DataBee
COMCAST TECHNOLOGY SOLUTIONS

DataBee TOMS

Schedule 1B — Description of the Technical and Organizational Security Measures implemented by the Data Importer

Company will maintain security measures as set out below with respect to the processing of Company Personal Information (PI) under the Agreement.

Organizational Safeguards

1. **Data Disclosure.** Comcast shall maintain written processes and procedures covering the public disclosure of Company PI including:
    - Reviewing and limiting the scope of Company PI disclosed to public authorities; and
    - Keeping an internal record of requests made by public authorities concerning Company PI
2. **Security Program.** Comcast has designated an information security team that identifies reasonably foreseeable internal and external risks, assesses the sufficiency of safeguards, and adjusts the security program based on business changes. Comcast reviews risks and prioritizes security-related projects and initiatives.
3. **Security Policies.** Information security policies are made available to relevant personnel and reviewed periodically.
4. **Hiring.** Comcast requires all new personnel to review and agree to its information security and confidentiality policies during the onboarding process.
5. **Training.** Comcast trains workforce members that have access to Customer Personal Data concerning appropriate privacy and security practices and compliance with Comcast's data protection obligations. Comcast also provides mandatory information security training on an annual basis to designated personnel.
6. **Subprocessors.** Comcast maintains policies to ensure appropriate access to Customer Personal Data in production environments. Comcast requires all Subprocessors that provide technology infrastructure components for Customer Personal Data to maintain appropriate cybersecurity measures. Comcast policy requires that agreements between Comcast and the Subprocessors include appropriate cybersecurity requirements associated with Customer Personal Data.
    - Comcast manages all changes to the provision of services by Subprocessors, including maintaining and improving existing cybersecurity policies, procedures, and controls. Any change to services provided by a Subprocessor are required to go through Comcast's Third-Party Security Assessment process.
    - All Subprocessors are vetted though Comcast's vendor management program.
    - All equipment partners and distributors are vetted through Comcast's procurement process.

Administrative Safeguards

7. **Security Program.** Comcast shall designate an information security team to identify reasonably foreseeable internal and external risks, assess the sufficiency of safeguards, and adjust the security program based on business changes. Such team shall review risks and prioritize security-related projects and initiatives. Management will assign a qualified person with the appropriate expertise in information security to direct and manage the information security program.
8. **Security Policies.** Comcast shall maintain a written information security program that describes the governance and structure of the information security program as well as documenting policies and standards that are reviewed annually.
9. **Hiring.** As part of their onboarding process, new Comcast personnel with access to Company PI shall undergo background checks and agree to Comcast's information security and confidentiality policies.
10. **Training.** Comcast shall train its personnel that have access to Company PI on appropriate privacy and security practices and Comcast's obligations under the Data Processing Agreement (DPA). Comcast shall also provide mandatory general information security training on an annual basis to appropriate personnel.
11. **Subprocessors**. Comcast shall require its Subprocessors that process Company PI to go through Comcast's Third-Party Security Assessment process and to maintain appropriate cybersecurity measures. In the event of a material change in the Subprocessors' services, such Subprocessors must be reassessed through the Third-Party Security Assessment process. Comcast shall have contracts in place with its Subprocessors that include appropriate privacy and security requirements no less protective of Company PI than the DPA.
12. **Assurance.** DataBee has received and holds current System and Organizational Controls (SOC) 2 Type 1 assessment and its ISO 27001, 27017, and 27018 certifications. Comcast will provide a copy of its current SOC 2 Type 1 assessment and its ISO 27001, 27017, and 27018 certifications upon Company's request. Such documentation shall be treated as Comcast's Confidential Information.

Physical Safeguards

13. **Access Control.** Comcast's facilities are secured with a building access control system, and its ingress and egress doors are secured. Controls shall be in place to prevent unauthorized persons from gaining access to premises where data processing systems that process Company PI are located.
    - Networking and other required equipment shall be physically secured in areas restricted only to personnel that require such access.
    - Staff shall be present 24x7 at Comcast's facilities.
    - Visitor access processes are implemented, and visitor access shall be controlled and logged.
14. **Termination of Access Controls.** Comcast shall terminate individuals' physical access to facilities that are dedicated to the provision of the Services when such individuals no longer need such access to perform Services. Documented processes shall be in place to offboard such individuals.
15. **Printing.** Comcast will not print hard copies of Customer Personal Information.
16. **Data Destruction.** Comcast shall securely destroy Company PI (such that the data is unreadable or unusable) from its systems at or before the expiration or earlier termination of this Agreement.

Technical Safeguards

17. **Access Controls.** Comcast shall have policies and procedures in place designed to ensure that access to Company PI is properly controlled with the following measures:
    - Access is granted based on an employee's job function.
    - Role-based access is used in granting access.
    - Administrative access is only allowed for a defined duration and approved by management (i.e., for only a few hours or a day if required).
    - Segregation of duties is considered when granting access.
    - Periodic access reviews are performed.
    - Multi-factor authentication is required to access Company PI and associated systems.
    - Access provisioning and de-provisioning processes are in place, including revoking access when an employee is separated from Comcast or no longer needs access based on job responsibilities.
    - Each individual that has access to Company PI shall have a unique ID.
    - Password sharing between users is prohibited, and passwords shall be changed upon initial log-in. The policy also requires subsequent passwords be changed at regularly scheduled intervals. Passwords shall be hashed and not kept in free-text form.
    - Comcast's computers and systems shall be configured to automatically lock after a period of inactivity, and a unique password shall be required to unlock such computer or system.
18. **Cryptography.** Comcast shall have a formal policy on the use of cryptographic controls for protection, including the use, protection, and lifecycle of cryptographic keys. Comcast shall protect Company PI and, where encrypted, shall use a Federal Information Processing Standard (FIPS)-compliant encryption product, also referred to as 140-2 compliant. Symmetric keys shall be encrypted with a minimum of 128-bit key, and asymmetric encryption requires a minimum of 1024-bit key length.
19. **Encryption.** Comcast shall utilize commercially available and industry standard encryption technologies for Company PI that is:
    - Being transmitted by Comcast over public networks (i.e., the internet) or when transmitted wirelessly; or
    - At rest, using TLS 1.2 encryption or higher in the design of all systems that support the Services
20. **Antivirus/Anti-Malware.** Comcast shall require that each employee's Comcast-managed workstation that is used to access Company PI has a functioning and updated antivirus/anti-malware program. In addition, Comcast shall scan all attachments for known malicious code and deploy URL filtering to limit systems from connecting to non-approved malicious websites.
21. **Network Security.** Comcast shall maintain network security controls to appropriately restrict access to Company PI, including:
    - Using network segmentation to limit only authorized hosts and users from accessing systems containing Company PI
    - Using AES-256 encryption for wireless networks accessing systems containing Company PI
    - Putting intrusion detection and prevention systems in place to detect anomalous activity and determine whether Comcast's computer network and/or server(s) have experienced an unauthorized intrusion
    - Only allowing approved ports and protocols that are required for business and reviewing the approved port listing by information security and subjected to change management procedures
    - Placing publicly accessible services on a separate, isolated network segment typically referred to as the Demilitarized Zone (DMZ)

- Segmenting, as appropriate, groups of information services, users, and information systems
- Terminating external network connections with a "deny all" rule. "Any any" rules are not allowed.
- Mitigating DDoS defense using various methods, including but not limited to ISP scrubbers, edge routers, application filters, and/or using separate logical channels

22. **Wireless Access Control.** Comcast shall protect wireless communications using:
    - Strong encryption (AES-256)
    - Authentication using multi-factor authentication
    - Wireless communication controls that include the performance of scans for unauthorized access points on a regular basis
23. **Application Security.** Comcast shall maintain the following application-based security controls:
    - Implementing processes to perform code reviews for applications and platforms storing Company PI
    - Not granting developers access to production environments
    - Reviewing and testing input validation and output encoding routines of application software
    - Segregating production environments from test and development environments
    - Documenting change management processes, including requirements for approvals, implementation and regression testing, and documented rollback procedures
    - Testing in-house developed and/or third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, when applications are updated, and on a recurring basis
    - Not making development artifacts (e.g., sample data and scripts, unused libraries, components, debug code or tools) accessible from the production environment
    - Providing data segmentation and separation capability (i.e., physical or logical separation) between clients (e.g., multi-client databases, on premise, or cloud services)
    - Providing, maintaining, and supporting Comcast's software, including subsequent updates, upgrades, and bug fixes, to keep the software from Common Software Vulnerabilities, in accordance with its product end-of-life (EOL) and end-of-sale (EOS) policy
    - Providing updates and patches to remediate security vulnerabilities based on severity using CVSSv3 scores and remediating known zero-day exploits without undue delay
24. **Security Patching.** Comcast shall have procedures in place to regularly update and patch operating systems and software that contain or access Company PI. Comcast shall implement updates it determines are critical in an accelerated timeline.
25. **Incident Response.** Comcast shall comply with its written incident response plan when responding to security incidents, which plan shall be reviewed at least annually. Comcast shall regularly test and monitor the effectiveness of key controls, systems, and procedures that are designed to prevent and detect security incidents. Comcast shall utilize a 24x7x365 dedicated incident response function, which it shall regularly test.
26. **Vulnerability Management.** Comcast shall conduct vulnerability scans on a regular basis on Comcast's computing environment that processes Company PI. Comcast shall regularly review vulnerabilities and prioritize vulnerabilities for remediation based on severity.
27. **Testing.** As part of its security testing, Comcast shall test unauthenticated and authenticated primary application components, and conduct manual and automated penetration testing to identify vulnerabilities. Comcast shall monitor vulnerability/threat intelligence feeds for up-to-date information about current general security threats, technology-specific vulnerabilities, and patch release information. In addition, Comcast shall use third-party auditors, at least annually, to conduct automated (i.e., SAST, DAST, and SCA) and manual security (i.e., penetration testing) assessments to scan the Product codebase for known exploitable conditions classified as "Critical/Very High" or "High," or otherwise captured on the OWASP Top 10 or SAN Top 25 lists.
28. **Secure Configuration.** Comcast shall employ secure hardening standards for all systems and applications. In addition, Comcast shall use baseline configuration tools to confirm that critical system files (including sensitive system and application executables, libraries, and configurations) have not been altered and enforce the configuration settings on a scheduled basis.
29. **Communications Security.** Comcast shall put data transfer policies and procedures in place to protect Company PI that is transferred electronically.
30. **Data Transfers.** Comcast shall have controls in place that are designed to prevent Company PI from being read, copied, modified, or deleted without authorization during electronic transport or storage. Such controls shall also enable Comcast to establish and verify the transmission facilities that receive Company PI. Comcast shall implement management connections to the servers that occur over encrypted Secure Shell (SSH), Transport Layer Security (TLS), or Virtual Private Network (VPN) channels and require multi-factor authentication for remote access. Comcast shall not allow management access from the internet as part of delivering the Services, unless the connection originates from a list of trusted IP addresses. Comcast shall implement a change management system to submit, authorize, and review changes made to the protection environment. Comcast shall maintain a dedicated Network Operations Center (NOC) and a dedicated Security Operations Center (SOC), which are staffed 24x7.

31. **System Logging.** Comcast shall log system errors and security events. Comcast shall protect log files from alteration and approve and document all procedures. In addition, Comcast shall actively monitor log files on an ongoing basis.
32. **Resilience and Business Continuity.** Comcast shall implement a business continuity and disaster recovery program in accordance with industry standards, including recovery of time and point objectives. Comcast shall provide redundancy of information processing facilities for disaster recovery purposes. Comcast shall review and validate all established and implemented cybersecurity continuity controls at regular intervals. Comcast shall put each release of its software providing the Services through its security development lifecycle process to implement cybersecurity guardrails.
33. **Compliance.** Comcast implements procedures to evaluate compliance with applicable regulatory and contractual requirements.
34. **Asset Management.** Comcast shall put asset management procedures in place, which include:
    - Maintaining an inventory of assets associated with Company PI and facilities processing such information
    - Assigning an individual or group to be accountable and responsible for each assigned asset processing Company PI
    - Implementing a policy to define acceptable use of assets processing Company PI
    - Documenting and tracking the return of assets from employees and contractors upon termination of their employment, contract, or agreement
    - Developing and implementing procedures for handling assets based on the nature of the Company PI