NEW YORK STATE MODEL DATA PRIVACY AGREEMENT FOR EDUCATIONAL AGENCIES

Batavia City School District

260 State Street
Batavia, NY 14020

and

[Contractor - Propio LS, LLC **]**

This Data Privacy Agreement ("DPA") is by and between the Batavia City School District ("EA"), an Educational Agency, and [Propio LS, LLC] ("Contractor"), collectively, the "Parties".

ARTICLE I: DEFINITIONS

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.

ARTICLE II: PRIVACY AND SECURITY OF PII

1. **Compliance with Law.**

   In order for Contractor to provide certain services ("Services") to the EA pursuant to a contract dated [25/26 school year] ("Service Agreement"); Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR

Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. The contractor agrees to maintain the confidentiality and security of PII in accordance with applicable New York, federal and local laws, rules and regulations.

2. **Authorized Use.**
   Contractor has no property or licensing rights or claims of ownership to PII, and Contractor must not use PII for any purpose other than to provide the Services set forth in the Service Agreement. Neither the Services provided nor the manner in which such Services are provided shall violate New York law.

3. **Data Security and Privacy Plan**.
   Contractor shall adopt and maintain administrative, technical and physical safeguards, measures and controls to manage privacy and security risks and protect PII in a manner that complies with New York State, federal and local laws and regulations and the EA's policies. Education Law Section 2-d requires that Contractor provide the EA with a Data Privacy and Security Plan that outlines such safeguards, measures and controls including how the Contractor will implement all applicable state, federal and local data security and privacy requirements. Contractor's Data Security and Privacy Plan is attached to this DPA as Exhibit C.

4. **EA's Data Security and Privacy Policy**
   State law and regulation requires the EA to adopt a data security and privacy policy that complies with Part 121 of the Regulations of the Commissioner of Education and aligns with the NIST Cyber Security Framework. The contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. **Right of Review and Audit.**
   Upon request by the EA, the Contractor shall provide the EA with copies of its policies and related procedures that pertain to the protection of PII. It may be made available in a form that does not violate Contractor's own information security policies, confidentiality obligations, and applicable laws. In addition, Contractor may be required to undergo an audit of its privacy and security safeguards, measures and controls as it pertains to alignment with the requirements of New York State laws and regulations, the EA's policies applicable to Contractor, and alignment with the NIST Cybersecurity Framework performed by an independent third party at Contractor's expense, and provide the audit report to the EA. Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices as an alternative to undergoing an audit.

6. **Contractor's Employees and Subcontractors.**

(a) Contractor shall only disclose PII to Contractor's employees and subcontractors who need to know the PII in order to provide the Services and the disclosure of PII shall be limited to the extent necessary to provide such Services. The contractor shall ensure that all such employees and subcontractors comply with the terms of this DPA.

(b) Contractor must ensure that each subcontractor performing functions pursuant to the Service Agreement where the subcontractor will receive or have access to PII is contractually bound by a written agreement that includes confidentiality and data security obligations equivalent to, consistent with, and no less protective than, those found in this DPA.

(c) The contractor shall examine the data security and privacy measures of its subcontractors prior to utilizing the subcontractor. If at any point a subcontractor fails to materially comply with the requirements of this DPA, Contractor shall: notify the EA and remove such subcontractor's access to PII; and, as applicable, retrieve all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance with this DPA. In the event there is an incident in which the subcontractor compromises PII, Contractor shall follow the Data Breach reporting requirements set forth herein.

(d) The contractor shall take full responsibility for the acts and omissions of its employees and subcontractors.

(e) Contractor must not disclose PII to any other party unless such disclosure is required by statute, court order or subpoena, and the Contractor makes a reasonable effort to notify the EA of the court order or subpoena in advance of compliance but in any case, provides notice to the EA no later than the time the PII is disclosed, unless such disclosure to the EA is expressly prohibited by the statute, court order or subpoena.

7. **Training**.

Contactor shall ensure that all its employees and Subcontractors who have access to PII have received or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access.

8. **Termination**

The obligations of this DPA shall continue and shall not terminate for as long as the Contractor or its sub-contractors retain PII or retain access to PII.

9. **Data Return and Destruction of Data.**

(a) Protecting PII from unauthorized access and disclosure is of the utmost importance to the EA, and Contractor agrees that it is prohibited from retaining PII or continued access to PII or any copy, summary or extract of PII, on any storage medium (including, without limitation, in secure data centers and/or cloud-based facilities) whatsoever beyond the period of providing Services to the EA, unless such retention is either expressly authorized for a prescribed period by the Service Agreement or other written agreement between the Parties, or expressly requested by the EA for purposes of facilitating the transfer of PII to the EA or expressly required by law. As applicable, upon expiration or termination of the Service Agreement, Contractor shall transfer PII, in a format agreed to by the Parties to the EA.

(b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, Contractor agrees to return or destroy all PII when the purpose that necessitated its receipt by Contractor has been completed. Thereafter, with regard to all PII (including without limitation, all hard copies, archived copies, electronic versions, electronic imaging of hard copies) as well as any and all PII maintained on behalf of Contractor in a secure data center and/or cloud-based facilities that remain in the possession of Contractor or its Subcontractors, Contractor shall ensure that PII is securely deleted and/or destroyed in a manner that does not allow it to be retrieved or retrievable, read or reconstructed. Hard copy media must be shredded or destroyed such that PII cannot be read or otherwise reconstructed, and electronic media must be cleared, purged, or destroyed such that the PII cannot be retrieved. Only the destruction of paper PII, and not redaction, will satisfy the requirements for data destruction. Redaction is specifically excluded as a means of data destruction.

(c) Contractor shall provide the EA with a written certification of the secure deletion and/or destruction of PII held by the Contractor or Subcontractors.

(d) To the extent that Contractor and/or its subcontractors continue to be in possession of any de-identified data (i.e., data that has had all direct and indirect identifiers removed), they agree not to attempt to re-identify de-identified data and not to transfer de-identified data to any party.

10. **Commercial or Marketing Use Prohibition.**

The contractor agrees that it will not sell PII or use or disclose PII for a Commercial or Marketing Purpose.

11. **Encryption.**

The contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. The contractor must encrypt PII at rest and in transit in accordance with applicable New York laws and regulations.

12. **Breach**.

(a) Contractor shall promptly notify the EA of any Breach of PII without unreasonable delay no later than seven (7) business days after discovery of the Breach. Notifications required pursuant to this section must be in writing, given by personal delivery, e-mail transmission (if contact information is provided for the specific mode of delivery), or by registered or certified, and must to the extent available, include a description of the Breach which includes the date of the incident and the date of discovery; the types of PII affected and the number of records affected; a description of Contractor's investigation; and the contact information for representatives who can assist the EA. Notifications required by this section must be sent to the EA's District Superintendent or other head administrator with a copy to the Data Protection Office. Violations of the requirement to notify the EA shall be subject to a civil penalty pursuant to Education Law Section 2-d. The Breach of certain PII protected by Education Law Section 2-d may subject the Contractor to additional penalties.

(b) Notifications required under this paragraph must be provided to the EA at the following address:

[Name: Wendy Villone

Title: Director of Educational Technology, Data Protection Officer

Address: 80 Union Street

City, State, Zip: Batavia, NY 14020

Email: wvillone@bataviacsd.org]

13. **Cooperation with Investigations.**

The contractor agrees that it will cooperate with the EA and law enforcement, where necessary, in any investigations into a Breach. Any costs incidental to the required cooperation or participation of the Contractor or its' Authorized Users, as related to such investigations, will be the sole responsibility of the Contractor if such Breach is attributable to Contractor or its Subcontractors.

14. **Notification to Individuals.**
Where a Breach of PII occurs that is attributable to Contractor, Contractor shall pay for or promptly reimburse the EA for the full cost of the EA's notification to Parents, Eligible Students, teachers, and/or principals, in accordance with Education Law Section 2-d and 8 NYCRR Part 121.

15. **Termination**.
The confidentiality and data security obligations of the Contractor under this DPA shall survive any termination of this DPA but shall terminate upon Contractor's certifying that it has destroyed all PII.

ARTICLE III: PARENT AND ELIGIBLE STUDENT PROVISIONS

1. **Parent and Eligible Student Access**.
Education Law Section 2-d and FERPA provide Parents and Eligible Students the right to inspect and review their child's or the Eligible Student's Student Data stored or maintained by the EA. To the extent Student Data is held by Contractor pursuant to the Service Agreement, Contractor shall respond within thirty (30) calendar days to the EA's requests for access to Student Data so the EA can facilitate such review by a Parent or Eligible Student, and facilitate corrections, as necessary. If a Parent or Eligible Student contacts Contractor directly to review any of the Student Data held by Contractor pursuant to the Service Agreement, Contractor shall promptly notify the EA and refer the Parent or Eligible Student to the EA.

2. **Bill of Rights for Data Privacy and Security**.
As required by Education Law Section 2-d, the Parents Bill of Rights for Data Privacy and Security and the supplemental information for the Service Agreement are included as Exhibit A and Exhibit B, respectively, and incorporated into this DPA. The contractor shall complete and sign Exhibit B and append it to this DPA. Pursuant to Education Law Section 2-d, the EA is required to post the completed Exhibit B on its website.

ARTICLE IV: MISCELLANEOUS

1. **Priority of Agreements and Precedence.**
In the event of a conflict between and among the terms and conditions of this DPA, including all Exhibits attached hereto and incorporated herein and the Service Agreement, the terms and conditions of this DPA shall govern and prevail, shall survive the termination of the Service

Agreement in the manner set forth herein, and shall supersede all prior communications, representations, or agreements, oral or written, by the Parties relating thereto.

2. **Execution.**

   This DPA may be executed in one or more counterparts, all of which shall be considered one and the same document, as if all parties had executed a single original document, and may be executed utilizing an electronic signature and/ or electronic transmittal, and each signature thereto shall be and constitute an original signature, as if all parties had executed a single original document.

EDUCATIONAL AGENCY	**CONTRACTOR**
BY: Wendy Villone	BY: ***[Signature]*** Christopher Pesce
Wendy Villone	***[Printed Name]*** Christopher Pesce
Batavia City School District **Director of Educational Technology** **Data Protection Officer**	**[Title]** CFO
Date:	Date:10/13/2025

EXHIBIT A - Education Law §2-d Bill of Rights for Data Privacy and Security

Parents (including legal guardians or persons in parental relationships) and Eligible Students (students 18 years and older) can expect the following:

1. A student's personally identifiable information (PII) cannot be sold or released for any Commercial or Marketing purpose. PII, as defined by Education Law § 2-d and the Family Educational Rights and Privacy Act ("FERPA"), includes direct identifiers such as a student's name or identification number, parent's name, or address; and indirect identifiers such as a student's date of birth, which when linked to or combined with other information can be used to distinguish or trace a student's identity. Please see FERPA's regulations at 34 CFR 99.3 for a more complete definition.

2. The right to inspect and review the complete contents of the student's education record stored or maintained by an educational agency. This right may not apply to Parents of an Eligible Student.

3. State and federal laws such as Education Law § 2-d; the Commissioner of Education's Regulations at 8 NYCRR Part 121, FERPA at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); and the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); protect the confidentiality of a student's identifiable information.

4. Safeguards associated with industry standards and best practices including, but not limited to, encryption, firewalls and password protection must be in place when student PII is stored or transferred.

5. A complete list of all student data elements collected by NYSED is available at www.nysed.gov/data-privacy-security/student-data-inventory and by writing to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234.

6. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the EA at: [Batavia City School District]. (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacy-security/report-improper-disclosure, by mail to: Chief Privacy Officer, New York State Education Department, 89 Washington Avenue, Albany, NY 12234; by email to privacy@nysed.gov; or by telephone at 518-474-0937.

7. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.

8. Educational agency workers that handle PII will receive training on applicable state and federal laws, policies, and safeguards associated with industry standards and best practices that protect PII.

9. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

CONTRACTOR	
[Signature]	Christopher Pesce
[Printed Name]	Christopher Pesce
[Title]	CFO
Date:	10/13/2025

EXHIBIT B

BILL OF RIGHTS FOR DATA PRIVACY AND SECURITY -

SUPPLEMENTAL INFORMATION FOR CONTRACTS THAT UTILIZE PERSONALLY IDENTIFIABLE INFORMATION

Pursuant to Education Law § 2-d and Section 121.3 of the Commissioner's Regulations, the Educational Agency (EA) is required to post information to its website about its contracts with third-party contractors that will receive Personally Identifiable Information (PII).

Name of Contractor	Propio LS, LLC
Description of the purpose(s) for which Contractor will receive/access PII	**Propio Language Services receives and accesses Personally Identifiable Information (PII) solely for the purpose of delivering language interpretation and translation services to clients. PII, such as IP addresses, medical record numbers, dates, and URLs, may be processed as part of service delivery, quality assurance (e.g., reviewing call recordings), and to fulfill client-specific requirements such as intake questions for billing or service documentation. Access to PII is strictly limited to authorized personnel on a need-to-know basis, following the principle of least privilege. PII is only collected, stored, or transmitted as required to provide contracted services and is protected in accordance with applicable privacy laws and contractual obligations. Data is retained only as long as necessary for the intended service purpose and is securely disposed of after the retention period.** Interpretation & Translation Services
Type of PII that Contractor will receive/access	Check all that apply: ☑ Student PII ☐ APPR Data
Contract Term	Contract Start Date ____________________ Contract End Date ____________________
Subcontractor Written Agreement Requirement	A contractor will not utilize subcontractors without a written contract that requires the subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by state and federal laws and regulations, and the Contract. (check applicable option) ☐ Contractor will not utilize subcontractors. ☒ Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: • Securely transfer data to EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties. • Securely delete and destroy data.
Challenges to Data Accuracy	Parents, teachers or principals who seek to challenge the accuracy of PII will do so by contacting the EA. If a correction to data is deemed necessary, the EA will notify the Contractor. The contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.

Secure Storage and Data Security	Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply) ☒ Using a cloud or infrastructure owned and hosted by a third party. ☐ Using Contractor owned and hosted solution ☐ Other: Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data: Please see the following page.
Encryption	Data will be encrypted while in motion and at rest.

CONTRACTOR	
[Signature]	Christopher Pesce
[Printed Name]	Christopher Pesce
[Title]	CFO
Date:	10/13/2025

Propio mitigates data security and privacy risks through a comprehensive framework of technical, organizational, and administrative controls. All sensitive data, including PII and PHI, is encrypted at rest using AES-256 and in transit using TLS 1.2 or higher. Access to data is strictly role-based, requires manager approval, and is logged and audited for traceability. Multi-factor authentication is enforced for internal applications, and the principle of least privilege is applied to all user accounts, including offshore resources. Data is logically segregated by Client ID and Access ID, ensuring client data is not combined or accessible by unauthorized parties. Regular security training, phishing simulations, and incident response drills are conducted for all personnel. Data Loss Prevention (DLP) solutions, endpoint protection, and secure file sharing are implemented across all endpoints. Propio maintains compliance with HIPAA, GDPR, CCPA, and holds certifications such as SOC 2 Type 2 and HiTrust. Continuous monitoring, regular audits, and prompt application of security patches further reduce risk. Privacy impact assessments and risk assessments are performed regularly, and privacy policies are reviewed and updated to reflect regulatory changes. In the event of a breach, an incident response plan ensures rapid containment, investigation, and notification as required by law. These measures collectively ensure that data security and privacy risks are proactively managed without compromising the security or integrity of the data.

EXHIBIT C.1 – NIST CSF TABLE

The table below will aid the review of a Contractor's Data Privacy and Security Plan. Contractors should complete the Contractor Response sections in the table below to describe how their policies and practices align with each category in the Data Privacy and Security Plan template. To complete these 23 sections, a Contractor may: (i) Demonstrate alignment using the National Cybersecurity Review (NCSR) Maturity Scale of 1-7 ; (ii) Use a narrative to explain alignment (may reference its applicable policies); and/or (iii) Explain why a certain category may not apply to the transaction contemplated. Further informational references for each category can be found on the NIST website at https://www.nist.gov/cyberframework/new-framework. Please use additional pages if needed.

Function	Category	Contractor Response
IDENTIFY (ID)	**Asset Management (ID.AM):** The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the	Please see Soc 2 Type II Attestation Letter and HiTrust Report

Function	Category	Contractor Response
	processes to identify, assess and manage supply chain risks.	
PROTECT (PR)	**Identity Management, Authentication and Access Control (PR.AC):** Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Awareness and Training (PR.AT): The organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Data Security (PR.DS): Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected and the potential impact of events is understood.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Detection Processes (DE.DP): Detection processes and procedures are maintained	Please see Soc 2 Type II Attestation Letter and HiTrust Report

Function	Category	Contractor Response
	and tested to ensure awareness of anomalous events.	
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure response to detected cybersecurity incidents.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
RECOVER (RC)	**Recovery Planning (RC.RP):** Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.	Please see Soc 2 Type II Attestation Letter and HiTrust Report
	Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centers, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors).	Please see Soc 2 Type II Attestation Letter and HiTrust Report

HITRUST

6175 Main Street
Suite 400
Frisco, TX 75034

November 15, 2024

Propio LS, LLC
10801 Mastin Street
Suite 580
Overland Park, Kansas 66210-1843

Based upon representation from management as to the accuracy and completeness of information provided, the procedures performed by an Authorized External Assessor to validate such information, and HITRUST's independent confirmation that the work was performed in accordance with the HITRUST® Assurance Program requirements, the following platforms, facilities, and supporting infrastructure of the Organization ("Scope") meet the HITRUST CSF® v11.3.2 Essentials, 1-year (e1) certification criteria:

Platforms:

- Propio One residing at Amazon Web Services (AWS East 2)
- Workforce OS residing at Amazon Web Services (AWS East 2)

Facilities:

- Amazon Web Services (AWS) (Data Center) managed by Amazon Web Services located in Ohio, AWS East 2, United States of America
- Amazon Web Services (AWS) (Data Center) managed by Amazon Web Services located in Oregon, AWS West 2, United States of America

The certification is valid for a period of one year assuming the following occurs. If any of these criteria are not met, HITRUST will perform an investigation to determine ongoing validity of the certification and reserves the right to revoke the Organization's certification.

- No data security breach reportable to a federal or state agency by law or regulation has occurred within or affecting the assessed environment, and

- No significant changes in the business or security policies, practices, controls, and processes have occurred that might impact its ability to meet the HITRUST Essentials, 1-year (e1) certification criteria.

HITRUST has developed the HITRUST CSF, a certifiable framework that provides organizations with the needed structure, detail and clarity relating to information protection. With input from leading organizations, HITRUST identified a subset of the HITRUST CSF requirements that an organization must meet to be HITRUST Essentials, 1-year (e1) Certified.

HITRUST performed a quality assurance review to ensure that the control maturity scores were consistent with the results of testing performed by the Authorized External Assessor. Users of this letter can refer to the document Leveraging HITRUST Assessment Reports: A Guide for New Users for questions on interpreting this letter and can contact HITRUST customer support at support@hitrustalliance.net. Users of this letter are assumed to be familiar with and understand the services provided by the organization listed above, and what specific services are being used by the user organization.

A full HITRUST Validated Assessment Report has also been issued by HITRUST which can also be requested from the organization listed above directly. Additional information on the HITRUST Assurance Program can be found at the HITRUST website at https://hitrustalliance.net.

HITRUST

HITRUST

Enclosures (2):

- Assessment Context
- Scope of Systems in the Assessment

Assessment Context

HITRUST Essentials, 1-year assessments address the need for a continuously-relevant cybersecurity assessment focusing on foundational cybersecurity controls and mitigations for the most pressing cybersecurity threats. Organizations successfully achieving a e1 certification can reliably demonstrate they meet a bar of essential cybersecurity hygiene.

This assessment is designed for lower assurance scenarios (such as those needing greater assurances than achieved through information security questionnaires or readiness assessments but less so than those achieved through more robust, higher effort assessments). However, an e1 assessment can also serve as a starting point for enterprises that are in the early stages of implementing their information security controls.

To ensure foundational cybersecurity is in place, e1 assessments focuses on a pre-set selection of HITRUST CSF requirements curated by HITRUST. While not a compliance assessment, the subject matter does overlap with authoritative sources sharing similar goals (such as CISA Cyber Essentials, Health Industry Cybersecurity Practices (HICP) for Small Healthcare Organizations, NIST SP 800-171's "Basic" requirements, and NIST IR 7621: Small Business Information Security Fundamentals.

HITRUST's analysis of cyber threat intelligence data from leading threat intelligence providers when curating the controls considered during e1 assessments, e1 is an evolving, threat-adaptive assessment. HITRUST continually evaluates this data in relation to the controls included in the e1 to ensure that the e1 continues to address the most critical cyber threats (such as ransomware, phishing, brute force, and abuse of valid accounts).

Scope of the Assessment

Company Background

Propio LS, LLC (Propio) is a premier language solutions partner that provides a robust suite of language services—including video, phone, and on-site interpretation, as well as translation and localization for textbooks and educational materials, financial documents, healthcare documents, the entirety of a company's digital footprint—for a range of industries, including healthcare, education, legal, and financial. Additionally, Propio's portfolio also includes WorkforceOS which is an end-to-end resource management platform that can help increase healthcare access and improve healthcare equity. But at the heart of its service offering, Propio connects clients to its network of top-tier linguists who represent more than 300 languages from around the world. And the company now has more than 10,000 client partners, regionally and nationally.

Propio's vision is "to eliminate the everyday obstacles of communication using advanced technology." Propio offers its clients multiple ways to access its secure, multi-platform products and services—including its proprietary app, Propio ONE—and has achieved industry-leading remote connection times with clients and interpreters.

In-scope Platforms

The following tables describe the platforms that were included in the scope of this assessment.

Propio One	
Description	Propio One is an AWS cloud-based phone and video interpreting application which can be used on-demand to connect with a qualified interpreter in seconds. Customers subscribed to the platform connect via the web. Each client has unique login credentials through their respective Active Directory integration through Single sign-on (SSO).
Application(s)	Propio One
Database Type(s)	Microsoft SQL Server
Operating System(s)	Windows and Linux
Residing Facility	AWS
Exclusion(s) from Scope	None

Workforce OS	
Description	Workforce OS is an AWS cloud-based application used for scheduling interpretation calls. Customers subscribed to the platform connect via the web. Each client has unique login credentials through their respective Active Directory integration through Single sign-on (SSO)
Application(s)	Workforce OS
Database Type(s)	MySQL
Operating System(s)	Amazon Linux
Residing Facility	AWS
Exclusion(s) from Scope	None

In-scope Facilities

The following table presents the facilities that were included in the scope of this assessment.

Facility Name	Type of Facility	Third-party Managed?	Third-party Provider	City	State	Country
Amazon Web Services (AWS)	Data Center	Yes	Amazon Web Services	-	Ohio, AWS East 2	United States of America
Amazon Web Services (AWS)	Data Center	Yes	Amazon Web Services	-	Oregon, AWS West 2	United States of America

Services Outsourced

The following table presents outsourced services relevant to the scope of this assessment. The "Consideration in this Assessment" column of this table specifies the method utilized for each service provider relevant to the scope of this e1 assessment. Organizations undergoing e1 assessments have two options of how to address situations in which a HITRUST CSF requirement is fully or partially performed by a service provider (e.g., by a cloud service provider):

- The Inclusive method, whereby HITRUST CSF requirements performed by the service provider are included within the scope of the assessment and addressed through full or partial inheritance, reliance on third-party assurance reports, and/or direct testing by the external assessor, and

- The Exclusive (or Carve-out) method, whereby HITRUST CSF requirements performed by the service provider are excluded from the scope of the assessment and marked N/A with supporting commentary explaining that the HITRUST CSF requirement is fully performed by a party other than the assessed entity (for fully outsourced controls) or through commentary explaining the excluded partial performance of the HITRUST CSF requirement (for partially outsourced controls).

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Twilio	Twilio serves as the underlying communication platform for both applications, enabling voice and video communication. It acts as a middleware that facilitates the technical aspects of placing calls, connecting users, and ensuring the reliability of the communication. Inside both the Propio One and Workforce OS platform, once a client initiates the request to conduct a call, Twilio handles the backend communication to establish the call, enabling the applications to deliver on-demand, high-quality voice and video sessions. Propio's applications initiate calls or video sessions, while Twilio handles the technical aspects of connecting participants and ensuring call quality.	Included

Third-party Provider	Relevant Service(s) Provided	Consideration in this Assessment
Amazon Web Services	Amazon Web Services (AWS) is the Cloud hosting for the Propio One and Workforce OS platform. The applications have replicated hosting for redundancy in AWS US-East (OHIO) and AWS US-West (Oregon). Core infrastructure services include Elastic Compute Cloud (EC2) for scalable virtual computing capacity, Simple Storage Service (S3) for secure object storage and data retrieval, and Elastic Container Service (ECS) for fully managed container orchestration. For enhanced networking, Application Load Balancer ensures secure and efficient Layer 7 routing for HTTP traffic, while Global Accelerator improves application availability and performance. MemoryDB and DynamoDB offer fully managed database solutions, with the former being a Redis-compatible in-memory database and the latter a NoSQL database service. Lambda is also leveraged for serverless computing.	Included

Overview of the Security Organization

Information Security at Propio follows risk based approach for its Information Security Program. A risk committee has been chartered with the agenda of identifying information security risk, mitigation, resolution, transfer, and avoidance. Following NIST guidelines for best practices and ensuring compliance with HIPAA , the team of analysts, engineers, and Vice President (VP) work with various other Information Technology (IT) teams to develop and implements information security best practices.

After rigorous efforts, the team was able to achieve attestation for SOC 2 Type 1 in September 2024.

PRESCIENT
ASSURANCE

Prescient Assurance LLC
25 W 36th Street Floor 11
New York, NY 10018

August 4, 2025

Propio LS, LLC
10801 Mastin St. #580, Overland Park, KS 66210
Name of Signatory: Christopher Pesce
Phone and Email of Signatory: 913-381-3143, cpesce@propio.com

Letter of Attestation

SOC 2 Type 2 Compliance

Unqualified Opinion
In our opinion, in all material respects:

a) The description presents Propio LS, LLC's system that was designed and implemented throughout the period April 1, 2025 to June 30, 2025 in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period April 1, 2025 to June 30, 2025, to provide reasonable assurance that Propio LS, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Propio LS, LLC's controls during that period.

c) The controls stated in the description operated effectively throughout the period April 1, 2025 to June 30, 2025, to provide reasonable assurance that Propio LS, LLC's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Propio LS, LLC's controls operated effectively throughout the period.

Prescient Assurance LLC confirms SOC 2 Type 2 compliance by Propio LS, LLC in accordance with the AICPA's Trust Service Criteria for Security, Confidentiality and Availability.

Prescient Assurance

Prescient Assurance, LLC.

AICPA
SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
™