COMCAST BUSINESS

Description of the Technical and Organizational Measures ("TOMs") implemented by the Data Importer (Comcast Business, Masergy, and Nitel) for Network, Security, and Unified Communications Services

This Appendix forms part of the Data Protection Addendum – Appendix 2.

More information about Comcast's security measures is available in the Comcast Cybersecurity Information Security Program Summary set forth on the Comcast Business Privacy Center (available at business.comcast.com/privacy).

Comcast will ensure an appropriate level of security, taking into account the nature, scope, context, and purposes of processing and the risks for the rights and freedoms of natural persons, including maintaining the following safeguards to protect Personal Data:

Measures for protection of personal data:

1. **Encryption and cryptography:** Personal Data is encrypted both at rest and in transit by default with industry-standard transport encryption (AES-256 encryption or TLS 1.2 or higher for data in transit). Use of comprehensive cryptographic controls for the protection of information that is processed by Comcast. Policies and procedures in place for the management of cryptographic keys including use, protection and lifetime of cryptographic keys.

2. **Segmentation:** Segregation of information services, users, and information systems.

3. **Information classification:** Information is classified based on value, criticality and sensitivity (based on Comcast assessment). Security controls are designed and implemented based on this classification.

4. **Access control:** Allocation and control of user credentials and privileged access rights on a least-privilege, role-based access basis based on business and cybersecurity requirements. Review of access and limits (as required) at regular intervals. Procedure to manage user access registration and de-registration. Removal or adjustment of access rights upon termination of employment, contract, or engagement, or role change.

5. **User identification:** MFA (where appropriate and consistent with Comcast's AC-S.07.01 Authentication Management and related standards). Password quality requirements which passwords must comply with. A Single Sign-On (SSO) is used to ensure consistent application of password policy.

6. **Physical security of locations at which Personal Data are processed:** Physical security requirements and monitoring including secure buildings, key-card access monitoring / badge-based access systems and logging of access. Visitor access controls including a pre-registration requirement, visitor identification (via QR codes) and visitor escorting.

7. **Data minimisation and quality:** Comcast applies data minimisation principles and personal data is only collected where necessary for the operation of the services. Procedures are in place to update or correct inaccurate administrative records, user details, contact records, access entitlements and incident logs.

8. **Retention:** Identifiable user data is only retained for as long as is required for the relevant purposes or in accordance with contractual and legal requirements and it is deleted when it is no longer required. Retention and disposal schedules are documented in public policies and technical specifications.

9. **Erasure and disposal:** Secure disposal of hardware once no longer required, including storing physical media which is awaiting disposal, in a separate controlled area with restricted access and periodic log views. Information assets are handled and/or disposed of according to their classification. Hardware assets are disposed of responsibly, securely and verifiably through accredited third-party partners. Software assets are retired and removed from service securely.

Measures for ongoing confidentiality, integrity, availability and resilience of systems and services

1. **Asset Management:** All assets related to the services are managed across the lifecycle. Automated mechanisms in place to detect unauthorised assets, and to report and/or escalate these in accordance with the relevant policy.

2. **Asset Inventories:** Asset inventory in place for systems/assets related to the services that process information with owners assigned to such assets and updated following relevant events. All assets are required to be returned by personnel upon termination of their employment, contract or engagement, via an asset return procedure.

3. **NIS protection:** Management and control of networks to protect information and systems and network segmentation, including firewalls (e.g. Web Application Firewall (WAF) where applicable for customer facing applications).

4. **Vulnerability management:** Vulnerability management processes for the scanning and management of systems and remediation of vulnerabilities within defined SLAs. Remediation of vulnerabilities based on risk using automated tools as appropriate to the system/ application. Penetration testing carried out where necessary and appropriate to the system.

5. **Patching:** Patching process in place for software updates and patches.

6. **Development and change management:** Development and change management processes to govern secure installation, configuration and updates to software on secure network systems. Changes are managed and controlled in accordance with Comcast change management processes. Each release of any new software or hardware goes through the security development lifecycle process to ensure all cybersecurity guardrails are implemented.

7. **Employee accountability:** Background checks for employment in accordance with relevant laws, regulations and ethics. All employees involved in the services are required to complete annual security and privacy awareness training and, where relevant, additional role-specific training. Employees and contractors are required to comply with information and assets and data handling policies. Equivalent standards are imposed on non-employee users by way of contractual acceptable use obligations.

Measures regarding the ability to restore the availability and access to Personal Data in a timely manner in the event of an incident

1. **Cybersecurity Incident Process:** Response process in place for cybersecurity incidents including assessment of cybersecurity events and determination of cybersecurity incidents. Internal reports of cybersecurity events are shared with employees/teams through appropriate management channels. Lessons learned from incidents are used to train and update policies/procedures.

2. **Management accountability for incidents**: Management responsibility and procedures in place in response to such incidents. Simulations include management engagement in decision-making authority, oversight responsibilities and accountability frameworks.

3. **Recovery:** A Business Continuity (BC) and Disaster Recovery (DR) programme is aligned with industry BC/DR standards and includes Recovery Time Objectives (RTO) and Business Continuity Plans (BCP). Such plans are tested on a regular basis.

4. **Backups and redundancy:** Comcast maintains encrypted backups of Personal Data (including configuration data required to restore services) with defined retention periods, access controls and integrity checks. Redundancy of information processing facilities is maintained for disaster recovery purposes.

5. **Physical protection measures:** Physical protection against natural disasters, malicious attack, accidents and power outage. Maintenance of equipment required for the provision of the services in accordance with its internal processes.

Processes for regularly testing, assessing and evaluating the effectiveness of TOMS

1. **Governance and management:** Information security management programme in place with documented policies which are aligned to recognised standards, including SOC 2.

2. **Cybersecurity responsibilities:** Cybersecurity responsibilities are defined, allocated and segregated across Comcast and group entities across: (A) Comcast Cyber Security (enterprise-level information security governance, including enterprise security policies and is responsible for incident response); (B) Comcast Information Security Team (reviews risks and prioritises security-related projects and initiatives); and (C) [product / service] engineering, and technical operations teams (services-level implementation of security controls and for secure development practices, in line with Comcast and ISO requirements). Comcast has dedicated and identified persons (BISO) that oversee the company's information security and compliance programme and data protection. Comcast has a data protection program in place which includes Data Protection Officer appointments. Please see the Comcast privacy policy for further details (https://www.xfinity.com/privacy/policy).

3. **Review and testing of controls:** Review of goals and objectives for cybersecurity at regular intervals (at least annually). Reviews conducted on a regular basis (at least annually) to assess

compliance of information systems with applicable policies and standards and certification frameworks under Comcast's security controls framework, Comcast Group Audit (CGA) programme, and TPSA recertification processes. Includes ongoing monitoring mechanisms, internal audits and independent SOC 2 Type 2 audit reports, external audits, third party penetration testing, periodic internal audits of its security controls with management oversight. Policies and processes are tested with war game exercises, tabletop exercises and technical failover tests on a regular basis.

4. **Audit:** Audit activities are planned and scoped in accordance with group methodologies and are risk-based. Security audits of internal systems conducted internally and using third parties. Selected managed network services have SOC certifications and are therefore audited in accordance with the SOC requirements.

Measures for Managing Suppliers

1. **TPSA**: Suppliers are required to meet defined and documented security requirements through a third-party security assurance programme that includes that (A) suppliers are subject to risk-based due diligence on information security and data protection capabilities including by completion of risk assessments; (B) suppliers are required to maintain certification or independent assurance proportionate to the services and to the Personal Data processed (such as ISO 27001, NIST, SOC 1 / SOC 2 or Cyber Essentials Plus or equivalent); (C) ongoing monitoring of supplier compliance through TPSA status tracking; and (D) supplier relationships are reviewed through TPSA processes and reassessments where risk levels change or incidents occur.

2. **Supplier contracts:** Suppliers are engaged pursuant to written contracts imposing obligations related to restricted transfers, security controls, and assistance with data subject measures. Requirements are at least as restrictive as the security obligations provided for Comcast employees. Suppliers are subject to a contractual right to audit, exercisable to verify their compliance with applicable information security and data protection requirements (as applicable and necessary for the services).

3. **Other measures:** Processes for handling law enforcement requests. Comcast periodically, and when required by changes in data protection laws or regulatory guidance, reviews policies in relation to overseas transfer of Personal Data for compliance with data protection laws.