GLOBAL DATA PRIVACY AGREEMENT

Data Controller – Customer defined as such in the MSA
Data Processor – Octoze Technologies ("Octoze")

This Global Data Privacy Agreement ("**DPA**") supplements the license and service agreement for Octoze Services between Octoze Technologies ("**Processor**") and the entity identified below ("**Customer**" or "**Controller**"), effective as of the last signature date. It supplements and amends the terms of Octoze's Main Services Agreement or any existing agreement for Octoze's services and products ("**the MSA**"). Octoze's Global Privacy Statement presents the Octoze Privacy Principles which are enforced by this DPA. In case of a conflict between the MSA and this DPA regarding data processing and privacy responsibilities, this DPA prevails. Octoze and Customer are individually known as a "**Party**" and collectively referred to as "**Parties.**"

The Parties are entering into this DPA to ensure that the processing by Octoze of Customer Data, within the service product by Customer and/or on based on the Customer's instructions, is done in a manner compliant with Applicable Law and its requirements regarding the processing of Customer Data. The Customer Data will be handled by Octoze and permitted third parties during the term of the MSA and after its termination on the following terms and conditions. Any capitalized terms not defined herein shall have the meaning given to them in the MSA.

1. Glossary of Terms.

"Controller", **"Data Subject"**, **"Personal Data"**, **"Personal Data Breach"**, **"Processor"** and **"Processing"** (includes **"Processed"**) shall have the same meaning as defined in the Applicable Law, as mentioned below.

1.1 **"Applicable Law"** means any law that regulates the processing, privacy, or security of Customer Data and that is directly applicable to each Party to this DPA. A non-exhaustive list is attached as Schedule 1-A.

1.2 **"Designated Representative"** means Customer or Processor employees as specified in the MSA to whom all notices required in this DPA will be sent.

1.3 **"Restricted Transfer"** means any transfer of Customer Data to a Third Country (as defined in the Jurisdiction Specific Terms), an international organization, or across national borders that would be prohibited by Applicable Laws {or by the terms of data transfer agreements put in place to address the data transfer restrictions of Applicable Data Protection Laws} in the absence of a lawful transfer mechanism or other evidence of adequate data protection standards.

1.4 **"Subprocessor"** means Octoze's subcontractors or agents, appointed by or on behalf of Octoze in Octoze's role as Processor to process Customer Data on behalf of Customer in accordance with the MSA.

2. Octoze Products and Solutions.

Octoze Products and Services shall have the same meaning as the services or products which the Customer has agreed to obtain license to access and use from Octoze as mentioned in the applicable MSA and Quotes or SOW thereon.

3. Processing of Customer Data.

3.1 Octoze shall ensure that all persons authorized to process Customer Data {employees and Subprocessors}, are bound by confidentiality obligations. These individuals shall process Customer Data strictly in accordance with the Customer's instructions and Applicable Laws.

3.2 Octoze may access and use Customer Data only on a need-to-know basis and as expressly authorized by the Customer, solely to fulfill its obligations under the MSA, this DPA, and any applicable Quote or Statement of Work. Such access or use shall be limited to the minimum extent necessary.

3.3 Unless expressly permitted by the Customer, Octoze shall not:

3.3.1. Use, sell, rent, transfer, distribute, alter, or disclose Customer Data to any third party without prior written consent from the Customer, except as required by Applicable Law or the MSA;

3.3.2. Use Customer Data for its own commercial benefit, including advertising or marketing directed toward children, parents, guardians, or Customer employees;

3.3.3. Use Customer Data to create a Student Profile other than as required to provide the contracted Services;

3.3.4. Store Customer Data outside the designated data residency regions without prior written notice to the Customer Designated Representative, ensuring compliance with security standards and Applicable Law.

3.4. The Customer is the "Data Collector" or "School Official," and Octoze is the "Data Processor." The Customer ensures it has obtained consent from the Data Subject for:

3.4.1. Collecting and processing Personal Information;

3.4.2. Transferring or allowing access to Personal Information;

3.4.3. Processing Personal Data to fulfill obligations under the MSA.

3.5. The Customer represents and warrants that it has obtained all necessary consents and government authorizations required by Applicable Law for Octoze to process Customer Data. Octoze shall not be liable for the Customer's failure to obtain such consents or authorizations.

3.6. The Customer agrees to indemnify and hold Octoze and its Affiliates harmless from any claims, expenses, damages, or costs related to Data Subject consents and government authorizations. Octoze agrees not to edit or use Customer Data unless:

3.6.1. Integral to the Services or permitted by the MSA or this DPA;

3.6.2. Written consent is obtained from the Customer;

3.6.3. Necessary to maintain the integrity of Customer Data.

4. Security of Processing.

Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Data Subjects, Octoze shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk. For further information on technical and organizational measures, see Schedule 1-B (Physical, Administration, and Technological Safeguards). Octoze shall make available to the Customer information necessary to demonstrate compliance with its obligations regarding providing security and maintaining compliance with Octoze's security plan/program laid described in Schedule 1 – C.

5. Subprocessors

5.1. Customer authorizes Octoze to appoint Subprocessors in accordance with this clause 5 and the MSA.

5.2. Octoze will enter into written agreements ("**Subprocessor Agreement**") whereby Subprocessors agree to secure and protect Customer Data in a manner consistent with the terms of this DPA and the MSA, including applicable mechanism for cross-border transfer of data. Accordingly, the Subprocessors shall:

5.2.1. not disclose Customer Data, in whole or in part, to any third party, excluding vetted Subprocessor;

5.2.2. not use any Customer Data to advertise or market to students or their parents/guardians;

5.2.3. access, view, collect, generate and use Customer Data only as necessary to fulfill obligations under this DPA and the MSA;

5.2.4. Delete or return all Customer Data, in its possession, custody or control, upon conclusion or termination of the work, as directed by the Customer through Octoze.

5.2.5. implement industry standard reasonable physical, administrative, and technical safeguards to secure Customer Data from unauthorized disclosure, access and use.

5.2.6. ensure that its employees and subcontractors having access to Customer Data have been adequately vetted, trained, and possess the necessary qualifications to comply with the terms of this DPA; and

5.2.7. not re-identify or attempt to re-identify any De-identified Data or use De-identified Data in the possession of a third-party affiliate, thereby posing risks of re-identification.

5.3. Octoze will periodically conduct or review compliance monitoring and assessments of Subprocessors to determine their compliance with this DPA and MSA.

6. Data Subject Rights.

6.1. The Customer shall be primarily responsible for responding to Data Subject requests regarding Customer Data, under any Applicable Law. Octoze will reasonably cooperate and assist Customer in adapting Octoze's support of Customer regarding responding to Data Subject requests.

6.2. For Data Subject requests, Octoze shall:

6.2.1. promptly notify the Customer upon receipt of request from a Data Subject;

6.2.2. reasonably cooperate and assist Customer in connection with requests, inquiries, and complaints from Data Subjects to whom the data relates or from data protection authorities; and

6.2.3. not directly respond to the request except on documented instructions of the Customer.

7. Return and Disposition of Customer Data.

7.1. Upon written request from Customer and in accordance with Section 13.9 (Return or Disposition of Customer Data) of the MSA, Octoze will return or dispose or delete all Customer Data within a commercially reasonable time period when it is no longer needed for the purpose for which it was obtained. Octoze will not retain Customer Data beyond the necessary period for disposition and notify the Customer when all Customer Data has been returned/disposed/deleted.

7.2. Customer must inform Octoze when Customer Data is no longer needed. Octoze will not dispose of Customer Data unless, the Customer provides affirmative written confirmation that it does not need

to be transferred to a separate account.

7.3. Upon termination Octoze will, at Customer's request and expense, securely transfer all Customer Data to a designated vendor's platform on a mutually agreed date and format. Octoze will provide the data in an industry-standard format but is not obligated to comply with the succeeding vendor's specific format requirements.

7.4. Disposition includes the shredding of any hard copies of Customer Data, erasing or otherwise modifying the personal information to make it unreadable or indecipherable by human or digital means.

7.5. Customer acknowledges that from the third (3) data return requests during the term of the MSA, there may be a reasonable service fee attached.

7.6. Customer may request partial disposal of Customer Data that is no longer needed, during the terms of the MSA. Such Partial disposal is subject to the Customer's request to transfer data to a separate account.

7.7. Octoze agrees to assist Customer, at Customer's expense, to transfer any Customer Data so long as it is commercially reasonable to do so.

7.8. If transfer or partial disposal is not commercially reasonable, Octoze will inform the Customer of the costs, and the Customer may choose to pay. If not, Octoze is not obligated to transfer the data.

7.9. All transfers must comply with Applicable Law. Octoze is not liable for denying a transfer that does not comply with the law. Customer must indemnify Octoze for any transfer made at their request. Octoze may retain Customer Data if required by Applicable Law.

8. Response to Legal Orders, Demands or Requests for Data.

8.1. The terms herein will not be construed as prohibiting either Party hereto from disclosing information to the extent required by law, regulation, or court order, provided such Party notifies, where not prohibited, the other party promptly after becoming aware of such obligations and provides the other Party an opportunity to seek a protective order or otherwise to challenge or limit such required disclosure.

8.2. Octoze will not disclose (and will not instruct any of its employees or Subprocessors to disclose) in any manner whatsoever any Customer Data to any third party unless:

8.2.1. such disclosure is required in order for Octoze to perform its obligations pursuant to the MSA or this DPA and any applicable Quote or Statement of Work;

8.2.2. such disclosure is permitted under Applicable Law;

8.2.3. If Octoze becomes legally compelled to disclose Customer Data, Octoze will, to the extent permitted by law and if time permits, provide Customer with prompt written notice thereof prior to disclosure.

9. Compliance with Applicable Law.

The Parties acknowledge that Customer Data may include Personal Data that is subject to Applicable Law of the applicable jurisdiction. As such, Parties shall comply with all obligations under the Applicable Law that apply.

10. Termination.

Upon the termination or expiration of the applicable MSA, and subject to agreed data return or transfer or disposal, this DPA will automatically terminate without any further action of the Parties. The obligations of Octoze and Customer, as necessary, under this DPA shall survive termination or expiration of this DPA or MSA, until all Customer Data has been returned or disposed.

11. Cross-Border Transfer of Data.

Where a data subject's Personal Data originates within a country requiring an adequate level of protection when disclosing or transferring such Personal Data outside the originating country, Octoze shall not disclose or transfer the Personal Data outside the originating country without ensuring an appropriate cross-border mechanism is in place to support such disclosures or transfers as required by Applicable Laws. Such safeguards will become an integral part of this DPA.

For all Customer Data disclosed or transferred from the European Economic Area or any other jurisdiction recognizing the Standard Contractual Clauses as a valid mechanism to transfer Personal Data to a Non-Adequate Country, Module 2 of the Standard Contractual Clauses are deemed as completed, and shall be an integral part of this DPA, provided that Parties agree that transfers to Octoze in the applicable processing jurisdiction from the EU/EEA shall be valid as Octoze participates in the Data Privacy Framework program.

12. General Terms.

12.1. The Parties to this DPA hereby submit to the choice of jurisdiction stipulated in the MSA with respect to any disputes or claims arising under this DPA. The terms of this DPA do not reduce Octoze's obligations under the MSA regarding the protection of Customer Data and does not permit Octoze to Process Customer Data in ways prohibited by the MSA.

12.2. In the event that there is a conflict or inconsistencies between this DPA, Applicable Law, and the Standard Contract Clauses regarding cross-board transfer issues, the conflict or inconsistencies shall be resolved in the following order: (i) first, Applicable Law, (ii) second, the applicable Standard Contract Clauses, and (iii) then the DPA.

12.3. In the event that there is a conflict or inconsistencies between the MSA and this DPA concerning data processing and Parties' responsibilities, this DPA controls.

SCHEDULE 1 – A

NON-EXHAUSTIVE LIST OF APPLICABLE DATA PRIVACY LAWS *

Sr. No.	Country	Data Privacy Law applicable	Link to the Data Privacy law
1.	European Union (EU) and EEA	General Data Protection Regulation (GDPR)	General Data Protection Regulation (GDPR) – Legal Text (gdpr-info.eu)
2.	United States	Family Educational Rights and Privacy Act (FERPA) and other applicable state laws	FERPA | Protecting Student Privacy (ed.gov)
3.	Canada	Personal Information Protection and Electronic Documents Act (PIPEDA)	The Personal Information Protection and Electronic Documents Act (PIPEDA) - Office of the Privacy Commissioner of Canada
4.	India	Digital Personal Data Protection Act, 2023	Digital Personal Data Protection Act 2023 | Ministry of Electronics and Information Technology, Government of India (meity.gov.in)
5.	Argentina	Personal Data Protection Law No. 25,326; Regulatory Decree No. 1558/2001; Access to Public Law No. 27,275	Personal Data Protection Law – Law 25,326 - 2000; and Protection of Personal Data Decree 1558/2001
6.	Australia	Privacy Act, 1988	The Privacy Act | OAIC
7.	Bermuda	Personal Information Protection Act, 2016	Personal Information Protection Act 2016
8.	Brazil	General Data Protection Law (LGPD)	Brazilian General Data Protection Law (LGPD, English translation) (iapp.org)
9.	China	Personal Information Protection Law (PIPL)	Personal Information Protection Law of the People's Republic of China (cdurl.cn)
10.	Egypt	Personal Data Protection Law No. 151 of 2020	Data-Protection-Law-Translation-dualtext.pdf (sharkawylaw.com)
11.	Hong Kong	Personal Data (Privacy) Ordinance (PDPO)	The Personal Data (Privacy) Ordinance
12.	Israel	Protection of Privacy Law, 5741-1981	Protection of Privacy Law, 5741-1981 - unofficial translation.doc (www.gov.il)
13.	Jamaica	Data Protection Act of 2020	7_2020 The Data Protection Act
14.	Japan	Act on the Protection of Personal Information (APPI)	Act on the Protection of Personal Information - English - Japanese Law Translation
15.	Malaysia	Personal Data Protection Act 2010	Malaysia Federal Legislation (agc.gov.my)
16.	Mexico	Federal Law on the Protection of Personal Data held by Private Parties (FDPL); Constitution of the United Mexican States, Privacy Notice Guidelines, Federal Consumer Protection Law	Ley Federal de Protección de Datos Personales en Posesión de los Particulares (Federal Law on the Protection of Personal Data held by Private Parties (FDPL))
17.	Morocco	Law No. 09-08, Decree no. 1-09-15; Consumer protection Law no. 31-08; Article 24 of the 2011 Constitution	Law No. 09-08 – relative à la protection des personnes physiques a l'éregard du traitement des données à caractère personnel
18.	New Zealand	Privacy Act 2020	Privacy Act 2020 No 31 (as at 01 July 2024), Public Act Contents – New Zealand Legislation
19.	Philippines	Data Privacy Act of 2012	Republic Act 10173 - Data Privacy Act of 2012 - National Privacy Commission
20.	Qatar	Law No. 13 Concerning Personal Data Privacy protection Law ("PDPPL")	Law No. 13 Concerning Personal Data Privacy protection Law ("PDPPL") 2016

Sr. No.	Country	Data Privacy Law applicable	Link to the Data Privacy law
21.	Saudi Arabia	Personal Data Protection Law (PDPL)	Personal Data English V2-23April2023-Reviewed-.docx (sdaia.gov.sa)
22.	Singapore	Personal Data Protection Act 2012 (PDPA)	Personal Data Protection Act 2012 - Singapore Statutes Online (agc.gov.sg)
23.	South Africa	Protection of Personal Information Act (POPIA)	Protection of Personal Information Act 4 of 2013 | South African Government (www.gov.za)
24.	South Korea	Personal Information Protection Act (PIPA)	PIPC, Korea
25.	Taiwan	Personal Data Protection Act	National Development Council -Content
26.	Thailand	Personal Data Protection Act (PDPA)	thailand-personal-data-protection-act-2019-en.pdf (thainetizen.org)
27.	Tunisia	Personal Data Protection Act (PDPA)	Organic Act No. 2004-63 of 27 July 2004
28.	Turkey	Law on the Protection of Personal Data No. 6698	K■■■SEL VER■LER■ KORUMA KURUMU | KVKK | Personal Data Protection Law
29.	United Arab Emirates	Federal Decree-Law No. 45 of 2021 on the Protection of Personal Data	uaelegislation.gov.ae/en/legislations/1972/download
30.	United Kingdom	Data Protection Act 2018	Data Protection Act 2018 - GOV.UK (www.gov.uk)
31.	Uruguay	Law No. 18.331 – 2008 - Protection of Personal Data and Habeas Data Action () (Regulating Decree Nº 414/009)	Ley de Protección de Datos Personals y Actión de Habeas Data

* Disclaimer. This list of privacy laws is not exhaustive. Applicable Laws include additional privacy laws directly applicable to each party to this DPA. Octoze does not represent that the links and context provided herein are the latest versions of the listed privacy laws.

SCHEDULE 1 – B

PHYSICAL, ADMINISTRATIVE, AND TECHNOLOGICAL SAFEGUARDS

A.1 Data Security. Octoze agrees to abide by and maintain adequate data security measures, consistent with industry standards for digital storage of Customer Data, to protect Customer Data from unauthorized disclosure or acquisition by an unauthorized person. The general security obligations of Octoze are set forth below. These security measures will include, but are not limited to:

A.1.1 Passwords and Employee Access. Octoze will secure usernames, passwords, and any other means of gaining access to the Services or to Customer Data, at a level meeting or exceeding the applicable standards. Octoze will only provide access to Customer Data to employees or contractors who require access pursuant to the MSA and this DPA, and only on terms consistent with or exceeding the data security measures required by this DPA between the Parties.

A.1.2 Security Protocols. The Parties agree to maintain security protocols that meet industry standards in the transfer or transmission of any data, including ensuring that data may only be viewed or accessed by parties legally allowed to do so. Octoze will maintain all data obtained or generated pursuant to the MSA in a secure digital environment.

A.1.3 Employee Training. Octoze will provide periodic security training to those employees who operate or have access to the system. Further, Octoze will provide Customer with contact information of an employee whom Customer may contact if there are any security concerns or questions.

A.1.4 Security Technology. Octoze will employ industry standard measures to protect data from unauthorized access. The service security measures will include server authentication and data encryption. Octoze will host data pursuant to the MSA in an environment using industry standard security controls are updated according to industry standards.

A.1.5 Monitoring. Octoze will log and analyze events across critical systems to identify potential threats to confidentiality, integrity, and availability of Customer Data.

A.1.6 Security Coordinator. Octoze will provide the name and contact information of Octoze's security coordinator for the Customer Data received pursuant to the MSA and this DPA upon written request.

A.1.7 Vendor-Data Subprocessors Bound. Octoze will enter into written agreements whereby Vendor-Data Subprocessors agree to secure and protect Customer Data in a manner consistent with the terms of this exhibit and the DPA. Octoze will periodically conduct or review compliance monitoring and assessments of Vendor-Data Subprocessors to determine their compliance with this exhibit and DPA.

A.1.8 Periodic Risk Assessment. Octoze acknowledges and agrees to conduct digital and physical periodic risk assessments at least annually and take commercially reasonable industry standard steps to remediate identified security and privacy vulnerabilities in a timely manner. Octoze shall provide reasonable assistance related to the nature of Processing to Customer in the event that a data protection impact assessment be required by Applicable Law.

A.1.9 Established Security Policies. Octoze will follow its established access security policies to support the confidentiality, integrity, and availability of the Customer Data against risks including but not limited to unauthorized access, collection, use, disclosure or disposal, loss, or modification. Such security arrangements will include, without limitation, reasonable physical, administrative, and

technical safeguards.

A.1.10 Audits and Compliance Reports. Octoze's security compliance is assessed by independent third-party auditors. Upon Customer agreeing to an NOA, Octoze shall provide access to information regarding Octoze's ISO 27001:2022 certification and SOC II Reports. To the extent that Octoze discontinues a third-party audit, Octoze will adopt or maintain an equivalent industry-recognized security standard.

B.1 Personal Data Breach. Customer agrees to notify Octoze immediately of any unauthorized use of Customer's accounts or any other breach of security.

B.1.1. Upon Octoze's becoming aware of a Personal Data Breach of Customer Data, Octoze shall immediately investigate the Personal Data Breach. Octoze shall:

B.1.1.1 take steps to mitigate and remediate the Personal Data Breach;

B.1.1.2 notify the Customer without undue delay, and within the time period required by Applicable Law.

B.1.1.3 provide the Customer with sufficient information to determine any notification under Applicable Law.

Cooperate with Customer and take commercially reasonable steps to assist in an investigation of the Data Breach.

B.2 Data Incident. In the event Customer Data is accessed or obtained by an unauthorized individual or third party, Octoze will:

B.2.1 provide notification to Customer within a reasonable amount of time of confirmation of the Incident, not exceeding seventy-two (72) hours.

B.2.2 comply with all reasonable requests from Customer in relation to such Incident and, in consultation with Customer and subject to any directions from Customer, take all reasonable steps to mitigate any harmful effect resulting from any such unauthorized access to, use or disclosure of Customer Data.

B.3 Post Incident Process. In the event of an Incident, Octoze will follow the following process:

B.3.1 Provide a security incident notification written in plain language after confirmation of the incident.

B.3.2 The security incident notification will include, at a minimum, the following information:

B.3.2.1 The name and contact information of Customer's Designee or his/her designee for this purpose.

B.3.2.2 A list of the types of Customer Data that were or are reasonably believed to have been the subject of an incident.

B.3.2.3 If the information is possible to determine at the time the notice is provided, then either (1) the date of the incident, (2) the estimated date of the incident, or (3) the date range within which the incident occurred. The notification will also include the date of the notice.

B.3.2.4 Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine and permitted at the time the notice is provided.

B.3.2.5 A general description of the incident, if that information is possible to determine at the time the notice is provided.

B.3.3 Octoze agrees to adhere to all requirements in applicable state, provincial and federal law with respect to an Incident related to Customer Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation, where commercially reasonable, of any such data breach.

B.3.4 Octoze maintains a written incident response plan that is consistent with industry standards and the applicable federal (country), state, or provincial law for responding to a data incident, security incident, privacy incident, or unauthorized acquisition or use of the Customer Data or any portion thereof, including personally identifiable information.

B.3.5 If Customer requests Octoze's assistance providing notice of unauthorized access, and such assistance does not take on a form unduly burdensome to Octoze, Octoze will reasonably cooperate and assist in, any investigation of a complaint that any Customer Data has been collected, used or disclosed contrary to Privacy Laws, or the policies of Customer, whether such investigation is conducted by Customer itself or a body having the legal authority to conduct the investigation, including but not limited to co-operation and assistance in notifying the affected Data Subject(s) of the unauthorized access.

SCHEDULE 1-C

OCTOZE DATA SECURITY AND PRIVACY PLAN

Additional elements of Octoze's Data Security and Privacy Plan are as follows:

(a) In order to comply with all Applicable Laws as related to data security and privacy requirements, Octoze follows its Data Security and Privacy Plan ("DSPP") and will: Review its data security and global privacy statement and practices to ensure that they are in conformance with all applicable federal, state, and local laws and the terms of this DSPP. In the event Octoze's policy and practices are not in conformance, Octoze will implement commercially reasonable efforts to ensure such compliance.

(b) As required by the ISO 27001:2022, in order to protect the security, confidentiality and integrity of the Protected Data that it receives under the Agreement, Octoze will have the following reasonable administrative, technical, operational and physical safeguards and practices in place throughout the term of the Agreement:

Data Security:

• Data-at-rest & data-in-transit (motion) are encrypted.

• Data leak protections are implemented Information Protection Processes and Procedures. Data destruction is performed according to contract and agreements.

• A plan for vulnerability management is developed and implemented with protective technology.

• Log/audit records are ascertained, implemented, documented, and reviewed according to policy. Network communications are protected.

Identity Management, Authentication and Access Control:

• Credentials and identities are issued, verified, managed, audited, and revoked, as applicable, for authorized devices, processes, and users.

• Remote access is managed. Octoze also conforms to the ISO 27001:2022 standard.

(c) For any of its employees (or employees of any of its subcontractors or assignees) who have access to Protected Data, Octoze has provided or will provide training on the federal and state laws governing confidentiality of such data prior to their receiving access, as follows: Annually, Octoze will require that all of its employees (or employees of any of its subcontractors or assignees) undergo data security and privacy training to ensure that these individuals are aware of and familiar with all applicable data security and privacy laws.

(d) In the event that Octoze engages any subcontractors, assignees, or other authorized agents to perform its obligations under the Agreement, it will require such subcontractors, assignees, or other authorized agents to execute written agreements requiring those parties to protect the confidentiality and security of Protected Data under applicable privacy laws.

(e) Octoze will manage data security and privacy incidents that implicate Protected Data, including identifying breaches and unauthorized disclosures, and Octoze will provide prompt notification of any breaches or unauthorized disclosures of Protected Data. More information on how incidents are handled can be found in the Main Service Agreement ("MSA").