

DATA PRIVACY AGREEMENT
BRIGHTON CENTRAL SCHOOL DISTRICT

and

eDynamic Holdings, LP

This Data Privacy Agreement ("DPA") is by and between the Brighton Central School District ("EA"), an Educational Agency, and eDynamic Holdings, LP ("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 materially 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 March 5, 2024 ("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 20 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. 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. Contractor shall comply with the EA's data security and privacy policy and other applicable policies.

5. Right of Review and Audit.

Upon reasonable written request by the EA, 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, when reasonable, subject to reasonable written notice, and during the normal course of business hours, 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. 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) 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) Contractor shall take full responsibility for the acts and omissions of its employees and subcontractors insofar as such acts and omissions pertain to services performed under the Agreement between the Contractor and the District.
- (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.

Contractor 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, after receiving written notice from EA to

delete student PII, 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), 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, within ninety (90) days of receiving notice from the District, 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 delete 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.

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

11. Encryption.

Contractor shall use industry standard security measures including encryption protocols that comply with New York law and regulations to preserve and protect PII. 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: Eric Jordan

Title: Director of Technology Services

Address: 2035 Monroe Ave.

City, State, Zip: Rochester, NY 14618

Email: Eric_Jordan@bcasd.org

13. Cooperation with Investigations.

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. 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.

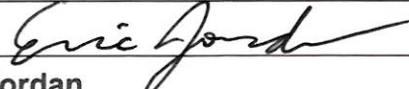
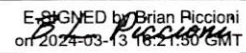
EDUCATIONAL AGENCY	CONTRACTOR
BY: 	BY: 
Eric Jordan	Brian Piccioni
Director of Technology Services	CFO
Date: 4/17/24	Date: March 13, 2024

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: Eric Jordan, 2035 Monroe Avenue, Rochester, NY 14618, Eric_Jordan@bcasd.org (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]	E-SIGNED by Brian Piccioni on 2024-03-13 16:21:52 GMT 
[Printed Name]	Brian Piccioni
[Title]	CFO
Date:	March 13, 2024

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	eDynamic Holdings LP
Description of the purpose(s) for which Contractor will receive/access PII	Access to the Knowledge Matters simulations
Type of PII that Contractor will receive/access	Check all that apply: <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
Contract Term	Contract Start Date 7/1/2024 Contract End Date 6/30/2025 This DPA shall apply to the contract term stated therein, and to any future service agreement between the parties.
Subcontractor Written Agreement Requirement	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) <input type="checkbox"/> Contractor will not utilize subcontractors. <input checked="" type="checkbox"/> Contractor will utilize subcontractors.
Data Transition and Secure Destruction	Upon expiration or termination of the Contract, Contractor shall: <ul style="list-style-type: none"> • 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 Contractor. Contractor agrees to facilitate such corrections within 21 days of receiving the EA's written request.
Secure Storage and Data Security	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p><input checked="" type="checkbox"/> Using a cloud or infrastructure owned and hosted by a third party.</p> <p><input type="checkbox"/> Using Contractor owned and hosted solution</p> <p><input type="checkbox"/> Other:</p> <p>Please describe how data security and privacy risks will be mitigated in a manner that does not compromise the security of the data:</p> <p>Please see attached information security plan.</p>
Encryption	Data will be encrypted while in motion and at rest.

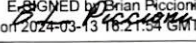
CONTRACTOR	
[Signature]	E-SIGNED by Brian Piccioni on 2024-03-13 16:21:54 GMT 
[Printed Name]	Brian Piccioni
[Title]	CFO
Date:	March 13, 2024

EXHIBIT C - CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN

The Educational Agency (EA) is required to ensure that all contracts with a third-party contractor include a Data Security and Privacy Plan, pursuant to Education Law § 2-d and Section 121.6 of the Commissioner's Regulations. For every contract, the Contractor must complete the following or provide a plan that materially addresses its requirements, including alignment with the NIST Cybersecurity Framework, which is the standard for educational agency data privacy and security policies in New York state. **While this plan is not required to be posted to the EA's website, contractors should nevertheless ensure that they do not include information that could compromise the security of their data and data systems.**

1	Outline how you will implement applicable data security and privacy contract requirements over the life of the Contract.	Over the life of the Contract, at eDynamic, we are committed to implementing applicable data security and privacy contract
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	<p>At eDynamic the protection of Personally Identifiable Information (PII) is of paramount importance to us. We have implemented a comprehensive set of administrative, operational, and technical safeguards and practices to ensure the utmost security and privacy of PII. Below is an overview of the safeguards and practices we have in place:</p> <p>1. Administrative Safeguards:</p> <ul style="list-style-type: none"> o Data Governance and Policies: We have established clear data governance frameworks and policies that outline the handling, processing, and storage of PII. These policies govern how employees and relevant stakeholders must interact with PII to maintain confidentiality and integrity. o Access Control and Authorization: Access to PII is strictly controlled through role-based access mechanisms. Employees are granted access to PII on a need-to-know basis, and permissions are regularly reviewed and updated. o Employee Training and Awareness: All employees undergo comprehensive

		<p>training on data security, privacy practices, and the importance of protecting PII. We regularly conduct awareness programs to keep our workforce informed about the latest security threats and best practices.</p> <p>o Incident Response and Management: We have a well-defined incident response plan in place to handle any potential security breaches or incidents involving PII. This plan includes predefined procedures for reporting, investigation, containment, and mitigation of such incidents.</p> <p>2. Operational Safeguards:</p> <p>o Data Minimization: We follow the principle of data minimization, ensuring that we only collect and retain the minimum amount of PII necessary to fulfill our contractual or legal obligations.</p> <p>o Data Retention Policies: PII is retained only for the required duration, as specified in our data retention policies. Once the retention period expires, we securely dispose of the data in accordance with best practices.</p> <p>o Secure Document Handling: PII in physical form is stored securely and access is restricted to authorized personnel only. We maintain secure storage facilities with restricted access to protect physical records.</p> <p>o Third-Party Risk Management: When third-party vendors are involved in processing PII, we conduct thorough assessments to ensure they meet the same high standards of data security and privacy protection.</p> <p>3. Technical Safeguards:</p> <p>o Data Encryption: PII is encrypted both in transit and at rest using</p>
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>industry-standard encryption algorithms. This ensures that even if unauthorized access occurs, the data remains unreadable and unusable.</p> <p>o Firewalls and Intrusion Detection Systems: We employ firewalls and intrusion detection systems to protect our network from unauthorized access and potential cyber threats.</p> <p>o Multi-Factor Authentication (MFA): To enhance the security of user accounts, we implement MFA, which requires multiple forms of authentication before granting access to sensitive data or systems.</p> <p>o Regular Security Updates and Patches: We proactively monitor and apply security updates and patches to our systems and software to prevent vulnerabilities that could be exploited.</p> <p>These administrative, operational, and technical safeguards and practices collectively form a robust and layered approach to protecting PII at eDynamic. We continuously evaluate and enhance our security measures to stay ahead of emerging threats and ensure the highest level of data security and privacy for our customers, partners, and employees.</p>
3	<p>Address the training received by your employees and any subcontractors engaged in the provision of services under the Contract on the federal and state laws that govern the confidentiality of PII.</p>	<p>We prioritize adherence to contractual requirements and data protection measures throughout our operations. To ensure that both our employees and subcontractors are bound by the requirements of the contract, we have established robust contracting processes. These processes are designed to create a legal framework that governs the relationship between all parties involved and reinforces our commitment to meeting contractual</p>

obligations. Below is an outline of our contracting processes:

Contract Review and Approval:
Before engaging in any business relationship with employees or subcontractors, we conduct a thorough review of the contract terms. Our legal and procurement teams carefully examine the agreements to ensure that they align with our company policies, applicable laws, and relevant data protection regulations.

Clear Definitions and Obligations:
Each contract explicitly outlines the roles and responsibilities of all parties involved. This includes specific references to the requirements that employees and subcontractors must adhere to during the course of the contract. Clear and unambiguous language is used to minimize any potential misunderstandings.

Incorporating Data Protection Requirements: Data protection and security are critical aspects of our contracting processes. We ensure that contracts with employees and subcontractors include clauses that mandate compliance with relevant data protection laws, confidentiality requirements, and any specific security measures outlined in the primary contract.

Mutual Non-Disclosure Agreements (NDAs): In cases where sensitive information or proprietary data is shared, we execute mutual non-disclosure agreements with employees

and subcontractors. These agreements legally bind all parties to maintain the confidentiality of the shared information.

Training and Awareness: Our onboarding process includes comprehensive training for employees and subcontractors, emphasizing their obligations under the contract. This training highlights the importance of data protection, security protocols, and the consequences of non-compliance.

Periodic Compliance Checks: Throughout the duration of the contract, we conduct regular compliance checks to ensure that all parties are adhering to the agreed-upon terms. These checks may involve audits, reviews, or assessments to validate compliance.

Contract Renewals and Amendments: As business needs evolve or regulatory requirements change, we regularly review our contracts to incorporate necessary updates. This ensures that the agreements remain relevant and enforceable, reflecting the current state of affairs.

Termination and Remediation: In the event of any non-compliance or breach of contract, we have predefined procedures for addressing the situation. Depending on the severity of the violation, corrective actions, remediation measures, or contract termination may be implemented.

		<p>Document Retention and Storage: All contractual documents are securely stored and retained according to our document retention policies. This practice facilitates quick access to relevant information during compliance checks or in the event of a dispute.</p> <p>By implementing these contracting processes, we aim to establish a strong foundation of trust and accountability with our employees and subcontractors. These practices not only ensure compliance with the contract's requirements but also uphold our commitment to maintaining the highest standards of data protection and professional conduct throughout our business relationships.</p>
4	<p>Outline contracting processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.</p>	<p>At eDynamic, we place great importance on ensuring that all parties involved in our contracts, including employees and subcontractors, are bound by written agreements that adhere to the requirements of the Contract, at a minimum. Our contracting processes are designed to create a legally binding framework that enforces compliance with contractual obligations and fosters a strong commitment to data security and privacy. Here is an outline of how we achieve this:</p> <p>1. Contract Review and Approval: Before engaging in any contractual relationship, our legal and procurement teams meticulously review and draft the contract to include all necessary requirements. This includes specific provisions that detail the obligations of employees and</p>

		<p>subcontractors in meeting the Contract's stipulations.</p> <p>2. Clear Definitions and Scope: The contract explicitly outlines the roles, responsibilities, and deliverables of all parties involved. By clearly defining the scope of work, each party understands its obligations, making it easier to ensure compliance.</p> <p>3. Incorporation of Data Security and Privacy Requirements: Data security and privacy are paramount in our contracting processes. We ensure that the contract includes clauses that mandate strict adherence to applicable data protection laws and confidentiality requirements.</p> <p>4. Confidentiality and Non-Disclosure Agreements: In cases where sensitive information or proprietary data is shared, we execute confidentiality and non-disclosure agreements with employees and subcontractors. These agreements legally bind all parties to maintain the confidentiality of shared information.</p> <p>5. Training and Awareness Programs: As part of the onboarding process, we conduct comprehensive training for employees. This training emphasizes their contractual obligations, including data security and privacy requirements.</p> <p>6. Oversight and Compliance Management: Throughout the contract's duration, we maintain oversight to ensure all parties are complying with the contract's provisions. Regular assessments and audits help identify areas for improvement and ensure continuous compliance.</p> <p>7. Monitoring and Incident Response: We implement monitoring tools to</p>
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>detect potential breaches or unauthorized access to data. In the event of any incidents, we have well-defined incident response procedures to address and mitigate the impact promptly.</p> <p>8. Vendor Management and Subcontractor Obligations: When subcontractors are involved, we ensure they sign agreements with data security and privacy requirements consistent with the primary contract. Regular evaluations of subcontractors' compliance are conducted.</p> <p>9. Documented Records and Retention: All contractual agreements, including confidentiality and non-disclosure agreements, are securely stored and retained as per our document retention policies. This ensures access to relevant information during compliance checks or disputes.</p> <p>10. Contract Renewals and Updates: As business needs evolve or regulations change, we regularly review and update the contract to incorporate necessary revisions. This ensures that the contract remains relevant and up-to-date with the latest data security and privacy requirements.</p> <p>By following these contracting processes, we aim to establish a robust legal framework that binds all parties involved to the requirements of the Contract. This approach ensures that our employees and subcontractors understand their obligations, fostering a culture of compliance and data protection throughout our engagements. The result is a strong commitment to data security and privacy that aligns with our dedication to responsible business practices.</p>
--	--	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

5	<p>Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents to the EA.</p>	<p>We take data security and privacy incidents very seriously, especially when they involve Personally Identifiable Information (PII). Our approach to managing such incidents is comprehensive and designed to ensure the protection of sensitive data and compliance with relevant regulations. Below, we outline our strategies for handling data security and privacy incidents that implicate PII, as well as our plans for identifying breaches and unauthorized disclosures and reporting incidents to the appropriate authorities, such as the EA</p> <p>Incident Response Team: We have a dedicated Incident Response Team composed of skilled professionals from various departments, including IT, legal, compliance, and management. This team is responsible for swiftly addressing and resolving any data security and privacy incidents.</p> <p>Incident Identification and Monitoring: We employ advanced monitoring and detection systems to identify potential breaches or unauthorized access to PII. These systems continuously analyze network activity, logs, and other data sources, allowing us to detect anomalies or suspicious activities promptly.</p> <p>Breach Notification Plan: In the event of a data breach that involves PII, we have a well-defined breach notification plan. This plan outlines the necessary steps to assess the scope and impact of the breach, contain it, and notify affected individuals and relevant</p>
---	-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>authorities within the required time frames.</p> <p>Communication Protocols: Effective communication is crucial during data security incidents. Our Incident Response Team maintains clear communication channels with all stakeholders, including customers, employees, partners, and regulatory bodies. Transparent and timely communication helps build trust and ensures that everyone is informed about the incident's status and measures being taken.</p> <p>Legal and Compliance Compliance: We work closely with legal and compliance experts to ensure that our incident response actions align with local and international data protection laws and regulations. This includes adhering to reporting requirements and providing the necessary documentation to the EA and other relevant authorities.</p> <p>Data Minimization and Encryption: To reduce the potential impact of a breach, we follow data minimization principles, only collecting and retaining essential PII. Additionally, sensitive data is encrypted both in transit and at rest to protect it from unauthorized access.</p> <p>Employee Training and Awareness: We invest in regular training and awareness programs to educate our employees about data security best practices and privacy policies. By fostering a culture of security</p>
--	--	----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>awareness, we empower our workforce to become the first line of defense against potential incidents.</p> <p>Regular Security Audits and Assessments: We conduct frequent security audits and risk assessments to identify vulnerabilities and proactively address potential weaknesses in our systems and processes. This allows us to stay ahead of emerging threats and continually improve our security measures.</p> <p>Continuous Improvement: Our incident response and data security policies are not static. We regularly review and update our procedures based on lessons learned from previous incidents and industry best practices.</p> <p>By implementing these strategies, we aim to maintain the highest level of data security and privacy protection, swiftly address any incidents that arise, and fulfill our obligations to report incidents to the EA and other relevant authorities as required. Safeguarding our customers' and stakeholders' data remains at the forefront of our commitment to responsible data management.</p>
6	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	At eDynamic, we understand the importance of responsible data management, including the secure transition of data to the EA when it is no longer needed to meet our contractual obligations. Our data transition process is carefully planned and executed to ensure the privacy and integrity of the data throughout the

transfer. Here is a description of how we handle the data transition:

1. Data Retention Policies: We establish data retention policies that specify the duration for which we will retain the data in accordance with contractual requirements and relevant legal obligations. Once the data is no longer needed to fulfill our contractual obligations, we initiate the data transition process.

2. Data Inventory and Categorization: Before transitioning the data, we conduct a thorough inventory and categorization of the information. This step helps us identify and segregate sensitive data, such as PII, proprietary information, or any other confidential data that requires special handling during the transition.

3. Secure Data Deletion: For data that is no longer required and does not need to be transferred to the EA, we employ secure data deletion methods, following industry best practices and standards. This process ensures that data is irreversibly removed from our systems and storage devices.

4. Data Anonymization or Aggregation: In some cases, the EA may require certain data for statistical analysis or reporting purposes without directly identifying individuals or organizations. In such instances, we anonymize or aggregate the data to protect individual privacy while still providing valuable insights.

5. Data Transfer Agreements: When transitioning data to the EA, we establish written agreements that outline the terms of the transfer, including the scope of data, data format, security requirements, and the purpose of the data's use by the EA.

		<p>These agreements ensure a clear understanding of the responsibilities and obligations of both parties during the transition.</p> <p>6. Data Security during Transfer: We employ secure data transfer methods to ensure the confidentiality and integrity of the data during the transition process. This prevents unauthorized access or interception of the data while it is in transit.</p> <p>7. Validation and Verification: Before completing the data transition, we validate and verify the accuracy and completeness of the transferred data. This step ensures that the EA receives the necessary information and that the data is in compliance with the agreed-upon format and specifications.</p> <p>8. Data Destruction Confirmation: For data that is deleted or no longer needed, we maintain records of the data destruction process and obtain confirmation to ensure that data has been securely removed.</p> <p>Our commitment to data security and privacy extends throughout the entire data lifecycle, including the data transition process. By following these procedures, we ensure that data is managed responsibly and ethically, meeting our contractual obligations while safeguarding the privacy and confidentiality of the information.</p>
7	Describe your secure destruction practices and how certification will be provided to the EA.	We utilize advanced and approved methods for secure data deletion. Our IT team oversees this process to ensure the thorough and effective removal of data.
8	Outline how your data security and privacy program/practices align with the EA's applicable policies.	At eDynamic , our data security and privacy program and practices are meticulously designed to align with the EA applicable policies. We recognize

		<p>the significance of adhering to the EA's specific requirements, and our commitment to data protection reflects our dedication to meeting those obligations. Below is an outline of how our data security and privacy program aligns with the EA's policies:</p> <p>1. Policy Review and Alignment:</p> <ul style="list-style-type: none">o We conduct thorough reviews of the EA's data security and privacy policies to understand their requirements fully.o Our internal policies and procedures are updated regularly to align with the latest EA guidelines and best practices. <p>2. Data Governance and Compliance:</p> <ul style="list-style-type: none">o Our data governance framework includes controls to ensure compliance with the EA's policies throughout the data lifecycle.o We have designated personnel responsible for monitoring and enforcing compliance with the EA's requirements. <p>3. Data Minimization and Purpose Limitation:</p> <ul style="list-style-type: none">o We strictly adhere to the principle of data minimization, collecting and retaining only the necessary data required for our engagements with the EA.o Data is processed solely for the purposes specified in the EA's policies and agreed-upon contracts. <p>4. Data Security Measures:</p> <ul style="list-style-type: none">o Our data security measures align with the EA's policies and include encryption, access controls, firewalls, and intrusion detection systems.
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<ul style="list-style-type: none">o We implement safeguards to protect against unauthorized access, data breaches, and other potential threats. <p>5. Data Sharing and Third-Party Management:</p> <ul style="list-style-type: none">o When sharing data with the EA or any third parties involved, we ensure compliance with the EA's policies and obtain any necessary permissions.o Third-party contracts include data protection clauses consistent with the EA's requirements. <p>6. Employee Training and Awareness:</p> <ul style="list-style-type: none">o Our employees receive comprehensive training on data security and privacy, including specific elements outlined in the EA's policies.o Regular awareness programs reinforce the importance of compliance with the EA's guidelines. <p>7. Incident Response and Reporting:</p> <ul style="list-style-type: none">o We have established incident response procedures that align with the EA's requirements, ensuring swift action in the event of a data security incident.o Timely and accurate incident reporting is conducted in accordance with the EA's guidelines. <p>8. Data Retention and Disposal:</p> <ul style="list-style-type: none">o Our data retention policies are designed to meet the EA's retention requirements, ensuring data is retained only for the necessary period. <p>9. Privacy Notices and Consent:</p> <ul style="list-style-type: none">o Privacy notices provided to individuals are aligned with the EA's requirements, outlining the purposes
--	--	------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

		<p>of data processing and individuals' rights.</p> <p>10. Continuous Improvement:</p> <ul style="list-style-type: none">o We regularly review our data security and privacy practices to identify areas for improvement and ensure ongoing alignment with the EA's policies.o Feedback from the EA is valued and considered to enhance our data protection efforts. <p>By closely aligning our data security and privacy program with the EA's applicable policies, we demonstrate our commitment to responsible data handling and compliance.</p>
--	--	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------