technical progress and further development, and the Processor may accordingly implement additional or alternative measures provided that it does not reduce the overall security level.

6.2 Processor shall ensure that only such persons who need access to personal data in order to fulfil Processor's obligations under the Agreement and this DPA have access to such data. Processor shall ensure that such persons are subject to appropriate means of confidentiality.

7 DISCLOSURE OF PERSONAL DATA AND CONTACTS WITH COMPETENT AUTHORITIES

7.1 Processor may not, without the prior written consent of Controller, disclose or otherwise make available personal data processed under this DPA to third parties, unless otherwise provided by applicable laws.

7.2 If a court or competent authority requests information from Processor regarding the processing of personal data covered by this DPA, Processor shall without undue delay notify Controller thereof, unless otherwise provided by applicable laws. Processor may not act on behalf of Controller or as its agent and may not, without the prior consent of Controller, transfer or otherwise make available personal data governed by this DPA or other information relating to the processing of such personal data to any third party, unless otherwise required by applicable laws.

8 DATA SUBJECTS' RIGHTS

8.1 Controller is responsible for responding to requests related to data subjects' rights and shall remain the primary point of contact for data subjects seeking to exercise their rights under Data Protection Laws.

8.2 Processor shall assist Controller by establishing and maintaining reasonable technical and organizational measures, insofar as this is possible, for the fulfilment of Controller's obligations to respond to requests to exercise data subjects' rights under Data Protection Laws. Taking into account the nature of the processing, Processor's assistance obligations under this clause shall be

limited to: (i) using reasonable efforts to retrieve, correct, delete, or restrict processing of specific personal data as instructed by Controller, where such actions are technically feasible; and (ii) providing information reasonably necessary for Controller to respond to the request, to the extent such information is within Processor's possession or control.

8.3 In the event a data subject's request is received by Processor, Processor will promptly inform Controller. Processor will not respond to any data subject's request without Controller's prior written consent, except to inform the data subject that the request has been received and forwarded to Controller.

9 PERSONAL DATA BREACH

9.1 Processor shall notify Controller without undue delay after becoming aware of a personal data breach. Such notification shall, where possible, contain:

a) the nature of the personal data breach, and, if possible, the categories of and the approximate number of data subjects concerned, and the categories of and the approximate number of personal data concerned;

b) the name and contact details of Processor's data protection officer or other designated contact point where more information may be obtained;

c) the likely consequences of the personal data breach; and

d) the measures taken or proposed to be taken by Processor to address the personal data breach and to mitigate its possible adverse effects.

9.2 Where, and in so far as, it is not reasonably possible to (i) provide the information within the agreed timeframe or (ii) provide all information at the same time, the information may be provided in phases without undue further delay. Processor shall cooperate with Controller to enable Controller to comply with its obligations under Data Protection Laws by providing any information regarding the personal data breach that is available to Processor and that is reasonably necessary for Controller to fulfil its obligations to notify the supervisory authority and affected data subjects.

9.3 In the event of a personal data breach under this DPA, Processor shall take reasonable measures to address the breach, including measures to mitigate its adverse effects.

10 DATA PROTECTION IMPACT ASSESSMENTS AND PRIOR CONSULTATION WITH SUPERVISORY AUTHORITIES

10.1 Upon Controller's written request, Processor shall provide reasonable assistance to Controller in connection with any data protection impact assessment ("**DPIA**") or prior consultations with supervisory authorities required under Data Protection Laws, to the extent that such assessment relates to Processor's processing of personal data.

10.2 Such assistance shall be limited to providing information that is: (i) within Processor's possession or control; (ii) reasonably necessary for the DPIA; (iii) not subject to confidentiality obligations to third parties; and (iv) not proprietary or commercially sensitive information of Processor. Processor may provide such information in summary or aggregated form where disclosure of detailed

information would compromise Processor's confidential information or intellectual property.

11 AUDIT RIGHTS

11.1 Controller shall have the right to audit Processor's processing of personal data once per year, unless more frequent audits are required by applicable laws, specific instruction of a competent data protection authority, or as warranted for cause. Such audits may be conducted by means of on-site inspections or by appointing a third-party auditor, provided that such auditors are not competitors of Processor. The Processor shall provide the Controller with reasonable access to its premises and personnel, and to all relevant documentation and systems, as necessary to facilitate the audit.

11.2 The following shall apply in relation to audits under this DPA:

a) Controller shall provide Processor with at least sixty (60) days' prior written notice of the audit;

b) the audit shall be conducted in accordance with a mutually agreed audit plan that sets out the scope, purpose, and methodology of the audit;

c) Controller shall comply with all reasonable security instructions provided by Processor;

d) Processor’s representative shall be entitled to be present during all stages of the audit, and the audit shall be conducted during Processor’s normal working hours;

e) Auditing shall be conducted in such a manner that Processor’s undertakings towards third parties are in no way jeopardized. All Controller’s representatives participating in the audit shall sign a confidentiality undertaking regarding any and all information disclosed to them during the audit;

f) Each Party shall bear its own costs and expenses in connection with the audit;

g) Controller shall keep the findings of the audit confidential, except to the extent that disclosure is required by applicable laws; and

h) If an audit reveals non-compliance by Processor with its obligations under this Agreement, Processor shall implement a remediation plan to resolve any non-compliance identified in the audit within a reasonable time period.

12 REMUNERATION

12.1 The Processor shall be entitled to reasonable remuneration on a time-and-materials basis at Processor's then-current professional services rates for all work and costs that arise based on: (a) Section 10; (b) audits going beyond the annual limitation set out in Section 11; or (c) additional instructions from the Controller that (i) go beyond the services, functions and the level of security that the Processor normally offers its customers or that are set out in the Agreement; or (ii) require significant time, resources, or expertise.

13 LIMITATION OF LIABILITY

13.1 The limitations of liability set out in the Agreement shall apply to Processor's liability under this DPA. Any reference in the Agreement to the aggregate liability of a Party means the aggregate liability of that Party under both the Agreement and this DPA. Notwithstanding any limitations on liability for indirect, consequential or similar damages, nothing in this DPA or the Agreement shall limit or exclude a Party's liability under Data Protection Laws for damages suffered by data subjects.

13.2 Any administrative fines imposed on a Party under Data Protection Laws should be paid by the Party that has failed in its performance of its legal obligations under the Data Protection Laws, as decided by the relevant supervisory authority or competent court authorized to impose such fines. In no event shall a Party be liable for the other Party's administrative fines, including under any indemnification obligations.

14 MISCELLANEOUS

Term

14.1 This DPA shall apply for the term of the Agreement or, if later, until all Services under the Agreement have been completed, provided however that the terms of this DPA shall continue to apply until all personal data processed under this DPA has been deleted or returned in accordance with Section 14.2 below.

Measures upon termination of this DPA

14.2 Upon termination of this DPA, Processor shall, as instructed and communicated in writing by Controller, either delete or return all personal data processed under this DPA without undue delay, and at the latest within thirty (30) days of receiving such notice from Controller, unless applicable laws require storage of the personal data.

14.3 At the request of Controller, Processor shall without undue delay provide Controller a written notice of the measures taken regarding the personal data, even if the Agreement or this DPA have been terminated.

Appendix 1

SPECIFICATION OF THE PROCESSING OF PERSONAL DATA

Nature and purpose Specify all purposes for which personal data will be processed by Processor	Personal data will be processed for Controller's access and use of the system, the performance of the Services and obligations under the Agreement, complying with this DPA, and any additional instructions from the Controller.
Categories of personal data Specify which categories of personal data Processor will process	Processor shall process the following categories of personal data: ☒ Email address ☒ Name ☒ Password (encrypted) ☒ Information contained in orders (where applicable) ☐ Other (please specify)
Categories of data subjects Specify for which categories of data subjects Processor will process personal data	☒ Users ☒ Recipients of orders (where applicable) ☐ Other (please specify)
Processing activities Specify which processing activities will be performed by Processor	Processor will perform the processing activities set forth in the Agreement, e.g. for authorization to the system and communicating with end users.
Duration Specify the duration of the processing	Personal data will be processed for the term of the Agreement and any additional period thereafter as set forth in the Agreement or this DPA. Personal data contained in orders processed on behalf of Controller will be erased 30 days after the respective order has been submitted to Processor. Personal data of users of the system will be erased in accordance with Section 7, unless instructed otherwise by Controller.

Location for the processing Specify all locations where personal data will be processed by Processor	Within EU/EEA

Appendix 2

PRE-APPROVED SUB-PROCESSORS

Name	**Address**	**Contact person's name, position & contact details**	**Description of the processing[1)]**
Azure (Microsoft)	Regeringsgatan 25, 111 53 Stockholm	As of the date of this DPA: Joakim Ragnmark Account manager +46734380050 Joakim.ragnmark@microsoft.com	Cloud-based data storage and management services: Azure provides secure data storage and analysis services, where personal data will be stored and retrieved as required, offering data backup, redundancy, and encryption services, ensuring the confidentiality and integrity of the data.

[1)] Including a clear delimitation of responsibilities in case several sub-processors are authorized.

TECHNICAL AND ORGANIZATIONAL MEASURES

Measures to ensure an appropriate level of security

The Processor has implemented and maintains the technical and organisational measures set out in this Appendix. The measures apply to the processing of personal data under the Data Processing Agreement (the DPA) and are designed to ensure a level of security appropriate to the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of natural persons. Capitalised terms used but not defined in this Appendix have the meanings given in the DPA.

1 INFORMATION SECURITY FRAMEWORK AND PROCESSING ENVIRONMENT

- The Processor operates an Information Security Management System certified to ISO/IEC 27001:2022 by InterCert. The certification covers Information Technology, Software Development, Information Security, Product Operations, Customer Success, Compliance and Finance. The certificate registration number is IC-IS-2601097 and the applicable Statement of Applicability is version 1.0.
- The Processor is Btwentyfour AG, Grafenauweg 8, 6300 Zug, Switzerland.
- Microsoft Azure is the Processor's hosting provider for the Services. All production operations for the Services are hosted within Microsoft Azure. The primary production environment is in Azure North Europe and is designed across multiple Availability Zones. Regional disaster recovery capabilities are maintained in Azure West Europe.
- The Processor maintains documented information security policies, assigned security responsibilities, risk assessment and treatment processes, internal audit activities, management review, security awareness training, incident management, change management and continual improvement processes.

2 MEASURES OF PSEUDONYMIZATION AND ENCRYPTION OF PERSONAL DATA

- Personal data is encrypted in transit and at rest using strong, industry-standard cryptographic mechanisms appropriate to the relevant system and risk.
- Authentication credentials are protected using strong cryptography. Passwords are stored using secure hashing and salting mechanisms where passwords are managed by the Processor. Secrets and credentials must not be hard-coded in source code or exposed in logs.
- Cryptographic keys are protected through restricted access, separation from protected data, encryption of stored keys, documented lifecycle management, rotation, revocation and replacement following suspected compromise. Access to key-management functions is limited to authorised personnel and is auditable.
- Pseudonymization, masking or anonymization is applied where appropriate to the processing purpose. Production personal data is not used in non-production environments unless specifically approved and protected through masking or equivalent safeguards.

3 MEASURES FOR ENSURING ONGOING CONFIDENTIALITY, INTEGRITY, AVAILABILITY AND RESILIENCE

- Access to systems and personal data is restricted by role, business need and the principle of least privilege. Privileged access is separately approved, documented, monitored and periodically reviewed.
- Production, development, testing and corporate environments are logically segregated. Network traffic is filtered through firewalls, access-control lists and security groups using deny-by-default and least-privilege principles.
- The Azure architecture uses multiple Availability Zones, redundant services, geo-redundant storage and a separate regional disaster recovery capability to reduce the impact of local and regional failures.
- Endpoint, network, application and cloud security controls include anti-malware protection, vulnerability management, security monitoring, alerting, DDoS protection, secure change management and controlled administrative access.

4 MEASURES FOR TIMELY RESTORATION OF AVAILABILITY AND ACCESS

- Critical Azure servers, databases and storage resources are covered by automated backup processes. Full snapshots and incremental backups are performed daily, and customer databases use point-in-time recovery capabilities where supported.
- Backup data is encrypted, access controlled and protected against unauthorised alteration or deletion. Geo-redundant backup and replication capabilities support recovery in Azure West Europe if recovery within Azure North Europe is insufficient.
- Backup status and replication health are monitored. Restoration tests are performed monthly and documented. Recovery procedures are maintained against defined Recovery Time Objectives and Recovery Point Objectives.
- Disaster recovery exercises, including Availability Zone recovery, regional failover, DNS behaviour, service accessibility and failback, are performed at least semi-annually. Business continuity and disaster recovery arrangements are reviewed at least annually and after material incidents or changes.

5 PROCESSES FOR TESTING, ASSESSING AND EVALUATING SECURITY MEASURES

- The Processor performs periodic risk assessments, internal audits, management reviews, access reviews, control testing and policy reviews as part of its ISO/IEC 27001:2022 certified ISMS.
- Automated internal vulnerability scanning is performed continuously, with findings reviewed regularly and remediation tracked according to severity and business risk.
- External vulnerability assessments and penetration tests are performed at least annually for critical systems and additionally following material releases or architectural changes. Application security assessments are required for new or major releases and use recognised practices such as OWASP.
- Findings from audits, scans, tests, incidents and recovery exercises are documented, assigned to responsible owners, risk assessed and tracked through remediation and validation.

6 MEASURES FOR USER IDENTIFICATION AND AUTHORIZATION

- Users are assigned unique accounts wherever possible. Shared and generic accounts are prohibited unless specifically approved and subject to compensating controls.

- Multi-factor authentication is enforced for critical systems and for company access where supported. Password controls include automated enforcement, protection against weak passwords, account lockout and controlled reset procedures.
- Access is granted through documented onboarding and approval processes based on role and business need. Elevated or privileged access requires separate approval and is recorded.
- Access rights are reviewed at least annually and after role changes. Inactive accounts are disabled or removed, and access is revoked promptly following termination or when no longer required.

7 MEASURES FOR THE PROTECTION OF DATA DURING TRANSMISSION

- Personal data transmitted over public or untrusted networks is protected using current secure protocols and encrypted channels, including TLS, HTTPS, SFTP, SSH, IPSec or approved VPN technologies, as appropriate.
- Administrative access is performed through encrypted management interfaces and trusted networks. Obsolete or insecure protocols and configurations are disabled.
- Certificates and cryptographic keys are validated, protected and replaced in accordance with documented key-management processes. Customer-provided certificates are subject to validation and documented approval before use.

8 MEASURES FOR THE PROTECTION OF DATA DURING STORAGE

- Personal data stored in Azure production systems, databases, file systems, storage accounts and backups is protected using Azure encryption capabilities and appropriate access controls.
- Sensitive data on laptops and other mobile devices is protected by full-disk encryption. Storage media is securely sanitised or disposed of when retired or reassigned.
- Encryption keys, secrets and administrative credentials are stored separately from protected data and are accessible only to authorised personnel or managed services with a documented business need.

9 MEASURES FOR ENSURING PHYSICAL SECURITY

- Physical security for the cloud infrastructure hosting the Services is provided through Microsoft Azure's controlled data-centre environment and is assessed through the Processor's supplier assurance and third-party risk management processes.
- Access to the Processor's offices, devices and physical information assets is restricted to authorised persons. Visitors and third parties are subject to appropriate access restrictions and supervision.
- Company devices are protected through encryption, authentication, secure configuration, inventory controls and secure return, sanitisation and disposal processes.

10 MEASURES FOR ENSURING EVENTS LOGGING

- Security-relevant events from systems, applications, authentication services and Azure infrastructure are logged and centrally monitored using Azure Monitor, Log Analytics or equivalent approved tooling.
- Logs include access and authentication events, privileged and administrative activity, security exceptions, unusual activity, changes and other events required for incident investigation and accountability.

- Access to logs is restricted to authorised personnel and maintained as read-only wherever possible. Logs are protected against unauthorised access, modification and deletion and are retained under documented retention requirements.
- Critical systems use synchronised time sources. Alerts and suspected violations are reviewed promptly, escalated where appropriate and handled through the incident management process.

11 MEASURES FOR ENSURING SECURE SYSTEM CONFIGURATION

- Documented baseline configurations and hardening requirements apply to cloud resources, networks, applications, endpoints and security devices. Default credentials are changed or disabled before deployment.
- Firewall, routing and access-control rules permit only necessary traffic and are reviewed at least quarterly. Direct Internet access to sensitive systems is prohibited, and administrative access is restricted to trusted networks.
- Changes to systems and configurations are risk assessed, reviewed, approved, tested, logged and subject to rollback arrangements. Emergency changes are documented and retrospectively reviewed.
- Systems are patched and updated according to vulnerability severity and risk. Infrastructure-as-code and version control are used where feasible to support consistent, auditable configuration.

12 MEASURES FOR INTERNAL IT AND SECURITY GOVERNANCE AND MANAGEMENT

- The Processor maintains defined responsibilities for executive management, the CISO, the Information Security Officer, IT Operations, Security Operations, System Owners, Development and incident response teams.
- Information security risks are recorded, assessed, treated and reviewed. Significant risks, audit findings, incidents and remediation status are reported to management and, where appropriate, the Board.
- Personnel and relevant contractors receive recurring security and privacy awareness training and acknowledge applicable policies at least annually. Confidentiality obligations apply to persons authorised to process personal data.
- Third parties are subject to due diligence, contractual security and data-protection obligations, risk review and ongoing oversight appropriate to the service provided.

13 MEASURES FOR CERTIFICATION AND ASSURANCE OF PROCESSES AND PRODUCTS

- The Processor maintains an ISO/IEC 27001:2022 certified ISMS. The current certificate was initially issued on 9 January 2026 by InterCert under registration number IC-IS-2601097, with surveillance validity through 8 January 2027 and recertification scheduled for 8 January 2029.
- The certification scope includes Information Technology, Software Development, Information Security, Product Operations, Customer Success, Compliance and Finance.
- Assurance activities include internal audits, management review, vulnerability scanning, independent penetration testing, supplier assurance, policy review, business continuity and disaster recovery testing, and tracking of corrective actions.
- Evidence of the Processor's certification and relevant assurance activities may be made available to the Controller subject to appropriate confidentiality and security restrictions.

14 MEASURES FOR ENSURING DATA MINIMIZATION

- Systems and processing activities are designed to limit the personal data collected, accessed and retained to what is necessary for the documented purpose and the performance of the Services.
- Role-based access, least privilege, masking and environment segregation limit unnecessary exposure. Production data is not used in non-production environments unless approved and protected through masking, anonymization or equivalent controls.
- Sensitive personal data and authentication secrets are excluded from application logs, debugging output and client-facing error messages unless strictly necessary and appropriately protected.

15 MEASURES FOR ENSURING DATA QUALITY

- The Services include controls and procedures appropriate to maintain the integrity and accuracy of personal data during authorised processing, including input validation, controlled changes, monitoring and error handling.
- The Processor supports the Controller, within the functionality of the Services and the Processor's obligations under the DPA, in correcting or updating inaccurate personal data.
- Changes to production systems and data structures are reviewed, tested, version controlled and subject to validation before deployment.

16 MEASURES FOR ENSURING LIMITED DATA RETENTION

- Personal data is retained only for the duration necessary to provide the Services, meet documented Controller instructions and satisfy applicable legal or contractual requirements.
- Personal data contained in orders is erased from active systems 30 days after the respective order has been submitted to the Processor, as specified in Appendix 1 to the DPA.
- Backup copies are maintained under documented, limited and automatically enforced retention schedules. They are isolated from normal use, accessed only for recovery and expire through scheduled deletion or overwriting.
- When data is restored from backup, applicable access restrictions, retention rules and deletion instructions are reapplied. Retention schedules are reviewed and records of deletion and restoration activities are maintained where appropriate.

17 MEASURES FOR ENSURING ACCOUNTABILITY

- Security and processing activities are supported by documented policies, assigned owners, approvals, audit trails, access reviews, change records, risk assessments, training records and incident records.
- Administrative and privileged activities are logged and monitored. Access, changes, vulnerabilities, incidents and corrective actions are recorded in approved systems and retained for audit and compliance purposes.
- The Processor maintains procedures to support the Controller with audits, data-subject requests, personal data breaches, data-protection impact assessments and evidence of compliance in accordance with the DPA.

18 MEASURES FOR ALLOWING DATA PORTABILITY AND ENSURING ERASURE

- The Processor maintains procedures and technical capabilities to retrieve, export, return, correct, restrict or erase personal data on the Controller's documented instruction, to the extent technically feasible and required under the DPA.
- Personal data can be exported in commonly used, structured formats where supported by the Services. Export and return activities are subject to authentication, authorisation, encryption and logging controls.
- Erasure is performed through controlled deletion from active systems and scheduled expiry from protected backup sets. Access to data pending backup expiry remains restricted, and the data is not used for any purpose other than recovery and continuity.
- Upon termination, personal data is returned or erased in accordance with the Controller's written instruction and the DPA, subject only to applicable legal retention requirements.

The Processor may update or replace individual measures to reflect technical progress, changes in risk or changes to the Services, provided that the overall level of security is not materially reduced.