EDUCATION LAW 2-d RIDER

New York State Education Law 2-d was enacted in 2014 to address concerns relative to securing certain personally identifiable information. In order to comply with the requirements of Education Law 2-d, educational agencies and certain third-party contractors who contract with educational agencies must take certain additional steps to secure such data. These steps include enacting and complying with a Parents' "Bill of Rights" relative to protected data, ensuring that each third-party contractor has a detailed data privacy plan in place to ensure the security of such data, and that each third-party contractor sign a copy of the educational agency's Parents' Bill of Rights, thereby signifying that the third-party contractor will comply with such Parents' Bill of Rights. This Agreement is subject to the requirements of Education Law 2-d and Kahoot! AS (the "Contractor") is a covered third-party contractor.

In order to comply with the mandates of Education Law 2-d, and notwithstanding any provision of the Agreement between the LINDENHURST UNION FREE SCHOOL DISTRICT (the "District") and Contractor to the contrary, Contractor agrees as follows:

Contractor will treat "Protected Data" (as defined below) as confidential and shall protect the nature of the Protected Data by using the same degree of care, but not less than a reasonable degree of care, as the Contractor uses to protect its own confidential data, so as to prevent the unauthorized dissemination or publication of Protected Data to third parties. Contractor shall not disclose Protected Data other than to those of its employees or agents who have a need to know such Protected Data under this Agreement. Contractor shall not use Protected Data for any other purposes than those explicitly provided for in this Agreement. All Protected Data shall remain the property of the disclosing party. As more fully discussed below, Contractor shall have in place sufficient internal controls to ensure that the District's Protected Data is safeguarded in accordance with all applicable laws and regulations, including, but not limited to, the Children's Internet Protection Act ("CIPA"), the Family Educational Rights and Privacy Act ("FERPA"), and the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), and Part 121 of the Regulations of the Commissioner of Education, as it may be amended from time-to-time if applicable.

"**Protected Data**" includes any information rendered confidential by State or federal law, including, but not limited to student data, student demographics, scheduling, attendance, grades, health and discipline tracking, and all other data reasonably considered to be sensitive or confidential data by the District. Protected Data also includes any information protected under Education Law 2-d including, but not limited to:

> "Personally identifiable information" from student records of the District as that term is defined in § 99.3 of FERPA,
>
> -AND-
>
> Personally identifiable information from the records of the District 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.

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any Protected Data shall comply with New York State Education Law § 2-d. As applicable, Contractor agrees to comply with District policy(ies) on data security and privacy. Contractor shall promptly reimburse the District for the full cost of notifying a parent, eligible student, teacher, or principal of an unauthorized release of Protected Data by Contractor, its subcontractors, and/or assignees. In the event this Agreement expires, is not renewed or is terminated, Contractor shall return all of the District's data unless otherwise provided, including any and all Protected Data, in its possession by secure transmission.

Data Security and Privacy Plan

Contractor and/or any subcontractor, affiliate, or entity that may receive, collect, store, record or display any of the District's Protected Data, shall maintain a Data Security and Privacy Plan which includes the following elements:

1. Specifies the administrative, operational and technical safeguards and practices in place to protect personally identifiable information that Contractor will receive under the contract;

2. Demonstrates Contractor's compliance with the requirements of Section 121.3 of Part 121;

3. Specifies how officers or employees of the Contractor and its assignees who have access to student data, or teacher or principal data receive or will receive training on the federal and state laws governing confidentiality of such data prior to receiving access;

4. Specifies how Contractor will utilize sub-contractors and how it will manage those relationships and contracts to ensure personally identifiable information is protected;

5. Specifies how Contractor will manage data security and privacy incidents that implicate personally identifiable information including specifying any plans to identify breaches and unauthorized disclosures, and to promptly notify the educational agency;

6. Specifies whether Protected Data will be returned to the District, transitioned to a successor contractor, at the District's option and direction, deleted or destroyed by the Contractor when the contract is terminated or expires.

Initial Here: Pursuant to the Plan Contractor will:

1. Have adopted technologies, safeguards and practices that align with the NIST Cybersecurity Framework referred to in Part 121.5(a);
_____

2. Comply with the data security and privacy policy of the District; Education Law § 2-d; and Part 121;
_____

3. Have limited internal access to personally identifiable information to only those employees or sub-contractors that need access to provide the contracted services;
_____

Initial Here:

4. Have prohibited the use of personally identifiable information for any purpose not explicitly authorized in this contract; _____

5. Have prohibited the disclosure of personally identifiable information to any other party without the prior written consent of the parent or eligible student: _____

    a. except for authorized representatives such as a subcontractor or assignee to the extent they are carrying out the contract and in compliance with state and federal law, regulations and its contract with the educational agency; or

    b. unless required by statute or court order and Contractor has provided a notice of disclosure to the department, district board of education, or institution that provided the information no later than the time the information is disclosed, unless providing notice of disclosure is expressly prohibited by the statute or court order.

6. Maintain reasonable administrative, technical and physical safeguards to protect the security, confidentiality and integrity of personally identifiable information in our custody; _____

7. Use encryption to protect personally identifiable information in its custody while in motion or at rest; and _____

8. Not sell personally identifiable information nor use or disclose it for any marketing or commercial purpose or facilitate its use or disclosure by any other party for any marketing or commercial purpose or permit another party to do so. _____

In the event Contractor engages a subcontractor to perform its contractual obligations, the data protection obligations imposed on the third-party contractor by state and federal law and contract shall apply to the subcontractor.

Where a parent or eligible student requests a service or product from a third-party contractor and provides express consent to the use or disclosure of personally identifiable information by the third-party contractor for purposes of providing the requested product or service, such use by the third-party contractor shall not be deemed a marketing or commercial purpose prohibited by the Plan.

Contractor's signature below shall also constitute an acknowledgement, acceptance, and signature of the District's Parent Bill of Rights.

NAME OF PROVIDER: Kahoot! AS

DocuSigned by: Yngve Kirkeby C1F58AD6FC1E454...

SIGNED BY: Yngve Kirkeby **DATED:** 30/9/2025 | 07:28 CEST

TITLE: VP Enterprise Sales

DATA PRIVACY AND SECURITY PLAN

CONTRACTOR'S DATA PRIVACY AND SECURITY PLAN IS ATTACHED HERETO AND INCORPORATED HEREIN.

1.	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	Contractor has robust data security and controls in place to ensure data privacy and protection, including a data security policy. The measures implemented to protect personal data includes; continuous Pen-testing by external vendor, information encryption in motion and at rest, access controls, password protection and regular awareness and privacy training for employees. Access to personal data is provided on a need-to-know basis. Contractor holds SOC2 type 1 certification and ensure that its sub-processors are certified at ISO270001 and/or SOC 2 level or similar. Contractor has adopted NIST Framework or equivalent safeguards in accordance with industry standards for Improving Critical Infrastructure Security.
2.	Address the training received by your employees, officers and any subcontractors engaged in the provision of services under the laws that govern the confidentiality of PII.	Contractor is committed to ensure the reliability and security of employees and any other person acting under its supervision. Access to personal data is provided on a need-to-know basis and all employees are subject to duty of confidentiality. Mandatory security, awareness and privacy training is provided annually to employees, including training on information handling and sector-specific demands.
3.	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.	Contractor will ensure that its employees, with whom Contractor shares PII abide by all applicable data protection and security requirements by entering into written agreements whereby such parties will perform their obligations in a manner consistent with the data protection and security requirements subject to the confidentiality obligations outlined in the Kahoot! Employee Code of Conduct. therein. Contractor enters into written contracts with all our sub-processors/subcontractors imposing the same level of security and data protection obligations that are undertaken by Contractor. All sub-processors/subcontractors hold the highest level of security and have current certifications for ISO27001, SOC2 type 2, or similar. A list of our sub-processors are available online.
4.	Specify how you will manage any data security and privacy incidents that implicate PII and describe any specific	Contractor will promptly notify of any Breach or unauthorized release of PII in the most expedient way possible and without unreasonable delay but no more

	plans you have in place to identify breaches and/or unauthorized disclosures, and to meet your obligations to report incidents.	than 72 hours after the discovery of such Breach. Contractor will cooperate to protect the integrity of investigations into the Breach as provided in the DPA. In addition to its data processing records, privacy policy and security measures, Contractor operates a security incident response plan and train staff in detecting and handling a security breach – including notification to affected parties.
5.	Describe how data will be transitioned to the EA when no longer needed by you to meet your contractual obligations, if applicable.	Upon termination of the agreement, Contractor shall securely transfer data to the EA, or a successor contractor at the EA's option and written discretion, in a format agreed to by the parties.
6.	Describe your secure destruction practices and how certification will be provided to the EA.	Upon termination of the agreement, all personal data will be deleted and destroyed utilizing an approved method of confidential destruction. Thereafter, upon request, Contractor will provide EA with certification of such destruction.
7.	Outline how your data security and privacy program/practices align with the EA's applicable policies.	Contractor ensures that its data handling and security policies at any time complies with relevant data protection and privacy law. Contractor runs regular security audits, and maintain systems and policies in accordance with state-of-the-art and industry best standards. Contractor enters into written contracts with all our sub-processors imposing the same level of security and data protection obligations that are undertaken by Contractor. Contractor will implement the data protection and security requirements as a "Third-Party Contractor" as outlined in 8 NYCRR Part 121 and in accordance with the EA's Policy, as well as include EA's Parents Bill of Rights and Supplemental Information to the Service Agreement.