

Central Islip Union Free School District

Program Information and Data Privacy

Third Party Agreement



To be completed by the vendor and submitted for all NEW and RENEWAL software/programs prior to purchase/implementation. Refusal of the vendor complete this agreement may serve as cause for the district to see similar services through another program and/or vendor. Failure to complete this form in its entirety will significantly delay any/all program purchases.

Software/Program Title:	Kahoot!
Publisher:	Kahoot! ASA
Contract Pricing	<input checked="" type="checkbox"/> BOCES Contract or Shared Service <input type="checkbox"/> NYS Contract Pricing <input type="checkbox"/> Federal Contract Pricing <input type="checkbox"/> Direct Pricing, Bid or RFP with Vendor
Account Management	<input checked="" type="checkbox"/> SSO through LDAP/AD/ADFS/AZURE/SAML for plans of 100+ licenses <input checked="" type="checkbox"/> SSO through Clever <input type="checkbox"/> NO SSO Option <input type="checkbox"/> Non SSO Centrally Managed (all Users) <input type="checkbox"/> N/A - Non-User Based Program/Not Applicable
Platform	<input type="checkbox"/> Local Install OR Device APP <input type="checkbox"/> Local Server/Network <input checked="" type="checkbox"/> 100% Web-based <input type="checkbox"/> Web-Based with Local application/plug-in Other/Explain: Mobile applications available in Apple and Google Play stores, but not necessary
License Structure:	<input type="checkbox"/> Per-User <input type="checkbox"/> Per-Student <input type="checkbox"/> Per-Classroom <input checked="" type="checkbox"/> Per-Teacher <input type="checkbox"/> Per-Building <input type="checkbox"/> Districtwide/Unlimited <input type="checkbox"/> N/A - Not Applicable
License Renewal	<input type="checkbox"/> Perpetual (no-renewal) <input type="checkbox"/> Annual <input checked="" type="checkbox"/> N/A - Not Applicable
Separate Hosting Fees:	<input checked="" type="checkbox"/> NO or N/A <input type="checkbox"/> YES - Annually <input type="checkbox"/> Other/Explain:

Adobe Flash	<input checked="" type="checkbox"/> Program DOES NOT require Adobe Flash <input type="checkbox"/> Program REQUIRES Adobe Flash Programs that still require Adobe Flash will not be considered for purchase or utilized
Configuration, Deployment, Initial Roll-Out Support	<input type="checkbox"/> Full On-Site Support Included in the Proposal/Fee <input checked="" type="checkbox"/> Remote Support Only <input type="checkbox"/> Remote Support Included/On-Site for Additional Fees <input type="checkbox"/> N/A - Not Applicable
Staff Training/Professional Development	<input type="checkbox"/> Full On-Site Training/Development Included in the Proposal/Fee <input checked="" type="checkbox"/> Remote/WebEx Training/Development and Support Only <input type="checkbox"/> Combined On-Site/WebEx Training included in proposal <input type="checkbox"/> N/A - Not Applicable
SIS-PowerSchool Integrations	<input checked="" type="checkbox"/> Program DOES NOT sync to SIS (PowerSchool) <input type="checkbox"/> Program DOES sync to SIS (PowerSchool) <input type="checkbox"/> N/A - Not Applicable

ALL LINKS MUST BE PROVIDED AND COMPLETED BY THE VENDOR!

Software Title:	Kahoot!
Publisher/Developer:	Kahoot! ASA
Developer/Vendor Name	Kahoot! ASA
Developer/Vendor Mailing Address	Fridtjof Nansens plass 7, 0160 Oslo, Norway
Developer/Vendor Privacy Policy Link:	https://trust.kahoot.com/privacy-policy/ <input type="checkbox"/> N/A - Not Applicable – Not Available

Developer/Vendor Parent Bill of Rights Link	<p>We do not have our own Parent Bill of Rights to provide. We review customer-supplied Parent Bill of Rights as they come in, and review / sign these on an individual basis.</p> <p><input type="checkbox"/> N/A - Not Applicable – Not Available</p>
--	---

This Data Privacy Agreement ("DPA") is by and between the Central Islip Union Free School District (herein known as "EA"), an **Educational Agency**, and the above listed software, app or extension developer (herein known as "**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 prekindergarten 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 below ("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. 65016502 (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. Contractor is a Norwegian company and relies on external hosting providers located solely in Canada and Europe. A list of locations where Student Data is stored can be found at <https://trust.kahoot.com/hosting-providers/>. EA further acknowledges and agrees to the foregoing locations where Contractor stores Student Data outside of the United States.

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.

^{DS}
MR

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 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, subject to confidentiality obligations, after reasonable notice EA may request and Contractor may provide the EA with a recent industry standard independent audit report on Contractor's privacy and security practices.

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.

- (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 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 or in accordance with Contractor's data retention policy, 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 the EA's request, 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 upon request 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

Contractor Initials: 

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 the information is available at the time of providing notice of Breach, 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:

Philip K. Voigt
Director of Instructional Technology
50 Wheeler Rd
Central Islip, NY 11722 Pvoigt@centralislip.k12.ny.us

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.

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. 65016502 (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/dataprivacysecurity/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's Director of Technology at pvoigt@centralislip.k12.ny.us (ii) Complaints may also be submitted to the NYS Education Department at www.nysed.gov/data-privacysecurity/reportimproper-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. 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.
8. Educational agency contracts with vendors that receive PII will address statutory and regulatory data privacy and security requirements.

EXHIBIT B

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).

<p>Description of the purpose(s) for which Contractor will receive/access PII</p>	<p>Description: Note to CISD: Kahoot! will process such personal data as required to deliver the service to the customer. Certain features of the Kahoot! services permit the host to collect information about players/employees as a group or as individuals, such as attendance, results, answers submitted when playing Kahoot! games and performance on Kahoot! games. We use such information only to provide the services, such as to permit the host (employer/company) to interact with players (employees) and track their progress over time. A host) may permit employees/players to share information with others, such as with other players/employees in the same organization or group.</p> <p>This includes:</p> <ol style="list-style-type: none"> 1. Employee account data; this may include names, email addresses, username, organization, picture/avatar, title 2. User data. This may include assigned Kahoot!s, results, scores and rating, date and time of game 3. Browser data, including IP addresses and logs <p>The data is submitted by the customer/employees (users) directly into the Kahoot! service or collected automatically. The data is used only for the purposes of delivering the Kahoot! service to the customer. For Kahoot!’s processing of personal data as a controller, please refer to our [Privacy Policy.](https://kahoot.com/privacy-policy/)</p> <p><input type="checkbox"/> NO PII OR DATA IS COLLECTED OR VIEWABLE THROUGH THIS PROGRAM/APP NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE</p>
<p>Type of PII that Contractor will receive/access</p>	<p>Check all that apply:</p> <p><input checked="" type="checkbox"/> Student PII</p> <p><input checked="" type="checkbox"/> Employee PII</p> <p><input type="checkbox"/> NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE</p>
<p>Contract Term</p>	<p>Each Data Privacy Agreement is valid through the software renewal period or 1 Year for non-paid/free/pilot programs.</p>

<p>Data Transition and Secure Destruction</p>	<p>Upon expiration or termination of the Contract, Contractor shall:</p> <p><input type="checkbox"/> 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.</p> <p><input checked="" type="checkbox"/> Securely delete and destroy data, six months after contract termination</p> <p><input type="checkbox"/> NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE</p>
<p>Challenges to Data Accuracy</p>	<p>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/emailed request.</p>
<p>Encryption</p>	<p><input checked="" type="checkbox"/> Data will be encrypted while in motion and at rest.</p> <p><input type="checkbox"/> NOT APPLICABLE - NO PII OR DATA IS COLLECTED/VIEWABLE</p>

EXHIBIT C – VENDOR DATA SECURITY & PRIVACY PLAN

Security Measures

Kahoot! recognizes Customer information and data as the most critical aspect and important success factor in our business. Having our Customers trust in our handling of their data is crucial to drive Kahoot! forward as the leading learning platform vendor.

To ensure the data is secure we at Kahoot! have implemented a set of safeguards and processes covering all parts of the data journey. In addition, with new features and opportunities in our learning platform continuously being added, we are driven by clear policies, principles and procedures to ensure data stays secure.

SECURITY CONTROLS

Kahoot! have implemented and maintains the following security controls for customer and user data, consistent with globally cloud service provider industry best practices, including:

1. Controls, Policies & Procedures. Appropriate technical and administrative controls, and organizational policies and procedures.
2. Named person in the role as a dedicated Chief information security officer (CISO) with focus on security in all areas of the Kahoot! business.
3. Access Authorization. Access controls for provisioning users, which shall include providing Customers mechanism to view Customer users and their access privileges for licensed users.
4. Logging. System and application logging where technically possible. Kahoot! retains logs for a maximum one (1) month, verify such logs periodically for completeness.
5. Malicious code and/or software. Malware prevention software (e.g. antivirus) is implemented on infrastructure where applicable. Using Kahoot! does not

- demand any Customer hardware installment. Users can choose to install App on mobile devices.
6. System Security. System and IT security controls at Kahoot! follows industry best practices, including: (i) A high-level diagram, which will be provided to Customers upon request; (ii) Kahoot! use a mix of industry standard cloud and software firewalls to dynamically limit external and internal traffic between our services; (iii) A program for evaluating security patches and implementing patches using a formal change process within defined time limits; (iv) Kahoot! Runs continuous penetration testing by an independent third party, with a detailed written report issued annually by such third party and provided to Customers upon request; (v) Documentation of identified vulnerabilities ranked based on risk severity, and corrective action according to such rank.
 7. Asset Management. An asset management policy is kept current, including asset classification (e.g., information, software, hardware).
 8. Kahoot! runs regularly cross company Risk Assessments to ensure potential risks are identified and managed.
 9. A Password policy and controls are implemented to protect data, including complexity requirements and multi factor authentication where available.
 10. Kahoot! uses sub-processors to strengthen the scalability. All sub-processors hold the highest level of security and have current certifications for, among others, ISO27001 and SOC2 Type 2.

DATA SECURITY

Kahoot! have a strong commitment to our Customers and users data. Compliance with the GDPR is a top priority for Kahoot! and our customers. The GDPR aims to strengthen personal data protection in Europe, and impacts the way we all do business. With Cloud, taking advantage of the global market is important to Kahoot!, delivering a learning platform to all. Kahoot! is diligent with its use of sub-processors, and never makes transfers outside the Europe/EEA without having appropriate safeguards in place. This may, where required, include additional safety measures.

1. Kahoot! will handle our Customers and Users data securely, and consistent. To ensure this is a cross company focus, Kahoot! employs a dedicated person that is responsible for data protection.
2. Encryption. Kahoot! have implemented encryption on all Customer and user data.
 1. At Rest: Customer data only resides in the production environment encrypted with industry best practices (currently AES-256 or similar).
 2. In Transit: All network communication uses TLS v1.2 or higher. Qualys' SSL Labs scored our SSL implementation as "A+" on their SSL Server test.
3. Data availability. Kahoot! runs multiple live data stores for availability
4. Backups. Kahoot! runs continuous backup processes to ensure data and information consistency with highest standards. Testing of the backups is done regularly.
5. Testing. Kahoot! never uses real Customer data in our development environment.

OPERATIONAL SECURITY

Running a service demands high focus on structure, best-practices, and proven methods. At the same time implement usage of new technologies when and where appropriate. This demands clear structure and procedures. For this Kahoot! has implemented, among others, following measures:

1. A Business Continuity and Disaster Recovery policy and plans. These are tested on a regular basis. The plans include infrastructure and applications used to host Customer Information and provide Services to our Customers.
2. To structure the work done Kahoot! uses an ISMS.
3. The operation is thoroughly monitored with uptime checks, logs, trends analysis and IDS. Any significant issues are alerted on 24/7.
4. Kahoot! operates a geo redundant platform with no fixed maintenance windows; The service is expected to be available continuously.

PEOPLE SECURITY

To ensure Kahoot! deliver on Customer expectation on quality, security, and privacy, Kahoot! have enforced controls on employee level

1. All employees are required to secure their equipment following the Information security policy, including antivirus, encryption, and MFA.
2. We run background checks and sign confidentiality agreements with all employees according to applicable laws. We also train them in Information Security and Secure Development Practices.
3. For Kahoot! inclusion, equality, respect and honesty is important in everything we do, and conduct regular training in our policies, including
 - a. Inclusion and Accessibility Policy
 - b. Anti-bribery & Anti-corruption Policy
 - c. Anti-Slavery & Anti-Child Labor Policy
 - d. Gender Equality & Anti-discrimination Policy
 - e. Whistleblowing policy
4. Systems access control. Employee's level of access is determined by the job position. Access reviews are performed periodically, and access is immediately removed if no longer necessary. Kahoot! enforces the least privilege principle.

As the duly authorized officer of the "contractor" as listed above I attest to all of the above submitted information to be true and accept any liability and/or responsibility for any data breaches or intrusions associated with this program, applications, software or browser extension.

DocuSigned by:

Mads Rebsdorf

7F009BDB0B294DC...

CRO

Signature of Vendor Official Representative

Date 28/9/2023 | 17:46 CE

If the program does not collect or transmit any PII, this document must still be completed, initialed (pages) and signed but you may and the select "NO PII OR DATA IS COLLECTED OR VIEWABLE" option above. No program/app/extension will be considered without a complete agreement.

of 10

Contractor Initials: 