Vendor Questionnaire (Data Privacy Agreement): 290607

Created Date: 5/20/2022 9:09 AM Last Updated: 6/13/2022 1:09 PM

Directions

Below is the Third Party contact that will fill out the Part 121//DPA questionnaire. If this is accurate, click the blue "Publish" button. If not, select the appropriate contact by clicking "Lookup" or create a new contact by clicking "Add New".

Vendor Compliance Contacts

Name (Full)	Email	Phone	Third Party Profile
Ryan Samari	ryan.samari@yuja.com		YuJa Inc.
Isaac Kingsmith	isaac.smith@yuja.com		YuJa Inc.
Nathan Arora	Nathan.Arora@yuja.com		YuJa Inc.

General Information

Third Party Profile:	YuJa Inc.	**Overall Status:**	Approved
Questionnaire ID:	290607	**Progress Status:**	100%
Engagements:	YuJa Inc. (DREAM) 22-23	**Portal Status:**	Vendor Submission Received
Due Date:	6/4/2022	**Submit Date:**	6/13/2022
		History Log:	**View History Log**

Review

Reviewer:	CRB Archer Third Party: Risk Management Team	**Review Status:**	Approved
		Review Date:	6/13/2022
Reviewer Comments:			
Unlock Questions for Updates?:	Assessment questions are set to read-only by default as the assessment should be completed by a vendor through the vendor portal. Do you need to unlock the questionnaire to manually make an update to the submitted questions? This field should be reset to null after the update is made, prior to existing the record.		

Data Privacy Agreement and NYCRR Part 121

As used in this DPA, the following terms shall have the following meanings:

1. **Breach:** The unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in a manner not permitted by State and federal laws, rules and regulations, or in a manner which compromises its security or privacy, or by or to a person not authorized to acquire, access, use, or receive it, or a Breach of Contractor's security that leads to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Personally Identifiable Information.
2. **Commercial or Marketing Purpose:** means the sale, use or disclosure of Personally Identifiable Information for purposes of receiving remuneration, whether directly or indirectly; the sale, use or disclosure of Personally Identifiable Information for advertising purposes; or the sale, use or disclosure of Personally Identifiable Information to develop, improve or market products or services to students.
3. **Disclose**: To permit access to, or the release, transfer, or other communication of personally identifiable information by any means, including oral, written or electronic, whether intended or unintended.
4. **Education Record:** An education record as defined in the Family Educational Rights and Privacy Act and its implementing regulations, 20 U.S.C. 1232g and 34 C.F.R. Part 99, respectively.
5. **Educational Agency**: As defined in Education Law 2-d, a school district, board of cooperative educational services, school, charter school, or the New York State Education Department.
6. **Eligible Student:** A student who is eighteen years of age or older.
7. **Encrypt or Encryption:** As defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule at 45 CFR 164.304, means the use of an algorithmic process to transform Personally Identifiable Information into an unusable, unreadable, or indecipherable form in which there is a low probability of assigning meaning without use of a confidential process or key.
8. **NIST Cybersecurity Framework**: The U.S. Department of Commerce National Institute for Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity Version 1.1.
9. **Parent:** A parent, legal guardian or person in parental relation to the Student.
10. **Personally Identifiable Information (PII):** Means personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g , and Teacher or Principal APPR Data, as defined below.
11. **Release:** Shall have the same meaning as Disclose.
12. **School:** Any public elementary or secondary school including a charter school, universal pre-kindergarten program authorized pursuant to Education Law § 3602-e, an approved provider of preschool special education, any other publicly funded pre-kindergarten program, a school serving children in a special act school district as defined in Education Law § 4001, an approved private school for the education of students with disabilities, a State-supported school subject to the provisions of Article 85 of the Education Law, or a State-operated school subject to the provisions of Articles 87 or 88 of the Education Law.
13. **Student:** Any person attending or seeking to enroll in an Educational Agency.
14. **Student Data:** Personally identifiable information as defined in section 99.3 of Title 34 of the Code of Federal Regulations implementing the Family Educational Rights and Privacy Act, 20 U.S.C 1232g.
15. **Subcontractor:** Contractor's non-employee agents, consultants and/or subcontractors engaged in the provision of services pursuant to the Service Agreement.
16. **Teacher or Principal APPR Data**: Personally Identifiable Information from the records of an Educational Agency relating to the annual professional performance reviews of classroom teachers or principals that is confidential and not subject to release under the provisions of Education Law §§ 3012-c and 3012-d.

NYCRR - 121.3 (b)(1):	What is the exclusive purposes for which the student data or teacher or principal data will be used, as defined in the contract?	Facilitate the support and training related to the organization's use of video within their organization.
NYCRR - 121.3 (b)(2):	Will the organization use subcontractors? If so, how will the organization ensure that the subcontractors, or other authorized persons or entities to whom the third-party contractor will disclose the student data or teacher or principal data, if any, will abide by all applicable data protection and security requirements, including but not limited to those outlined in applicable State and Federal laws and regulations (e.g., FERPA; Education Law section 2-d, NIST Cybersecurity Framework)?	We only hire full-time staff with no use of contractors or outside temp agencies.
NYCRR - 121.3 (b)(3):	What is the duration of the contract including the contract's expected commencement and expiration date? If no contract applies, describe how to terminate the service. Describe what will happen to the student data or teacher or principal data upon expiration. (e.g., whether, when and in what format it will be returned to the educational agency, and/or whether, when and how the data will be securely destroyed and how all copies of the data that may have been provided to 3rd parties will be securely destroyed)	As part of our American Institute of CPAs (AICPA), SOC 2 audit, we have formalized processes for data repurposing and disposal. The Video Platform can provide an automatic video clean-up report based on pre-established rules that could include historical usage, creation date, threshold of usage, and more. Further, all data deletion is done within the guidelines recommended by Amazon AWS, specifically NIST 800-99 ("Guidelines for Media Sanitization").

NYCRR - 121.3 (b)(4):	How can a parent, student, eligible student, teacher or principal challenge the accuracy of the student data or teacher or principal data that is collected?	If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.
NYCRR - 121.3 (b)(5):	Describe where the student data or teacher or principal data will be stored, described in such a manner as to protect data security, and the security protections taken to ensure such data will be protected and data security and privacy risks mitigated.	We use world-class primary data centers hosted by Amazon Web Services (AWS). We currently use the Virginia and Oregon data center locations across multiple availability zones and multiple redundant sub-systems. We also place zones behind load-balancers to ensure redundancy and scalability. The AWS infrastructure is a highly stable, fault-tolerant and secure attested by the following certifications: Statement on Auditing Standards No. 70 (SAS 70) Type II audited, Service Organization Controls 1 (SOC 1) reported and published under both the Statement on Standards for Attestation Engagements 16 (SSAE 16), International Standard on Assurance Engagements 3402 (ISAE 3402) standards, Certified ISO/IEC 27001:2005 Information Technology, and a Level 1 service provider under the Payment Card Industry (PCI) Data Security Standard (DSS). All third parties, namely AWS, that operate or store client data have security and data attestations that are verified by our Chief Technology Officer annually. We do not use any third-parties for any purpose whose data governance is weaker that the SOC 2 attestation that we commit to our customers.
NYCRR - 121.3 (b)(6):	Please describe how and where encryption is leveraged to protect sensitive data at rest and while in motion. Please confirm that all encryption algorithms are FIPS 140-2 compliant.	YuJa utilizes the Open Web Application Security Project recommendations on key life cycle management, key recovery, key storage, and key agreement. Cryptographic keys are at least the Federal Information Processing Standards (FIPS) standard for generation. We employ 256-bit encryption for in-transit and at-rest data. Per our SOC 2 attestation, the SOC2-6.1.8 - Key Management control covers key management, including key rotation. A summary of these requirements include: 1) A custom key must be used to encrypt all applicable resources; 2) Keys must be rotated annually; 3) API key and secret must be rotated semi-annually and old key should be deactivated after a set period of 30 days. The storage of keys utilizes a SOC 2-compliant storage vault that uses a SOC 2-compliant procedure for ensuring that keys are protected, backed up, and safe from tampering. Further, within our application-level code, we use industry-standard cryptographic libraries that are validated by third-party organizations including FIPS.
NYCRR - 121.6 (a):	Please submit the organization’s data security and privacy plan that is accepted by the educational agency.	YuJa Inc - CONFIDENTIAL - HECVAT3 - March-01-2022.xlsx

NYCRR - 121.6 (a)(1):	Describe how the organization will implement all State, Federal, and local data security and privacy contract requirements over the life of the contract, consistent with the educational agency's data security and privacy policy.	YuJa Inc. makes extensive investments into auditing and security tools. These span internal investments, consulting relationships, as well as industry partnerships. Though not an exhaustive list, we have provided a summary in the table below. Internal Penetration and Security Testing Tools: Our Operations Team and Test Team use internally created and off-the-shelf products to internally test our systems. Third-Party, Independent Technology Auditor: YuJa Inc. contracts with an experienced Technical Auditor that is responsible for validating our software systems including security validation, penetration testing, secure configuration testing and more. These third-party security audits continuously, 24/7, 365 with full human-based audit scans performed monthly. Our selected auditor performs audits against WASC 2.0’s threats including the following attack vectors: 1) Application Misconfiguration, 2) Directory Indexing, 3) HTTP Response Smuggling, 4) Improper Input Handling, 5) Insufficient Transport Layer Protection, 6) OS Commanding, 7) Remote File Inclusion, 8) SQL Injection, 9) XML External Entities, 10) XQuery Injection, 11) Content Spoofing, 12) Fingerprinting, 13) HTTP Response Splitting, 14) Improper Output Handling, 15) Mail Command Injection, 16) Path Traversal, 17) Routing Detour, 18) SSL Injection, 19) Injection, 20) Cross-Site Scripting, 21) Format String Attack, 22) Improper File System Permissions, 23) Information Leakage, 24) Null Byte Injection, 25) Predictable Resource Location, 26) Server Misconfiguration, 27) URL Redirector Abuse, and 28) XPath Injection. Third-Party, Independent Governance Auditor: YuJa Inc. contracts with an experienced compliance auditing firm that holds designations as a Certified Public Accountant (“CPA”), Certified Information Systems Auditor (“CISA”), Certified Information Systems Manager (“CISM”), or Certified Internal Auditor (“CIA”). These audits are performed annually with quarterly checkpoints to perform testing of the compliance controls that are in place. Dedicated Security Testing Processes: Our Test Team performs specific tests that are similar in nature to those outlined by the Open Web Application Security Project (OWASP), a 501(c)(3) worldwide not-for-profit organization focused on improving the security of software. Utilization of Third-Party Tools and Applications: Across our Product Development, Operations Teams, and Test Teams, we use a variety of third-party tools to access both security and compliance. These include dynamic and static code analysis tools, tools to identify server configuration vulnerabilities, as well as firewall and penetration testing tools. Continuous Improvement Processes: Our Continuous Update methodology ensures that fixes and improvements to our system are deployed promptly to ensure continued safety, compliance, and performance.

NYCRR - 121.6 (a)(2):	Specify the administrative, operational and technical safeguards and practices it has in place to protect personally identifiable information that it will receive under the engagement. If you use 3rd party assessments, please indicate what type of assessments are performed.	YuJa Inc. is audited by three separate organizations that are responsible for performing both deep technical and governance auditing. A summary of this is included below: • Technical Auditor – YuJa Inc. contracts with an experienced Technical Auditor that is responsible for validating our software systems including security validation, penetration testing, secure configuration testing, and more. Our third-party security audits 24/7, on a 365-day basis, with full human-based audit scans performed monthly. • Governance Auditor – YuJa Inc. contracts with an experienced compliance auditing firm that holds designations as a Certified Public Accountant ("CPA"), Certified Information Systems Auditor ("CISA"), Certified Information Systems Manager ("CISM") and Certified Internal Auditor ("CIA"). These audits are performed annually. • Accessibility Auditor – YuJa Inc. contracts with an external, third-party accessibility auditor to ensure compliance with WCAG 2.0 and WCAG 2.1 Level A and Level AA standards.
NYCRR - 121.6 (a)(4):	Specify how officers or employees of the organization and its assignees who have access to student data, or teacher or principal data receive or will receive training of the Federal and State laws governing confidentiality of such data prior to receiving access.	Our Chief Technology Officer and select full-time employees on the Operations Team have access facilities to the systems that can manage system data. Access approval is conditional on a number of factors including full-time employment, approval (based on need) by our Chief Technology Officer and compliance with our security protocols. Any request for specification information on names of individuals who have access must be completed via request from our Legal Counsel and Human Resources. Requests must document a reason for the law request, maintain confidentiality with the provided information, and comply with all Labor Laws and privacy restrictions that govern YuJa's disclosure of this information.
NYCRR - 121.6 (a)(5):	Specify if the organization will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected.	All third parties, namely AWS, that operate or store client data have security and data attestations that are verified by our Chief Technology Officer annually. We do not use any third-parties for any purpose whose data governance is weaker that the SOC 2 attestation that we commit to our customers.
NYCRR - 121.6 (a)(6):	Specify how the organization will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency.	The Disaster Recovery Plan does include a communication and response policy. As per our SOC2 auditor's recommendation, this escalation plan is documented within our Incident Response Policy document.
NYCRR - 121.6 (a)(7):	Describe whether, how and when data will be returned to the educational agency, transitioned to a successor contractor, at the educational agency's option and direction, deleted or destroyed by the third-party contractor when the contract is terminated or expires. Vendor will be required to complete a Data Destruction Affidavit upon termination of the engagement.	The Video Platform can provide an automatic video clean-up report based on pre-established rules that could include historical usage, creation date, threshold of usage, and more. All data deletion is done within the guidelines recommended by Amazon AWS, specifically NIST 800-99 ("Guidelines for Media Sanitization").
NYCRR - 121.9 (a)(1):	Is your organization compliant with the NIST Cyber Security Framework?	Yes

NYCRR - 121.9 (a)(2):	Describe how the organization will comply with the data security and privacy policy of the educational agency with whom it contracts; Education Law section 2-d; and this Part.	We utilize Amazon Web Services (AWS). AWS offers a highly secure data center that includes best-in-class infrastructure security, perimeter security, data security and environmental security. AWS is continuously innovating the design and systems of our data centers to protect them from man-made and natural risks. As a result, the most highly regulated organizations in the world trust AWS every day. AWS Service Organization Control Reports are independent third-party examination reports that demonstrate how AWS achieves key compliance controls and objectives. AWS is also ISO 27001 certified to provide security management that is specified to have comprehensive security controls. We use the Principal of Least Privilege to govern and approve access to data. Under the guidance and approval of the Chief Technology Officer of YuJa, the general principal that the Product Team uses is Principal of Least Privilege. That is, each employee only has access to the systems and data that are required for their job function. In terms of personnel who have access to user data, please use the following guideline: • Direct access to the servers, systems, data storage, databases, system process and mechanisms This is limited to a specific sub-set of our Operations Team that directly manages our server infrastructure. This level of access is required to manage and administer and backup our production systems on a regular basis. • Platform-level access to features and capabilities that can manage data To assist end-users and Administrators with questions, our Support and Customer Success Teams can remotely login to end-user accounts to assist. Our Operations Team uses multi-factor authentication to access our data center systems. Direct access to all production systems is governed by multi-factored authentication schemes which require both a username, password, and direct access to an MFA device for a secondary authentication code.
NYCRR - 121.9 (a)(3):	Describe how the organization will limit internal access to personally identifiable information to only those employees or sub-contractors that need authorized access to provide services.	Under the guidance and approval of the Chief Technology Officer of YuJa Inc., the general principal that the Product Team uses is Principal of Least Privilege. That is, each employee only has access to the systems and data that are required for their job function. In terms of personnel who have access to user data, we use the following guideline: • Direct access to the servers, systems, data storage, databases, system process and mechanisms. This is limited to a specific sub-set of our Operations Team that directly manages our server infrastructure. This level of access is required to manage and administer and backup our production systems on a regular basis. • Platform-level access to features and capabilities that can manage data. To assist end-users and Administrators with questions, our Support and Customer Success Teams can remotely login to end-user accounts to assist. • Our Operations Team Uses Multi-Factor Authentication to Access our Data Center Systems. Direct access to all production systems is governed by multi-factored authentication schemes which require both a username, password and direct access to a MFA device for a secondary authentication code.

NYCRR - 121.9 (a)(4):	Describe how the organization will control access to the protected data and not use the personally identifiable information for any purpose not explicitly authorized in its contract. (e.g. Role Based Access, Continuous System Log Monitoring/Auditing)	The Video Platform provides capabilities for Administrators and Sub-Administrators, as well as two additional non-administrator roles. These standard and customized roles can also be delegated with certain role-based functional limitations and scope limitations. The Video Platform's ability to create custom sub-administrator roles can be defined based on virtually any role scope and functional need. This enables organizations to implement Principle of Least Privilege best practices.
NYCRR - 121.9 (a)(5):	Describe how the organization will not disclose any personally identifiable information to any other party without the prior written consent of the parent or eligible student: (i)except for authorized representatives of the third-party contractor such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with State and Federal law, regulations and its contract with the educational agency; or (ii)unless required by statute or court order and the third-party contractor provides a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.	We do not share content with any third parties without permission. The only aspect that is shared with a third-party is our optional auto-captioning which uses a licensed and third-party hosted product to perform auto-captioning.
NYCRR - 121.9 (a)(6):	Describe how the organization will maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in its custody.	As part of the SOC2 auditing process, YuJa Inc. is also required to perform background checks on all personnel. We use a third-party firm to perform our background checks which include multi-jurisdiction criminal background verification. Under the guidance and approval of the Chief Technology Officer of YuJa Inc, the general principal that the Product Team uses is Principal of Least Privilege. That is, each employee only has access to the systems and data that are required for their job function. Our Operations Team uses multi-factor authentication to access our data center systems. Direct access to all production systems is governed by multi-factored authentication schemes which require both a username, password and direct access to a MFA device for a secondary authentication code.
NYCRR - 121.9 (a)(7):	Describe how the organization will use encryption to protect personally identifiable information in its custody while in motion or at rest.	We employ 256-bit encryption for in-transit and at-rest data. Additionally, the following rigorous procedures to our data transmission workflows: • Data Security – All sensitive user data is transmitted through an encrypted SSL channel which uses 256-bit encryption. • Data Center Security – We use Amazon Web Services (AWS) as our data center. • At- Rest Data Security – All sensitive user data is either transmitted or stored via encryption. • User Security – Access to YuJa systems that utilizes data store in our data centers is restricted to authorized and full-time YuJa employees. We do not use external contractors or temp agencies.
NYCRR - 121.9 (a)(8):	Affirmatively state that the organization shall not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or permit another party to do so.	Affirm
NYCRR - 121.9 (a)(b):	Describe how the organization will supervise its subcontractors to ensure that as subcontractors perform its contractual obligations, the subcontractor will conform with obligations imposed on the third-party contractor by State and Federal law to keep protected data secure.	YuJa does not utilize subcontractors for any aspect of its work. This allows us to maintain a more secure environment and directly supervise all employees.

NYCRR - 121.10 (a):	Describe how the organization shall promptly notify each educational agency with which it has a contract of any breach or unauthorized release of personally identifiable information in the most expedient way possible and without unreasonable delay but no more than seven calendar days after the discovery of such breach.	YuJa Inc. is a SOC 2-compliant organization with multiple processes in place to detect and act on potential security breaches including: • Implementation of Intrusion Detection System (IDS) – The IDS infrastructure will transparently send suspicious network traffic to a third-party global monitoring center for review and alerts. • Secure Network Inbound and Outbound Rules – We utilize AWS as our chosen data center provider with advanced system-hardening that includes well-defined inbound and outbound security rules. Any anomalies detected by these systems is reviewed by our Chief Technology Officer and reported accordingly both our Legal Counsel and Chief Business Officer. In the event of a documented incident, this is reported to customers, in writing, within 24 hours.
NYCRR - 121.10 (f):	Affirmatively state that where a breach or unauthorized release is attributed to the organization, the organization shall pay for or promptly reimburse the educational agency for the full cost of such notification.	Affirm
NYCRR - 121.10 (f.2):	Please identify the name of your insurance carrier and the amount of your policy coverage.	The Hartford Group - Workers Compensation: $1,000,000 - Professional Indemnity: $1,000,000 / $2,000,000 - Commercial General Liability - $1,000,000 / $2,000,000
NYCRR - 121.10 (c):	Affirmatively state that the organization will cooperate with educational agencies and law enforcement to protect the integrity of investigations into the breach or unauthorized release of personally identifiable information.	Affirm
Acceptable Use Policy Agreement:	Do you agree with the Capital Region BOCES Acceptable Use Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=BU4QYA6B81BF)	I Agree
Privacy Policy Agreement:	Do you agree with the Capital Region BOCES Privacy Policy? (Click here: http://go.boarddocs.com/ny/crboces/Board.nsf/goto?open&id=BWZSQ273BA12)	I Agree
Parent Bill of Rights:	Please upload a signed copy of the Capital Region BOCES Parent Bill of Rights. A copy of the Bill of Rights can be found here: https://www.capitalregionboces.org/wp-content/uploads/2021/03/CRB_Parents_Bill_Of_Rights_-Vendors.pdf	Completed CRB_Parents_Bill_Of_Rights_-Vendors.pdf
DPA Affirmation:	By submitting responses to this Data Privacy Agreement the Contractor agrees to be bound by the terms of this data privacy agreement.	I Agree

Attachments

Name	Size	Type	Upload Date	Downloads
No Records Found				

Comments

Question Name	Submitter	Date	Comment	Attachment
No Records Found				

Vendor Portal Details

Contact Name:	The Risk Mitigation & Compliance Office	**Publish Date:**	
Required Portal Fields Populated:	Yes	**Contact Email Address:**	crbcontractsoffice@neric.org
About NYCRR Part 121:	In order for a vendor to engage with a New York State Educational Agency, the vendor must provide information required by the New York State Commissioner's Regulations Part 121 (NYCRR Part 121) and the National Institute of Standards and Technology Cyber Security Framework. If deemed appropriate, the responses you provide will be used as part of the data privacy agreement between the vendor and the Albany-Schoharie-Schenectady-Saratoga BOCES. This Data Privacy Agreement ("DPA") is by and between the Albany-Schoharie-Schenectady-Saratoga BOCES ("EA"), an Educational Agency, and YuJa Inc. ("CONTRACTOR"), collectively, the "Parties". The Parties enter this DPA to address the requirements of New York law. Contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.	**Requesting Company:**	Capital Region BOCES
Created By:		**Third Party Name:**	YuJa Inc.
		Name:	YuJa Inc.-290607