STANDARD STUDENT DATA PRIVACY AGREEMENT

(NDPA Standard Version 1.0)

Sandwich CUSD #430

(School district/education agency)

and

Soundation AB

This Student Data Privacy Agreement ("DPA") is entered into on the date of full execution (the "Effective Date") and is entered into by and between:

(School District Name)	Sandwich CUSD #430
located at	720 S. Wells Street, Sandwich, IL 60548

(the "Local Education Agency" or "LEA")

and

Soundation AB, located at Soundation AB, Götgatan 15, 116 46, Stockholm, Sweden (the "Provider").

WHEREAS, the Provider is providing educational or digital services to LEA.

WHEREAS, the Provider and LEA recognize the need to protect personally identifiable student information and other regulated data exchanged between them as required by applicable laws and regulations, such as the Family Educational Rights and Privacy Act ("FERPA") at 20 U.S.C. § 1232g (34 CFR Part 99); the Children's Online Privacy Protection Act ("COPPA") at 15 U.S.C. § 6501-6506 (16 CFR Part 312), applicable state privacy laws and regulations and

WHEREAS, the Provider and LEA desire to enter into this DPA for the purpose of establishing their respective obligations and duties in order to comply with applicable laws and regulations.

NOW THEREFORE, for good and valuable consideration, LEA and Provider agree as follows:

1. A description of the Services to be provided, the categories of Student Data that may be provided by LEA to Provider, and other information specific to this DPA are contained in the Standard Clauses hereto.

2. Special Provisions. Check if Required

- □ If checked, the Supplemental State Terms and attached hereto as Exhibit "G" are hereby incorporated by reference into this DPA in their entirety.

- □ If checked, LEA and Provider agree to the additional terms or modifications set forth in Exhibit "H". (Optional)

- □ If checked, the Provider, has signed Exhibit "E" to the Standard Clauses, otherwise known as General Offer of Privacy Terms

3. In the event of a conflict between the SDPC Standard Clauses, the State or Special Provisions will control. In the event there is conflict between the terms of the DPA and any other writing, including, but not limited to the Service Agreement and Provider Terms of Service or Privacy Policy the terms of this DPA shall control.

4. This DPA shall stay in effect for three (3) years. Exhibit “E” will expire three (3) years from the date the original DPA was signed.

5. The services to be provided by Provider to LEA pursuant to this DPA are detailed in Exhibit “A” (the “Services”).

6. Notices. All notices or other communication required or permitted to be given hereunder may be given via e-mail transmission, or first-class mail, sent to the designated representatives below.

The designated representative for the LEA for this DPA is:

Name:	Glen Bloemker
Title:	Director of Technology
Address	720 S. Wells Street, Sandwich, IL 60548
Phone:	815-786-2187 opt 6, opt 3
Email:	gbloemker@sandwich430.org

The designated representative for the Provider for this DPA is:

Name:	Adam Hasslert
Title:	CEO
Address	Soundation AB, Götgatan 15, 116 46, Stockholm Sweden
Phone:	+46704321000
Email:	adam@soundation.com

IN WITNESS WHEREOF, LEA and Provider execute this DPA as of the Effective Date.

LEA (School district name):	Sandwich CUSD #430
By:	Glen Bloemker
Date:	28 Aug 2023
Printed name:	Glen Bloemker
Title/Position:	Director of Technology

Soundation AB

By:	CEO
Date:	9 Jun 2023
Printed name:	Adam Hasslert
Title/Position:	CEO

ARTICLE I: PURPOSE AND SCOPE

1. Purpose of DPA.
The purpose of this DPA is to describe the duties and responsibilities to protect Student Data including compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time. In performing the Services, the Provider shall be considered a School Official with a legitimate educational interest, and performing services otherwise provided by the LEA. Provider shall be under the direct control and supervision of the LEA, with respect to its use of Student Data

2. Student Data to Be Provided.
In order to perform the Services described above, LEA shall provide Student Data as identified in the Schedule of Data, attached hereto as Exhibit "B".

3. DPA Definitions.
The definition of terms used in this DPA is found in Exhibit "C". In the event of a conflict, definitions used in this DPA shall prevail over terms used in any other writing, including, but not limited to the Service Agreement, Terms of Service, Privacy Policies etc.

ARTICLE II: DATA OWNERSHIP AND AUTHORIZED ACCESS

1. Student Data Property of LEA.
All Student Data transmitted to the Provider pursuant to the Service Agreement is and will continue to be the property of and under the control of the LEA. The Provider further acknowledges and agrees that all copies of such Student Data transmitted to the Provider, including any modifications or additions or any portion thereof from any source, are subject to the provisions of this DPA in the same manner as the original Student Data. The Parties agree that as between them, all rights, including all intellectual property rights in and to Student Data contemplated per the Service Agreement, shall remain the exclusive property of the LEA. For the purposes of FERPA, the Provider shall be considered a School Official, under the control and direction of the LEA as it pertains to the use of Student Data, notwithstanding the above.

2. Parent Access.
To the extent required by law the LEA shall establish reasonable procedures by which a parent, legal guardian, or eligible student may review Education Records and/or Student Data correct erroneous information, and procedures for the transfer of student-generated content to a personal account, consistent with the functionality of services. Provider shall respond in a reasonably timely manner (and no later than forty five (45) days from the date of the request or pursuant to the time frame required under state law for an LEA to respond to a parent or student, whichever is sooner) to the LEA's request for Student Data in a student's records held by the Provider to view or correct as necessary. In the event that a parent of a student or other individual contacts the Provider to review any of the Student Data accessed pursuant to the Services, the Provider shall refer the parent or individual to the LEA, who will follow the necessary and proper procedures regarding the requested information.

3. Separate Account.
If Student-Generated Content is stored or maintained by the Provider, Provider shall, at the request of the LEA, transfer, or provide a mechanism for the LEA to transfer, said Student-Generated Content to a separate account created by the student.

4. Law Enforcement Requests.
Should law enforcement or other government entities ("Requesting Party(ies)") contact Provider with a request for Student Data held by the Provider pursuant to the Services, the Provider shall notify the LEA in advance of a compelled disclosure to the Requesting Party, unless lawfully directed by the Requesting Party not to inform the LEA of the request.

5. Subprocessors.
Provider shall enter into written agreements with all Subprocessors performing functions for the Provider in order for the Provider to provide the Services pursuant to the Service Agreement, whereby the Subprocessors agree to protect Student Data in a manner no less stringent than the terms of this DPA.

ARTICLE III: DUTIES OF LEA

1. Provide Data in Compliance with Applicable Laws.
LEA shall provide Student Data for the purposes of obtaining the Services in compliance with all applicable federal, state, and local privacy laws, rules, and regulations, all as may be amended from time to time.

2. Annual Notification of Rights.
If the LEA has a policy of disclosing Education Records and/or Student Data under FERPA (34 CFR § 99.31(a)(1)), LEA shall include a specification of criteria for determining who constitutes a school official and what constitutes a legitimate educational interest in its annual notification of rights.

3. Reasonable Precautions.
LEA shall take reasonable precautions to secure usernames, passwords, and any other means of gaining access to the services and hosted Student Data.

4. Unauthorized Access Notification.
LEA shall notify Provider promptly of any known unauthorized access. LEA will assist Provider in any efforts by Provider to investigate and respond to any unauthorized access.

ARTICLE IV: DUTIES OF PROVIDER

1. Privacy Compliance.
The Provider shall comply with all applicable federal, state, and local laws, rules, and regulations pertaining to Student Data privacy and security, all as may be amended from time to time.

2. Authorized Use.

The Student Data shared pursuant to the Service Agreement, including persistent unique identifiers, shall be used for no purpose other than the Services outlined in Exhibit “A” or stated in the Service Agreement and/or otherwise authorized under the statutes referred to herein this DPA.

3. Provider Employee Obligation.

Provider shall require all of Provider’s employees and agents who have access to Student Data to comply with all applicable provisions of this DPA with respect to the Student Data shared under the Service Agreement. Provider agrees to require and maintain an appropriate confidentiality agreement from each employee or agent with access to Student Data pursuant to the Service Agreement.

4. No Disclosure.

Provider acknowledges and agrees that it shall not make any re-disclosure of any Student Data or any portion thereof, including without limitation, user content or other nonpublic information and/or personally identifiable information contained in the Student Data other than as directed or permitted by the LEA or this DPA. This prohibition against disclosure shall not apply to aggregate summaries of De-Identified information, Student Data disclosed pursuant to a lawfully issued subpoena or other legal process, or to Subprocessors performing services on behalf of the Provider pursuant to this DPA. Provider will not Sell Student Data to any third party.

5. De-Identified Data:

Provider agrees not to attempt to re-identify De-Identified Student Data. DeIdentified Data may be used by the Provider for those purposes allowed under FERPA and the following purposes: (1) assisting the LEA or other governmental agencies in conducting research and other studies; and (2) research and development of the Provider's educational sites, services, or applications, and to demonstrate the effectiveness of the Services; and (3) for adaptive learning purpose and for customized student learning. Provider's use of De-Identified Data shall survive termination of this DPA or any request by LEA to return or destroy Student Data. Except for Subprocessors, Provider agrees not to transfer de-identified Student Data to any party unless (a) that party agrees in writing not to attempt re-identification, and (b) prior written notice has been given to the LEA who has provided prior written consent for such transfer. Prior to publishing any document that names the LEA explicitly or indirectly, the Provider shall obtain the LEA’s written approval of the manner in which De-Identified Data is presented.

6. Disposition of Data.

Upon written request from the LEA, Provider shall dispose of or provide a mechanism for the LEA to transfer Student Data obtained under the Service Agreement, within sixty (60) days of the date of said request and according to a schedule and procedure as the Parties may reasonably agree. Upon termination of this DPA, if no written request from the LEA is received, Provider shall dispose of all Student Data after providing the LEA with reasonable prior notice. The duty to dispose of Student Data shall not extend to Student Data that had been De-Identified or placed in a separate student account pursuant to section II 3. The LEA may employ a “Directive for Disposition of Data” form, a copy of which is attached hereto as Exhibit “D”. If the LEA and Provider employ Exhibit “D”, no further written request or notice is required on the part of either party prior to the disposition of Student Data described in Exhibit “D”.

7. Advertising Limitations.

Provider is prohibited from using, disclosing, or selling Student Data to (a) inform, influence, or enable Targeted Advertising; or (b) develop a profile of a student, family member/guardian or group, for any purpose other than providing the Service to LEA. This section does not prohibit Provider from using Student Data (i) for adaptive learning or customized student learning (including generating personalized learning recommendations); or (ii) to make product recommendations to teachers or LEA employees; or (iii) to notify account holders about new education product updates, features, or services or from otherwise using Student Data as permitted in this DPA and its accompanying exhibits

(1) The security breach notification described above shall include, at a minimum, the following information to the extent known by the Provider and as it becomes available:
i. The name and contact information of the reporting LEA subject to this section.
ii. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach.
iii. If the information is possible to determine at the time the notice is provided, then either (1) the date of the breach, (2) the estimated date of the breach, or (3) the date range within which the breach occurred. The notification shall also include the date of the notice.
iv. Whether the notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided; and a general description of the breach incident, if that information is possible to determine at the time the notice is provided.

(2) Provider agrees to adhere to all federal and state requirements with respect to a data breach related to the Student Data, including, when appropriate or required, the required responsibilities and procedures for notification and mitigation of any such data breach.

(3) Provider further acknowledges and agrees to have a written incident response plan that reflects best practices and is consistent with industry standards and federal and state law for responding to a data breach, breach of security, privacy incident or unauthorized acquisition or use of Student Data or any portion thereof, including personally identifiable information and agrees to provide LEA, upon request, with a summary of said written incident response plan.

(4) LEA shall provide notice and facts surrounding the breach to the affected students, parents or guardians.

(5) In the event of a breach originating from LEA’s use of the Service, Provider shall cooperate with LEA to the extent necessary to expeditiously secure Student Data.

ARTICLE VI: GENERAL OFFER OF TERMS

Provider may, by signing the attached form of “General Offer of Privacy Terms” (General Offer, attached hereto as **Exhibit “E”**), be bound by the terms of **Exhibit “E”** to any other LEA who signs the acceptance on said Exhibit. The form is limited by the terms and conditions described therein.

ARTICLE VII: MISCELLANEOUS

1. Termination.
In the event that either Party seeks to terminate this DPA, they may do so by mutual written consent so long as the Service Agreement has lapsed or has been terminated. Either party may terminate this DPA and any service agreement or contract if the other party breaches any terms of this DPA.

2. Effect of Termination Survival.
If the Service Agreement is terminated, the Provider shall destroy all of LEA’s Student Data pursuant to Article IV, section 6.

3. Priority of Agreements.
This DPA shall govern the treatment of Student Data in order to comply with the privacy protections, including those found in FERPA and all applicable privacy statutes identified in this DPA. In the event there is conflict between the terms of the DPA and the Service Agreement, Terms of Service, Privacy Policies, or with any other bid/RFP, license agreement, or writing, the terms of this DPA shall apply and take precedence. In the event of a conflict between **Exhibit “H”**, the SDPC Standard Clauses, and/or the Supplemental State Terms, **Exhibit “H”** will control, followed by the Supplemental State Terms. Except as described in this paragraph herein, all other provisions of the Service Agreement shall remain in effect.

4. Entire Agreement.
This DPA and the Service Agreement constitute the entire agreement of the Parties relating to the subject matter hereof and supersedes all prior communications, representations, or agreements, oral or written, by the Parties relating thereto. This DPA may be amended and the observance of any provision of this DPA may be waived (either generally or in any particular instance and either retroactively or prospectively) only with the signed written consent of both Parties. Neither failure nor delay on the part of any Party in exercising any right, power, or privilege hereunder shall operate as a waiver of such right, nor shall any single or partial exercise of any such right, power, or privilege preclude any further exercise thereof or the exercise of any other right, power, or privilege.

5. Severability.
Any provision of this DPA that is prohibited or unenforceable in any jurisdiction shall, as to such jurisdiction, be ineffective to the extent of such prohibition or unenforceability without invalidating the remaining provisions of this DPA, and any such prohibition or unenforceability in any jurisdiction shall not invalidate or render unenforceable such provision in any other jurisdiction. Notwithstanding the foregoing, if such provision could be

more narrowly drawn so as not to be prohibited or unenforceable in such jurisdiction while, at the same time, maintaining the intent of the Parties, it shall, as to such jurisdiction, be so narrowly drawn without invalidating the remaining provisions of this DPA or affecting the validity or enforceability of such provision in any other jurisdiction.

6. Governing Law; Venue and Jurisdiction.

THIS DPA WILL BE GOVERNED BY AND CONSTRUED IN ACCORDANCE WITH THE LAWS OF THE STATE OF THE LEA, WITHOUT REGARD TO CONFLICTS OF LAW PRINCIPLES. EACH PARTY CONSENTS AND SUBMITS TO THE SOLE AND EXCLUSIVE JURISDICTION TO THE STATE AND FEDERAL COURTS FOR THE COUNTY OF THE LEA FOR ANY DISPUTE ARISING OUT OF OR RELATING TO THIS DPA OR THE TRANSACTIONS CONTEMPLATED HEREBY.

7. Successors Bound:

This DPA is and shall be binding upon the respective successors in interest to Provider in the event of a merger, acquisition, consolidation or other business reorganization or sale of all or substantially all of the assets of such business In the event that the Provider sells, merges, or otherwise disposes of its business to a successor during the term of this DPA, the Provider shall provide written notice to the LEA no later than sixty (60) days after the closing date of sale, merger, or disposal. Such notice shall include a written, signed assurance that the successor will assume the obligations of the DPA and any obligations with respect to Student Data within the Service Agreement. The LEA has the authority to terminate the DPA if it disapproves of the successor to whom the Provider is selling, merging, or otherwise disposing of its business.

8. Authority.

Each party represents that it is authorized to bind to the terms of this DPA, including confidentiality and destruction of Student Data and any portion thereof contained therein, all related or associated institutions, individuals, employees or contractors who may have access to the Student Data and/or any portion thereof.

9. Waiver.

No delay or omission by either party to exercise any right hereunder shall be construed as a waiver of any such right and both parties reserve the right to exercise any such right from time to time, as often as may be deemed expedient.

<u>EXHIBIT “A”</u>

DESCRIPTION OF SERVICES

Soundation Education is an online digital audio workstation (DAW) specifically tailored for contemporary music education in school environments. It allows students to create music using a wide variety of tools and share their projects within the safe space of whichever organization they belong to, and it allows teachers or mentors to create assignments and manage projects submitted by their students.

EXHIBIT “B”

SCHEDULE OF DATA

Category of Data	**Elements**	**Check if Used by Your System**
Application Technology Meta Data	IP Addresses of users, Use of cookies, etc.	☑
	Other application technology meta data-Please specify:	□
Application Use Statistics	Meta data on user interaction with application	□
Assessment	Standardized test scores	□
	Observation data	□
	Other assessment data-Please specify:	□
Attendance	Student school (daily) attendance data	□
	Student class attendance data	□
Communications	Online communications captured (emails, blog entries)	□
Conduct	Conduct or behavioral data	□
Demographics	Date of Birth	□
	Place of Birth	□
	Gender	□
	Ethnicity or race	□
	Language information (native, or primary language spoken by student)	□
	Other demographic information-Please specify:	□
Enrollment	Student school enrollment	□
	Student grade level	□
	Homeroom	□

	Guidance counselor	□
	Specific curriculum programs	□
	Year of graduation	□
	Other enrollment information-Please specify:	□
Parent/Guardian Contact Information	Address	□
	Email	□
	Phone	□
Parent/Guardian ID	Parent ID number (created to link parents to students)	□
Parent/Guardian Name	First and/or Last	□
Schedule	Student scheduled courses	□
	Teacher names	□
Special Indicator	English language learner information	□
	Low income status	□
	Medical alerts/ health data	□
	Student disability information	□
	Specialized education services (IEP or 504)	□
	Living situations (homeless/foster care)	□
	Other indicator information-Please specify:	□
Student Contact Information	Address	□
	Email	☑
	Phone	□
Student Identifiers	Local (School district) ID number	□
	State ID number	
	Provider/App assigned student ID number	
	Student app username	
	Student app passwords	
Student Name	First and/or Last	□

Student In App Performance	Program/application performance (typing program student types 60 wpm, reading program-student reads below grade level)	□
Student Program Membership	Academic or extracurricular activities a student may belong to or participate in	□
Student Survey Responses	Student responses to surveys or questionnaires	□
Student work	Student generated content; writing, pictures, etc	☑
	Other student work data -Please specify: Recorded audio and midi patterns	
Transcript	Student course grades	□
	Student course data	
	Student course grades/ performance scores	
	Other transcript data - Please specify:	
Transportation	Student bus assignment	□
	Student pick up and/or drop off location	
	Student bus card ID number	
	Other transportation data – Please specify:	
Other	Please list each additional data element used, stored, or collected by your application:	□
None	No Student Data collected at this time. Provider will immediately notify LEA if this designation is no longer applicable	□

EXHIBIT “C”

DEFINITIONS

De-Identified Data and De-Identification: Records and information are considered to be De-Identified when all personally identifiable information has been removed or obscured, such that the remaining information does not reasonably identify a specific individual, including, but not limited to, any information that, alone or in combination is linkable to a specific student and provided that the educational agency, or other party, has made a reasonable determination that a student’s identity is not personally identifiable, taking into account reasonable available information.

Educational Records: Educational Records are records, files, documents, and other materials directly related to a student and maintained by the school or local education agency, or by a person acting for such school or local education agency, including but not limited to, records encompassing all the material kept in the student’s cumulative folder, such as general identifying data, records of attendance and of academic work completed, records of achievement, and results of evaluative tests, health data, disciplinary status, test protocols and individualized education programs.

Metadata: means information that provides meaning and context to other data being collected; including, but not limited to: date and time records and purpose of creation Metadata that have been stripped of all direct and indirect identifiers are not considered Personally Identifiable Information.

Operator: means the operator of an internet website, online service, online application, or mobile application with actual knowledge that the site, service, or application is used for K–12 school purposes. Any entity that operates an internet website, online service, online application, or mobile application that has entered into a signed, written agreement with an LEA to provide a service to that LEA shall be considered an “operator” for the purposes of this section.

Originating LEA: An LEA who originally executes the DPA in its entirety with the Provider.

Provider: For purposes of the DPA, the term “Provider” means provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Student Data. Within the DPA the term “Provider” includes the term “Third Party” and the term “Operator” as used in applicable state statutes.

Student Generated Content: The term “Student-Generated Content” means materials or content created by a student in the services including, but not limited to, essays, research reports, portfolios, creative writing, music or other audio files, photographs, videos, and account information that enables ongoing ownership of student content.

School Official: For the purposes of this DPA and pursuant to 34 CFR § 99.31(b), a School Official is a contractor that: (1) Performs an institutional service or function for which the agency or institution would otherwise use employees; (2) Is under the direct control of the agency or institution with respect to the use and maintenance of Student Data including Education Records; and (3) Is subject to 34 CFR § 99.33(a) governing the use and re-disclosure of Personally Identifiable Information from Education Records.

Service Agreement: Refers to the Contract, Purchase Order or Terms of Service or Terms of Use

Student Data: Student Data includes any data, whether gathered by Provider or provided by LEA or its users, students, or students' parents/guardians, that is descriptive of the student including, but not limited to, information in the student's educational record or email, first and last name, birthdate, home or other physical address, telephone number, email address, or other information allowing physical or online contact, discipline records, videos, test results, special education data, juvenile dependency records, grades, evaluations, criminal records, medical records, health records, social security numbers, biometric information, disabilities, socioeconomic information, individual purchasing behavior or preferences, food purchases, political affiliations, religious information, text messages, documents, student identifiers, search activity, photos, voice recordings, geolocation information, parents' names, or any other information or identification number that would provide information about a specific student. Student Data includes Meta Data. Student Data further includes "Personally Identifiable Information (PII)," as defined in 34 C.F.R. § 99.3 and as defined under any applicable state law. Student Data shall constitute Education Records for the purposes of this DPA, and for the purposes of federal, state, and local laws and regulations. Student Data as specified in **Exhibit "B"** is confirmed to be collected or processed by the Provider pursuant to the Services. Student Data shall not constitute that information that has been anonymized or De-Identified, or anonymous usage data regarding a student's use of Provider's services.

Subprocessor: For the purposes of this DPA, the term "Subprocessor" (sometimes referred to as the "Subcontractor") means a party other than LEA or Provider, who Provider uses for data collection, analytics, storage, or other service to operate and/or improve its service, and who has access to Student Data. Subscribing LEA: An LEA that was not party to the original Service Agreement and who accepts the Provider's General Offer of Privacy Terms.

Targeted Advertising: means presenting an advertisement to a student where the selection of the advertisement is based on Student Data or inferred over time from the usage of the operator's Internet web site, online service or mobile application by such student or the retention of such student's online activities or requests over time for the purpose of targeting subsequent advertisements. "Targeted Advertising" does not include any advertising to a student on an Internet web site based on the content of the web page or in response to a student's response or request for information or feedback.

Third Party: The term "Third Party" means a provider of digital educational software or services, including cloud-based services, for the digital storage, management, and retrieval of Education Records and/or Student Data, as that term is used in some state statutes. However, for the purpose of this DPA, the term "Third Party" when used to indicate the provider of digital educational software or services is replaced by the term "Provider."

EXHIBIT “D”

DIRECTIVE FOR DISPOSITION OF DATA

____

(District or LEA)
Provider to dispose of data obtained by Provider pursuant to the terms of the Service Agreement between LEA and Provider. The terms of the Disposition are set forth below:

1. Extent of Disposition

□ Disposition is partial. The categories of data to be disposed of are set forth below or are found in an attachment to this Directive:

Student and staff personally identifiable information

□ Disposition is Complete. Disposition extends to all categories of data.

2. Nature of Disposition

□ Disposition shall be by destruction or deletion of data.

□ Disposition shall be by a transfer of data. The data shall be transferred to the following site as follows:

Vendor will send a notification that the data destruction has been completed as described above.

3. Schedule of Disposition

Data shall be disposed of by the following date:

□ As soon as commercially practicable.

□ By date:

____

4. Signature

____

Authorized Representative of LEA Date

Adam Hasslert 2023-10-05

____

Authorized Representative of Provider Date

<u>EXHIBIT “E”</u>

GENERAL OFFER OF PRIVACY TERMS

Privacy Policy

Last Amended: Jan 4th, 2023

Table of contents

1. Introduction

Thank you for choosing to use our service and a special thanks for taking the time to thoroughly read through this Privacy Policy. We would like to begin with a short summary explaining why we have created this policy.

Our fundamental objectives are to:

Give you a brief introduction to personal data;

Explain why we handle certain kinds of personal information;

Ensure that you understand what information we gather and what we actually do with said information;

Show you how we work to protect your rights and your integrity.

Our goal is that you, after having read this policy, will feel secure in that your personal integrity is respected and that your personal data is treated in a correct manner. We therefore also work on a continuous basis with securing that our treatment of personal data is completely in compliance with current legislation, especially the General Data Protection Regulation (GDPR) which will be in effect as of May the 25th, 2018.

2. What is personal data and what does the processing of personal data mean?

2.1 Personal data consists of all information that directly, or indirectly together with other information, can be connected to a living (physical) person. A non-exhaustive list with examples of personal data consists of, among others:
Name
Personal ID number
Email-address
IP-address
Pictures and video

2.2 The Processing of personal data includes every action connected to the use of the personal data, regardless of whether such an action is performed automatically or not. This means that the following actions, among others, are included:
Collection
Registration
Use
Alteration
Storage
Disclosure by transmission
Deletion

3. For whom is this policy applicable?

This Privacy Policy shall in the first instance be applicable to individuals who are users of our Services and from whom we collect and process personal data (”Data Subjects”). Different parts of this Privacy Policy may also be relevant to you depending on your relationship with us. All in all, this policy is relevant for persons who:
are customers or users of ours – when handling your account in order to provide you with the best possible user experience
visit our website or our social media platforms
otherwise communicate with us, for example through our customer service
By agreeing to this Privacy Policy you agree to our processing of your personal data in accordance with this Privacy Policy.

4. For what areas is this policy applicable?

This Privacy Policy regulates how we may collect and process personal data to be able to continue delivering and developing our Services.

5. What does it mean to be a Data Controller?

A Data Controller is a legal person or other entity that determines the purpose and means for the processing of personal data. A corporation is a Data Controller in regards to personal data it has for its own benefit in regards to its employees, customers, partners, users and others.

6. Soundation as a Data Controller

We, Soundation AB (company reg. no. 556561-6629) are the Data Controller and therefore accountable in accordance with applicable legislation, for the processing that occurs with your personal data, within the scope of our Services.

7. Why are we allowed to process personal data?

7.1 For it to be permissible for us to process personal data there must always be support for said treatment within the GDPR, so-called lawful basis. Such lawful basis may include:

Consent from the Data Subject.

That the processing of personal data is necessary to fulfill the terms of an agreement with the Data Subject, for example in relation to the use of the Services.

Fulfilling a legal obligation, for example storing certain information due to legislation regarding certain accounting standards and practices. This could also be the case when handling opt-out settings requests concerning your rights as a Data Subject in accordance with GDPR.

A weighing of interests when we have a legitimate interest in using your data, for example for statistical purposes and to market our services, and to secure payment and prevent fraud.

7.2 It may occur that the same personal data is processed both through support in terms of fulfilling an agreement as well as in terms of specific consent or in terms of the processing of that specific information is necessary to fulfill other legal obligations. This means that even though you may revoke your consent and the treatment based on said consent ceases, that specific personal data may remain with us for separate reasons.

8. What personal data do we process, and why?

In this section, we explain how your personal data is used in order for us to be able to provide you with relevant experiences, services, and offers.

8.1 When you sign up for our Services

When you register an account at soundation.com we handle the following personal data which you personally provide to us:

Your name and your contact information

Your credit card number and bank information, stored by our payment provider and in compliance with PCI DSS (security requirements for businesses that store, process or transmit cardholder data)

8.1.1 We handle your personal data in order to:

Identify you as a user

Charge you for the services and products that you have ordered

In order to discover, and prevent, fraud in conjunction with bank card payments

Handle and deliver what you have purchased in accordance with our terms and conditions

Notifying you (through email, or similar) regarding information connected to your usage of our Services

Market our Services and products, for example by email

Produce statistics regarding purchases and usage, in order to improve our services

Prevent any type of intellectual property infringement

8.1.2 Legal grounds for the processing

We process your personal data based on:
performance of a contract when we provide our Services;
based upon a weighing of interests when we have a legitimate interest in using your data for statistical purposes and to market our services, as well as to secure payment and prevent fraud and
based upon a legal obligation for handling opt-out settings requests concerning your rights in accordance with the GDPR
8.1.3 Period of storage
We save data about you for up to 12 months after termination of your user account, among other reasons to provide information regarding any complaints.

8.2 Users and members of Soundation
When you are a user of our Services, in addition to the provisions described in sections 8.1, we also process:
data about your user account, for example, user number and subscription
data about your usage of our Services
data about your purchasing history with Soundation
8.2.1 The personal data is processed in order to:
administer your user account
analyze and categorize you in relation to our other users based on information you have provided to us and based on how you use our services (musical style, preferences and purchasing history)
inform you of personal and tailor-made offers, campaigns, and benefits from us and our cooperating partners, for example by email
produce statistics and carry out analytical actions in order to develop our services and offers, including long-term analytical actions in order to understand trends over time
ensure the security of our Services, and discover or prevent various types of unlawful use, or use which otherwise contravenes the terms and conditions of our Services
8.2.2 Legal grounds for the processing:
We process your personal data based on
performance of a contract when we fulfill our obligations towards you as a user (for example administering your user account and providing relevant offers) and
based on a weighing of interests when we have a legitimate interest in using data about your usage of the service and your purchasing history to produce statistics needed to develop, improve, and ensure the functionality and security of our services.
8.2.3 Period of storage:
We save your personal data during the time that you have an active account at soundation.com and for up to 12 months after the termination of the said account. In order to ensure traceability, we save data regarding our communications with you for 12 months.

8.3 Persons with a login account
When you have a login account, in addition to the provisions described in sections 8.1, 8.2, we also process:
data about your login account, for example, username and password
data which you personally choose to save in your profile, for example name, contact information, etc.
data regarding your musical preferences and purchasing history, or how you otherwise use our services or our digital channels, for example, information regarding your most recent

logins
8.3.1 The personal data is processed in order to:
administer your login account
contact you with information and general offers, for example by email
produce statistics and carry out analytical actions to improve our services, goods, and offers, including long-term analytical actions needed to understand trends over time
provide, maintain, test, improve and develop the digital services and the technical platform used to provide our Services
ensure the security of our Services in order to discover or prevent various types of unlawful use, or use which otherwise breaches the terms and conditions
8.3.2 Legal grounds for the processing:
We process your personal data based on the
performance of a contract when we provide our Services
8.3.3 Period of storage:
We save your login information as long as you actively use your login account (up to 6 months after the last use) or have an active account with us. In order to ensure traceability, we save data regarding our communications with you for 12 months.
8.4 When you communicate with us
You can choose to communicate with us in many different ways, for example via social media and emails with our customer service.
When you communicate with us, we process data which you personally provide to us, for example:
name and contact information
information regarding your views, questions, or matters
8.4.1 We process your personal data in order to:
answer questions and handle your matters, for example addressing defects, handling complaints, questions about your musical content
improve our services and the information we provide and publish on our website
8.4.2 Legal grounds for the processing:
We process your personal data for our, and your, legitimate interest in administering your matter (weighing of interests).
8.4.3 Period of storage:
We save your personal data for up to 12 months after the matter is closed in order to ensure traceability in your communications with us.

9. How long do we generally store personal data?

Your personal data is stored only during the period for which there is a need to store the information to be able to fulfill the terms of the agreement. We may store your personal data longer if this is necessary from a legal standpoint or to safeguard our legal interests, for example within the scope of legal proceedings that we are involved in.

10. Our actions to protect personal data

10.1 We have ensured that we have taken all necessary and appropriate technical and organizational measures to safeguard your personal data against loss, misuse or unauthorized access.
10.2 To technically ensure that personal data is processed in a safe and confidential manner we use digital networks that are breach protected through for example encryption, firewalls, and password protection. In any instance where a breach may occur we have created

routines to identify, assess and minimize any damage that may occur as well as inform said damage to all affected parties.
10.3 To ensure an adequate knowledge level regarding the processing of personal data we will arrange ongoing educational efforts regarding GDPR, both for our employees as well as the consultants that may from time to another be contracted to do work for us.

11. When do we share personal data?
11.1 We will not sell, make available or spread personal data to third parties with the exception of what is stated throughout this Privacy Policy. Within the scope of the Services, personal data may be shared with subcontractors or partners, if this is necessary for the fulfillment and performance of our Services, for example, to process your payments. In any instance where we choose to share personal data we will enter into a Data Processing Agreement to ensure that the recipient of the personal data processes said information in accordance with applicable legislation as well as to ensure that the recipient has taken the necessary technical and organizational actions to, in a satisfactory fashion, be able to protect the rights and freedoms of you as a Data Subject.
11.2 Furthermore we may share personal data if we are required to do so by law, court order or if withholding such personal data would hinder an ongoing legal investigation.

12. Your rights
12.1 We are responsible for your personal data being processed in accordance with applicable legislation.
12.2 Upon your request, or at our own initiative, we will correct, de-identify, delete or complete any information that has been found to be wrongful, incomplete or misleading.
12.3 You have the right to demand access to your personal data. This means that you have the right to demand transcripts regarding the processing that we have maintained over your personal data. You also have the right to receive a copy of the personal data that are being processed. You have the right to, once a year and through written application, without cost receive a transcript regarding what personal data is stored in regards to you, the purpose of the storage and processing as well as to whom said information has been made accessible. You also have, within the transcripts, the right to be informed of the period of time in which the personal data will be stored and what criteria we have used to determine that period of time.
12.4 You have the right of correction of your personal data. We will, upon your request and as quickly as possible correct the incorrect or incomplete personal data we process in regards to you.
12.5 You have the right to demand deletion of your personal data. This means that you have the right to demand that your personal data is removed if it is no longer necessary for the objectives for which it was gathered. There may exist legal requirements stating that we may not immediately delete personal data (for example in terms of auditing and taxation related legislation). We will in any such case cease the processing being done for any other reasons than to adhere to the legislation of GDPR.
12.6 You have the right to object to any processing of personal data that is carried out on a lawful basis of weighing of interests. If you object to such processing we will only continue the processing if there are legitimate reasons for the processing that outweigh your interests.
12.7 You have the right to report our processing of your personal data to any public authority responsible for monitoring the application of the GDPR, for example, The Swedish Data

Protection Authority in Sweden. However, we do recommend that you contact us first so that we can try solving the matter in a more efficient and timely manner.

13. Cookies

When you visit our website, we may also collect information and data about you by using what is referred to as cookies. A cookie is a small file which asks permission to be placed on your computer's hard drive. Once you agree, the file is added and the cookie helps analyze web traffic or lets you know when you visit a particular site. Cookies allow web applications to respond to you as an individual. The web application can tailor its operations to your needs, likes and dislikes by gathering and remembering information about your preferences.

We use traffic logging cookies to identify which pages are being used. This helps us analyze data about web page traffic and improve our website in order to tailor it to customer needs. We only use this information for statistical analysis purposes and then the data is removed from the system.

Overall, cookies help us provide you with a better website, by enabling us to monitor which pages you find useful and which you do not.

14. Changes to this policy

We reserve the right to make amendments to this Privacy Policy from time to another. The date for the latest amendment is stated at the beginning of this Privacy Policy. Material changes to this Privacy Policy will be notified to the user email address provided to us, and the Privacy Policy will become effective six (6) weeks after such notification. You will have no obligation to continue using the Services following any such notification, but if you do not terminate your account as described in the Termination section in our Terms of Service during such six (6) week period, your continued use of the Platform after the end of that six (6) week period will constitute your acceptance of the revised Privacy Policy.

15. Contact

Soundation AB (company reg. no. 556561-6629) is the Data Controller for the processing of your personal data.

If you would like to have additional information on how your personal data is handled, please contact us through a written and personally signed request sent to:
Soundation AB
Mailbox 2452 36
111 75 Stockholm
Sweden

In the letter, please include your name, address, email, telephone number and personal ID number. Please also enclose a copy of your ID. A reply will be sent to your email address.

EXHIBIT "F"

DATA SECURITY REQUIREMENTS

Adequate Cybersecurity Frameworks

2/24/2020

The Education Security and Privacy Exchange ("Edspex") works in partnership with the Student Data Privacy Consortium and industry leaders to maintain a list of known and credible cybersecurity frameworks which can protect digital learning ecosystems chosen based on a set of guiding cybersecurity principles* ("Cybersecurity Frameworks") that may be utilized by Provider .

Cybersecurity Frameworks

	MAINTAINING ORGANIZATION/GROUP	**FRAMEWORK(S)**
	National Institute of Standards and Technology (NIST)	NIST Cybersecurity Framework Version 1.1
	National Institute of Standards and Technology (NIST)	NIST SP 800-53, Cybersecurity Framework for Improving Critical Infrastructure Cybersecurity (CSF), Special Publication 800-171
	International Standards Organization (ISO)	Information technology — Security techniques — Information security management systems (ISO 27000 series)
	Secure Controls Framework Council, LLC	Security Controls Framework (SCF)
	Center for Internet Security (CIS)	CIS Critical Security Controls (CSC, CIS Top 20)
	Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S))	Cybersecurity Maturity Model Certification (CMMC, ~FAR/DFAR)

EXHIBIT "G"

Supplemental SDPC State Terms for

Version 1.0

[The State Supplement is an ***optional*** set of terms that will be generated on an as-needed basis in collaboration between the national SDPC legal working group and the State Consortia. The scope of these State Supplements will be to address any state specific data privacy statutes and their requirements to the extent that they require terms in addition to or different from the National Standard Clauses. The State Supplements will be written in a manner such that they will not be edited/updated by individual parties and will be posted on the SDPC website to provide the authoritative version of the terms. Any changes by LEAs or Providers will be made in amendment form in an Exhibit (**Exhibit "H"** in this proposed structure).]

EXHIBIT “H”

Additional Terms or Modifications

Version 1.0

LEA and Provider agree to the following additional terms and modifications:

None