

## DATA PRIVACY AGREEMENT

**Shenendehowa Central School District**

**and**

**Spotify USA Inc.**

This Data Privacy Agreement ("DPA") is by and between the Shenendehowa Central School District ("EA"), an Educational Agency, and Spotify USA Inc. ("Contractor"), collectively, the "Parties".

### ARTICLE I: DEFINITIONS

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

1. **Breach:** The actual unauthorized acquisition, access, use, or disclosure of Personally Identifiable Information in Contractor's possession or Breach of Contractor's security that compromises the security or privacy of that information, in a manner not permitted by applicable State and federal laws, rules and regulations or .
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 processing Student Data 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 the Soundtrap for Education services ("Services") to the EA pursuant to the Soundtrap Terms of Use located at <https://www.soundtrap.com/legal/terms> ("Service Agreement"), entered into by the parties, which this DPA is hereby incorporated into; Contractor may receive PII regulated by several New York and federal laws and regulations, among them, the Family Educational Rights and Privacy Act ("FERPA") at 12 U.S.C. 1232g (34 CFR Part 99); Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. 6501-6502 (16 CFR Part 312); Protection of Pupil Rights Amendment ("PPRA") at 20 U.S.C. 1232h (34 CFR Part 98); the Individuals with Disabilities Education Act ("IDEA") at 20 U.S.C. 1400 et seq. (34 CFR Part 300); New York Education Law Section 2-d; and the Commissioner of Education's Regulations at 8 NYCRR Part 121. The Parties enter this DPA to address the requirements of New York law. 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 or as permitted by this DPA. Neither the Services provided nor the manner in which such Services are provided shall violate applicable 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 applicable New York State, federal and local laws and regulations and the EA's policies as applicable to the Contractor. 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 CyberSecurity Framework. Contractor shall comply with the EA's data security and privacy policy, as applicable to the Contractor.

**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. Contractor will periodically assess and update its own security program, and upon request Contractor will provide the EA with completed questionnaires, assessments, or supporting documentation regarding Contractor's compliance with its 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 will be contractually required to comply with terms that are at least as protective of Student Data as those imposed on Contractor under 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 Contractor has actual knowledge a subcontractor fails to materially comply with the requirements of its own security and privacy obligations, which are substantially similar to this DPA, Contractor shall take the appropriate measures, including notify the EA and remove such subcontractor's access to PII to the extent EA's PII is negatively impacted by such subcontractor's failure, Contractor will contractually require subcontractor to , as applicable, return all PII received or stored by such subcontractor and/or ensure that PII has been securely deleted and destroyed in accordance its contractual obligations . In the event Contractor is made aware of an actual incident by the subcontractor which results in an actual unauthorized disclosure of 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) Except as permitted under this DPA, 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, will receive, or will be contractually required to 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 Subcontractors 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 except as permitted under this DPA it is

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

- (b) If applicable, once the transfer of PII has been accomplished in accordance with the EA's written election to do so, upon written request 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 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, upon written request 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. Notwithstanding anything to the contrary, Contractor shall not be required to return or destroy any computer records or files containing Student Data that have been created pursuant to its standard archiving or backup procedures, or contained in any archived electronic communications (e.g. emails). Contractor may also retain a copy of Student Data if required by applicable law. The confidentiality obligations contained herein shall apply to the archived and legally required copies so long as they exist.
- (c) Upon written request, 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. Notwithstanding anything to the contrary herein, Contractor is not prohibited from using de-identified data, including to improve its services or for internal analysis.

**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 actual 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 to the extent known 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:

**Rebecca Carman**  
**Shenendehowa District Privacy Officer**  
**5 Chelsea Place**  
**Clifton Park, NY 12065**  
**carmrebe@shenschools.org**

**13. Cooperation with Investigations.**

Contractor agrees that it will reasonably cooperate with the EA and law enforcement, where necessary, in any investigations into an actual Breach. Any costs actually incurred by the EA in providing required notice of the Breach, 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 without unreasonable delay 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, unless parents are afforded such rights by law or order.

**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	Spotify USA Inc.
BY: <i>[Signature]</i> Rebecca Carman	BY: <i>[Signature]</i> Michael Bell
<i>[Printed Name]</i> Rebecca Carman	<i>[Printed Name]</i> Michael Bell
<i>[Title]</i> DPO	<i>[Title]</i> Head of Sales, Soundtrap
Date: 10/18/21	Date: October 20, 2021

## 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:

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, place of birth, social security number, biometric record & mother's maiden name, which when linked to or combined with other information that, alone or in combination, is linked or linkable to a specific student and would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or any information requested by a person if the educational agency or institution reasonably believes that person knows the identity of the student to whom the education record relate

1. 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.
2. 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.
3. 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.
4. A complete list of all student data elements collected by NYSED is available at [www.nysed.gov/data-privacy-security/student-data-inventory](http://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.
5. The right to have complaints about possible breaches and unauthorized disclosures of PII addressed. (i) Complaints should be submitted to the Shenendehowa Central School District, Director of Policy & Community Development/Data Protection Officer, 5 Chelsea Place, Clifton Park, NY 12065. (ii) Complaints may also be submitted to the NYS Education Department at [www.nysed.gov/data-privacy-security/report-improper-disclosure](http://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](mailto:privacy@nysed.gov); or by telephone at 518-474-0937.
6. To be notified in accordance with applicable laws and regulations if a breach or unauthorized release of PII occurs.
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.

**CONTRACTOR: Spotify USA Inc.**

[Signature]	<i>Michael Bell</i>
[Printed Name]	Michael Bell
[Title]	Head of Sales, Soundtrap
Date:	October 20, 2021

## 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).

<b>Name of Contractor</b>	Spotify USA Inc.
<b>Description of the purpose(s) for which Contractor will receive/access PII</b>	Contractor will receive PII data to provide the Soundtrap for Education services under the Soundtrap Terms of Use located at <a href="https://www.soundtrap.com/legal/terms">https://www.soundtrap.com/legal/terms</a> .
<b>Type of PII that Contractor will receive/access</b>	Check all that apply:  <input checked="" type="checkbox"/> Student PII <input type="checkbox"/> APPR Data
<b>Contract Term</b>	Contract Start Date: Effective Date in Contract  Contract End Date: -In accordance with the Service Agreement.

<b>Subcontractor Written Agreement Requirement</b>	<p>Contractor will contractually require subcontractors to adhere to, at a minimum, materially similar data protection obligations imposed on the contractor by applicable state and federal laws and regulations, and the Contract. (check applicable option)</p> <p><input type="checkbox"/> Contractor will not utilize subcontractors.</p> <p>Contractor will utilize subcontractors.</p>
<b>Data Transition and Secure Destruction</b>	<p>Upon expiration or termination of the Contract, Contractor shall:</p> <ul style="list-style-type: none"> <li>• Upon written request, 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.</li> <li>• Upon written request, securely delete and destroy data in accordance with the DPA.</li> </ul>
<b>Challenges to Data Accuracy</b>	<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 30 days of receiving the EA's written request.</p>
<b>Secure Storage and Data Security</b>	<p>Please describe where PII will be stored and the protections taken to ensure PII will be protected: (check all that apply)</p> <p>Using a cloud or infrastructure owned and hosted by a third party.</p> <p>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: Please see attached Data Security and Privacy Plan.</p>
<b>Encryption</b>	<p>Data will be encrypted while in motion and at rest. X</p>

CONTRACTOR: Spotify USA Inc.	
[Signature]	<i>Michael Bell</i>
[Printed Name]	Michael Bell
[Title]	Head of Sales, Soundtrap
Date:	October 20, 2021

## 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.	X
2	Specify the administrative, operational and technical safeguards and practices that you have in place to protect PII.	X
3	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.	X
4	Outline processes that ensure that your employees and any subcontractors are bound by written agreement to the requirements of the Contract, at a minimum.	X
5	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.	X
6	Describe how data will be transitioned to the EA when no longer	X

	needed by you to meet your contractual obligations, if applicable.	
7	Describe your secure destruction practices and how certification will be provided to the EA.	X
8		
9	Outline how your data security and privacy program/practices materially align with the NIST CSF v1.1 using the Framework chart below.	X PLEASE USE TEMPLATE BELOW.