DataBee
COMCAST TECHNOLOGY SOLUTIONS

Data Processing Agreement

This Data Processing Agreement ("DPA") between Comcast and Company (each a "Party") is part of and incorporated into the Agreement. Except as expressly stated, in the event of a conflict between the documents comprising the Agreement, the order of precedence in descending order is: SCCs, UK SCCs, DPA body, DPA appendices, and remainder of the Agreement.

1. **Definitions.** The following words and their derivations shall have the meanings given to them in this section:

   1.1 **"Agreement"** means the agreement between Comcast and Company that references this DPA.

   1.2 **"Affiliates"** of a Party means an entity that directly or indirectly, through one or more intermediaries, controls, is controlled by, or is under common control with such Party.

   1.3 **"Business Contact Information"** means Personal Information that a Party collects from the other Party's personnel for the sole purpose of maintaining a business relationship with that Party (e.g., contracting, billing, general relationship inquiries). For the avoidance of doubt, this excludes Personal Information related to the substance of the Services.

   1.4 **"Business Purpose"** means the purposes of processing Personal Information listed in the Processing Activities Table.

   1.5 **"Comcast"** means Comcast Cable Communications, LLC and its Affiliates.

   1.6 **"Company"** means the Party receiving the Services from Comcast under the Agreement.

   1.7 **"Company PI"** means Personal Information listed in the Processing Activity Table below that Comcast receives from, or on behalf of, Company and that Comcast processes on behalf of Company in connection with the Services. For the avoidance of doubt, Company PI does not include information that has been aggregated or anonymized.

   1.8 **"Controller"** means the Party that determines the purpose and means of the processing of Personal Information.

   1.9 **"Data Subject"** means the individual or household that the Personal Information is attributed to.

   1.10 **"Data Subject Request"** means a request from a Data Subject to exercise his or her rights afforded under Privacy Law.

   1.11 **"European PI"** Company PI that is subject to GDPR or FADP (as such terms are defined in Schedule 1) and originates from one of the European Territories.

   1.12 **"European Territories"** means the European Economic Area, United Kingdom, or Switzerland.

   1.13 **"Personal Information"** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked with an identifiable individual or device.

   1.14 **"Personnel"** means Comcast's employees, Subprocessors, subcontractors, agents, and officers processing Company PI.

   1.15 **"PI Breach"** means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Company PI while within the possession of Comcast.

   1.16 **"Privacy Laws"** means applicable laws and regulations relating to data security, protection, and/or privacy.

   1.17 **"Processing"** means an operation or set of operations performed on data.

   1.18 **"Processor"** means the Party that processes Personal Information on behalf of and at the direction of the Controller.

   1.19 **"Restricted PI"** means Company PI (i) revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, (ii) that is genetic data, biometric data processed for the purposes of uniquely identifying a natural person, data, concerning health, or data concerning a natural person's sex life or sexual orientation, (iii) relating to criminal convictions and offenses, (iv) related to Data Subjects under the age of 18, or (v) similar categories of Personal Information that receive a highlighted level of protection under Privacy Laws.

   1.20 **"Services"** means the services and/or products supplied by Comcast to Company pursuant to the Agreement.

   1.21 **"Subprocessor"** means any entity that processes Company PI on behalf of Comcast.

Personal Information Processing Activities ("Processing Activity Table")	
Specific Business Purpose and Services for which Company PI is Processed	• To provide the Data Bee Services as further described in Introduction (databee.buzz) • Building or improving the quality of the services, provided that it is not used to perform services on behalf of another
Categories of Company PI Processed	Workforce IDs, user IDs, workforce titles, first and last names who have active directory/ IDP registrations, workforce email addresses, workforce IDs, connection data, IP address, MAC address, business hierarchy
Data Subjects	Company workforce inclusive of full-time employees and other authorized users of Company
Special Categories of Company PI	None
Subprocessors	Amazon Web Services, AWS hosting service
Duration of Processing	Up to 7 days , unless otherwise agreed to by the parties
Location of Processing	AWS data center locations as determined mutually by Comcast and Company
Data Exporter Information	Name: [ ] Address: [ ] Contact person's name, position, and contact details: [ ] Activities relevant to the data transferred under these SCCs: [ ] Role (controller/processor):

2. Status of the Parties and Scope.

   2.1 **Comcast as Processor.** As between Comcast and Company, Company is the Controller and Comcast is the Processor of Company PI. The Company PI is described in the Processing Activity Table. Company shall not provide or otherwise make Personal Information available to Comcast other than the Company PI described in the Processing Activity Table.

   2.2 **Business Contact Information.** Each party is the Controller of the Business Contact Information it receives related to the Personnel of the other party. Business Contact Information may only be used for the business purpose of maintaining the business relationship, and it must be protected using appropriate technical and organizational measures in accordance with Privacy Laws. Comcast's privacy notice at xfinity.com/privacy/policy describes Comcast's information practices in relation to Company's Business Contact Data.

3. **Company Obligations.** Company represents and warrants that (i) it has complied, and will continue to comply, with Privacy Laws with respect to its processing of Personal Information, (ii) it is permitted and has all necessary consents and notices to allow Company to process Company PI in accordance with this DPA, (iii) its instructions for the processing of Company PI comply with Privacy Laws, and (iv) it will not share or otherwise make Restricted PI available to Comcast under the Agreement. Company shall have sole responsibility for the accuracy, quality, and legality of Company PI and for Company's collection, use, and disclosure thereof.

4. **Limitations on Processing.** Comcast shall process Company PI in accordance with Company's written instructions. Comcast certifies that it understands and will comply with the restrictions of the DPA. Comcast and its Subprocessors shall, unless otherwise permitted by Privacy Law:

   4.1 Only process the Company PI for the Business Purposes described in the Processing Activity Table;

   4.2 Not sell Company PI for valuable consideration or share Company PI for cross-context behavioral advertising;

   4.3 Not process Company PI outside the direct business relationship between Comcast and Company;

   4.4 Not combine Company PI with Personal Information that it receives from or on behalf of another person or collects from its own interaction with the Data Subject, except in furtherance of the Business Purposes;

   4.5 Implement reasonable security procedures and practices appropriate to the nature of the Company PI designed to protect from unauthorized or illegal processing;

   4.6 Promptly notify Company if it determines it can no longer meet its obligations under Privacy Law or the DPA;

   4.7 Notify Company if, in Comcast's opinion, Company's instructions violate Privacy Law; and

   4.8 Restrict access to Company PI to those authorized persons who need such information to fulfill the Business Purposes and ensure such authorized persons (i) process Company PI in accordance with the Agreement, (ii) are obligated to maintain the confidentiality of Company PI, (iii) are appropriately supervised, and (iv) are provided with appropriate training in the care and handling of Personal Information.

5. **Data Subject Requests.** Comcast will maintain appropriate measures to assist Company in responding to Data Subject Requests. In the event Comcast receives a Data Subject Request or any other request or complaint related to Company PI, Comcast shall promptly notify Company. Comcast will cooperate with Company to the extent necessary to fulfill a Data Subject Request.

6. **Cooperation.** Comcast will cooperate with Company in its efforts to comply with Privacy Laws. If Comcast receives a governmental inquiry related to Company PI, Comcast will inform Company and will cooperate with Company's reasonable requests. In the event that Comcast receives a request from a governmental authority that requires the disclosure of Company PI, Comcast shall (i) attempt to redirect the governmental authority to request such information directly from Company, and (ii) inform Company of such request.
7. **Subprocessing.** Company gives its general authorization for Company to use the Subprocessors listed in the Processing Activity Table in connection with its provision of the Services. Company also authorizes Comcast to add or remove Subprocessors with 15 days prior notice to Company. Company has 15 days from such initial notice to raise reasonable objections, related to data protection, with such new Subprocessors. The Parties shall work together in good faith to resolve any such objections. If the Parties cannot come to a mutually agreeable resolution, and Comcast is unable or unwilling to continue to offer the Services without the use of the objectionable Subprocessor, then Company may terminate the applicable portion of the Services upon 30 days written notice to Comcast.
8. **Security.** Comcast shall maintain commercially reasonable physical, administrative, and technical security controls with respect to its processing of Company PI that are appropriate to the context and the risk of its activities and the Company PI being processed.
9. **Audits.** Comcast grants Company the right, upon written notice and mutual agreement of the means and scope, to (i) take reasonable and appropriate steps to help ensure that Comcast's use of Company PI is consistent with Company's obligations under the DPA and Privacy Laws, and (ii) reasonably request that Comcast stop and remediate any unauthorized use of Company PI by Comcast. Company may conduct a reasonable written assessment of Comcast's compliance under this DPA pursuant to Privacy Laws, and Comcast will provide reasonable information to demonstrate its compliance with such obligations. Company will treat all information received pursuant to this section as Confidential Information consistent with the terms of the Agreement.
10. **Personal Information Breach.** In the event Comcast becomes aware of a PI Breach, it will (i) notify Company without undue delay, (ii) provide reasonable assistance to remediate, investigate, and mitigate the PI Breach, and (iii) assist Company in meeting its obligations under Privacy Law. Comcast's notice shall describe the nature of the PI Breach, including, where known, the categories and approximate number of Data Subjects concerned and the categories and approximate number of Personal Information records concerned; communicate the name and contact details of the data protection officer or other contact point where more information can be obtained; describe the likely consequences of the PI Breach; and describe the measures taken or proposed to be taken to address the PI Breach, including, where appropriate, measures to mitigate its possible adverse effects.
11. **Limitation of Liability.** Comcast's liability arising out of or related to this DPA, whether in contract, tort, or under any other theory of liability, is subject to the "Limitation of Liability" (or similarly titled) section of the Agreement, and any reference in such section to the liability of a Party means the aggregate liability of that Party under the Agreement as a whole, including this Addendum.
12. **European Transfer.** Company acknowledges that the Services may involve the processing of Company PI in locations outside the European Territories, including the United States. The Parties shall comply with Schedule 1 if the Company PI contains European PI, either because such data was imported directly to Comcast from the European Territories or was provided to Comcast as part of an onward transfer.

IN WITNESS WHEREOF, each of the Parties has caused this DPA to be executed by its duly authorized representative.

COMCAST CABLE COMMUNICATIONS MANAGEMENT, LLC	**Customer**
By: _____	By: _____
Name: Nicole Bucala	Name: _____
Title: VP/GM Comcast Technology Solutions	Title: _____
Date: _____	Date: _____

Schedule 1 — European Transfers

1. **Additional Definitions.**

   1.1 **"FADP"** means the Swiss Federal Act on Data Protection of 25 September 2020 and its implementing regulations.

   1.2 **"GDPR"** means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

   1.3 **"SCCs"** means the European Union standard contractual clauses or any successor documents or data transfer schemes. As of the date of this DPA, "SCCs" means the clauses contained in the annex to the Commission Implementing Decision (EU) 2021/914 of 4 June 2021.

   1.4 **"UK SCCs"** means the United Kingdom standard contractual clauses or any successor documents or data transfer schemes. As of the date of this Exhibit, a reference to "UK SCCs" means the UK Addendum to the EU Commission Standard Contractual Clauses issued by the UK Information Commissioner's Office.

2. **Data Transfers From a European Territory.** To the extent that Comcast processes European PI in a country that has not been designated by the European Commission, United Kingdom Government, or Swiss Federal Data Protection Authority as providing an adequate level of protection for Personal Information (a "Restricted Territory"), Company agrees to authorize such processing, and the parties will comply with the obligations in the SCCs. Company authorizes Comcast to enter into the SCCs and/or UK SCCs (where applicable) with such third party on Company's behalf. Schedules 1A and 1B set forth the Parties' statuses and obligations and the information required by the SCCs. The Parties also agree to the following with respect to such transfers:

   2.1 **The Parties' Roles.** With respect to the SCCs, to the extent that Company transfers European PI from a European Territory to a Comcast site located in a Restricted Territory, then Company is a data exporter and Company is a data importer. If Company transfers such European PI to Comcast from outside of a European Territory, then such transfer shall be an onward transfer. In either case, the Parties shall comply with the applicable module of the SCCs.

   2.2 **Applicable SCC Module.** Where Company is a Controller and Comcast a Processor, Module Two of the SCCs apply. Where Company is a Processor and Comcast is also a Processor, Module Three of the SCCs apply.

   2.3 **Applicable SCCs Provisions.** The following terms shall apply to the SCCs:

      2.3.1 **Clause 7:** The docking clause will not apply.

      2.3.2 **Clause 8.9:** Company may exercise its audit and inspection rights in accordance with Section 9 of the DPA.

      2.3.3 **Clause 9:** Option 2 shall apply, and such rights shall be exercised in accordance with Section 7 of the DPA.

      2.3.4 **Clause 11:** Such clause related to an independent dispute resolution body shall not be included.

      2.3.5 **Clause 17:** Option 1 shall apply, and the governing law shall be the Republic of Ireland.

      2.3.6 **Clause 18:** Disputes arising from the SCCs shall be resolved by the courts of the Republic of Ireland.

   2.4 **Applicable UK SCCs Provisions.** The following terms shall apply to the UK SCCs, as permitted by Clause 17 of the UK SCCs, and the Parties agree to change the format of the information set out in Part 1 of the addendum so that:

      2.4.1 The details of the Parties in Table 1 shall be as set out in Schedule 3A (with no requirement for signature).

      2.4.2 For the purposes of Table 2, the addendum shall be appended to the SCCs (including the selection of modules and disapplication of optional clauses as noted above), and paragraph 2.2.3 of this Schedule 3 selects the option and timescales for Clause 9.

      2.4.3 The appendix information listed in Table 3 is set out in Schedule 3A.

   2.5 To the extent required by Privacy Law, the technical and organization measures that Comcast implements that are designed to ensure the security of European PI are set forth in Schedule 1B.

   2.6 The term "member state" in the SCCs must not be interpreted in such a way as to exclude Data Subjects in Switzerland from the possibility of suing for their rights in their place of habitual residence (Switzerland) in accordance with Clause 18(c) of the SCCs. The references in the SCCs to the GDPR should be understood as references to the FADP insofar as the data transfers are subject to the FADP. The SCCs also protect the data of legal entities, in addition to natural persons, until the entry into force of the revised FADP (issued 25 September 2020).

   2.7 In the event that the Company gives its consent to Comcast transferring Company PI outside the Restricted Territory and a relevant European Commission decision or other valid adequacy method under applicable Privacy Laws on which the Company has relied in authorizing the transfer is held to be invalid, or that any supervisory authority requires transfers of Personal Information made pursuant to such decision to be suspended, then the Parties agree to discuss in good faith and facilitate the use of an alternative transfer mechanism.

Schedule 1A

The following chart includes the information required by Annex 1 of the SCCs.

Data Exporter	See Processing Activities Tables
Data Importer (or Party receiving an onward transfer as described in Section 2.1 of Schedule 1)	Name: Comcast Cable Communications Management, LLC Address: 1701 John F Kennedy Blvd., Philadelphia, PA 19103, United States Contact person's name, position, and contact details: Christin McMeley, Chief Privacy Officer, Comcast_Privacy@comcast.com Activities relevant to the data transferred under these Clauses: Processing of Company PI as necessary to provide the Services Role (controller/processor): Processor
Data Subjects	See Processing Activities Tables
Categories of Personal Information	See Processing Activities Tables
Special Category Personal Information (if applicable)	See Processing Activities Tables
Frequency of the Transfer	The transfer will occur on a continuous basis throughout the duration of the Agreement.
Nature of the Processing	The Personal Information transferred will be subject to the processing activities described in the Agreement.
Purposes of Data Transfer and Further Processing	Comcast's purposes of processing are to facilitate its provision of products or services to Company, which are explained in the Agreement.
Period for which the Company PI will be retained	Comcast will retain Company PI for up to 7 days.
Method of Processing	Comcast will process Personal Information by performing any operation or set of operations on the Personal Information such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, transferring, or otherwise making available, alignment or combination, blocking, erasure, or destruction.
Recipients of Personal Information transferred to the Data Importer	See list of Subprocessors in Processing Activities Tables
For Transfers to Subprocessors, Subject Matter, Nature and Duration of the Processing	Transfers to Subprocessors comprise the same categories of Data SPubjects and Personal Information, and duration as set out above. The Subprocessors provide services to Company in connection with the delivery of the Services.
Location of Processing	The United States, unless requested otherwise to be in the EU and Switzerland otherwise by Customer in the Order
Competent supervisory authority/ies in accordance with Clause 13	• For transfers from the European Economic Area, the Dutch Data Protection Authority (Autoriteit Persoonsgegevens), PO Box 93374, 2509 AJ DEN HAAG, Netherlands; • For transfers from the UK, the UK Information Commissioner's Office, Wycliffe House Water Lane, Wilmslow, Cheshire, SK9 5AF; • For transfers from Switzerland, the Swiss Federal Data Protection and Information Commissioner (FDPIC), Feldeggweg 1 CH – 3003

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 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 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